MP210372 MITRE PRODUCT

MITRE

Sponsor: AFLCMC/CROWS Dept. No.: N141 Contract No.: FA8702-21-C-0001 Project No.: 03214PA0-SG

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

For MITRE-Internal and AFLCMC/CROWS Use Only. Other distribution prohibited without explicit written authorization.

©2021 The MITRE Corporation. All rights reserved.

Bedford, MA

USAF Cyber Resiliency Office for Weapon Systems (CROWS) Evaluation of the Cigent Dynamic Data Defense Engine (D3E) App and Self-Encrypting Solid-State Drive

Feature Verification and Assessment of D3E on USAF Windows Platforms

Author: John G. Mulrey

July 2021

Approved By

22JUL2021

Christian E. Fiore II CROWS Task Leader

Date

Abstract

At the request of the United States Air Force Cyber Resiliency Office for Weapons Systems (USAF CROWS) program, MITRE evaluated Cigent Technology's data-protection solution consisting of (1) Dynamic Data Defense Engine (D3E) software version 2.4.4 and (2) firmware protection afforded by D3E-equipped self-encrypting Solid-State Drives (SSDs).

D3E Software Protection

The purpose of the D3E app is to protect any endpoint files designated as sensitive, even when endpoint cybersecurity protection has been bypassed and user credentials have been compromised [1]. D3E supplements a platform's DoD CAC¹/login authentication, requiring the use of additional authentication to access designated sensitive information under prescribed conditions.

Cigent D3E software lets administrators assign protection levels to file types and folders, based on the sensitivity of the data. The table below provides a brief overview of the D3E protection afforded for each data-sensitivity designation, as well as the locked status and authentication requirements for each data-protection level.

| Sensitivity of Data | Most Sensitive | Sensitive | Considered Not Sensitive |
|------------------------------------|-------------------|--|-----------------------------|
| Data-Protection Requirements | Highest | High | Protection Unnecessary |
| D3E Protection Designation | Always On | Dynamic | None |
| D3E Locked Status | Locked by Default | Locked Conditionally When D3E Detects Threat | Unlocked |
| Requires MFA/PIN to Unlock Data | Always | Under Threat Conditions | N/A |

D3E software currently does not encrypt files or folders to protect them. Instead, D3E uses "a mini-filter driver which blocks access to protected files, asking for authentication before allowing access. In the near future, there will be an option in D3E to encrypt files in protected folders. These can then be shared with others in a protected manner via email/cloud file systems/etc." [2]. Cigent is seeking FIPS² 140-2 certification for the future D3E encryption [3].

Cigent tailored their D3E software to work with the following Air Force platform types³:

• Windows 10 (Win10), 64-bit Operating System (OS)

¹ DoD CAC = Department of Defense Common Access Card

² FIPS = Federal Information Processing Standard(s)

³ D3E also works with Windows 8, but the Air Force did not cite that as a needed D3E platform.

- Windows 7 (Win7), 64-bit OS
- Win7, 32-bit OS

MITRE evaluated D3E on each of these platform types. An overview of the evaluation results is contained in Section 3 and details are described in Appendix A.

D3E did an admirable job of protecting sensitive data. File types and folders requiring the highest level of security were marked for *Always On* protection, meaning that the information's default state was locked and inaccessible. Such information could be unlocked only by the user's entry of a PIN⁴. Sensitive information requiring a slightly lower level of security was marked for *Dynamic* protection. Files and folders with *Dynamic* protection normally are unlocked and accessible; such information was locked automatically only when D3E sensed a threat and engaged *ActiveLock*. When D3E's AI⁵-driven Analysis Engine determines that the threat level is elevated, "D3E responds by securely locking files, blocking suspicious devices, or sending an alert to a SIEM⁶ or SOC⁷" [4]. Under *ActiveLock*, file types or folders designated for protection, whether *Dynamic* or *Always On*, are accessible only after authentication has been used.

We executed a variety of tests at each of the three laptops to ensure that D3E (1) triggered *ActiveLock* status when appropriate and (2) allowed or disallowed file access in accordance with data sensitivity and the threat status at the protected computer.

Cigent Firmware Protection

Cigent also supports *Firmware Locking* by means of D3E-equipped self-encrypting SSDs. The primary roles of Cigent firmware protection are data protection and information hiding. Cigent secure SSDs also support such features as undetectable data-access logs and verification of drive-erasure status. Cigent's K2 SSD "is in the process of FIPS 140-2 certification with expected timeframe of September this year" [3].

Important features of the self-encrypting SSDs are summarized below. We evaluated *Firmware Locking* using a Cigent-provided Win10 laptop.

- <u>Data Protection</u>: Firmware in the Cigent self-encrypting SSDs checks continuously to ensure that D3E and host security are running. If the firmware detects that security agents⁸ are missing or have stopped, D3E engages *ActiveLock* and locks any files marked for *Dynamic* protection. (Files with *Always On* protection are locked by default; however, if any *Always On* files happen to be open when a security incident occurs, those files will be locked, as well.)
 - Among the ways Cigent SSDs protect information is the *KeepAlive* feature. *KeepAlive* tethers Cigent Secure SSDs to the D3E software running on them by means of a non-replayable heartbeat between the drive and D3E. When the feature is activated, Secure SSDs will enact *ActiveLock* and prevent file access if

⁴ PIN = Personal Identification Number

⁵ AI = Artificial Intelligence

⁶ SIEM = Security Information and Event Management system

⁷ SOC = Security Operations Center

⁸ D3E is integrated with Windows Defender and other antivirus solutions registered with Windows Security Center [8].

the drive fails to receive the heartbeat signal in time. The feature is designed to prevent hackers from stopping D3E protection on unlocked Secure Drives.

- <u>Information hiding</u>: Secure drives/partitions become "invisible" when threats are detected. With *Always On* security, secure drives are locked. They remain unmounted and invisible to the Operating System (OS) until the administrator unlocks (mounts) them by following the prescribed authentication method. Similarly, secure drives marked for *Dynamic* security "disappear" from the Windows OS when a detected threat triggers D3E to lock them [1].
- <u>Undetectable Data-Access Logs</u>: Data access logs stored securely in SSD firmware cannot be detected or erased, yielding a valuable tool for post-breach analysis.
- <u>Verification of Drive Erasure Status</u>: Cigent's *True Erase* feature is useful for assessing the erasure status of attached SSDs. *True Erase* provides reliable feedback on whether a previously-wiped drive has, in fact, been erased, "report(ing) each block's erased or unerased state after a wipe attempt" [1].

A detailed summary of the *Software & Firmware Locking* evaluations is contained in Appendix A to this report. Each of the D3E functions performed well, meeting the performance capabilities advertised in Cigent documentation. There were a few instances of anomalous or unexpected behavior, however, which MITRE identified to Cigent. Anomalies are listed below and summarized in greater detail in Appendix B. MITRE also offered suggestions about how to make D3E more convenient for the end user. Our recommendations are contained in Section 4 of this report.

Anomalies⁹:

- 1. Password/PIN reuse is allowed.
- 2. Honeypot files can be moved, changed, and deleted.
- 3. Windows Service host process periodically tries to access the default honeypot file.¹⁰
- 4. APPCRASH condition occurred on the Win7 64-bit laptop.

Summary:

The Cigent products performed well. MITRE recommends that Cigent D3E and Secure SSDs be considered for further evaluation. An Air Force *Innovation Pitch* event would be an excellent venue for Cigent to showcase its products. We believe that, in addition to its data-protection role, the Cigent solution could be beneficial for defensive and offensive cyber operations.

⁹ The first two anomalies are attributable to D3E software, and modifications are expected to be easy to implement. Items three and four will require further testing.

¹⁰ MITRE is working with Cigent to determine which process is attempting to access the *Deception* file. If the application is deemed legitimate, it could be designated a "Safe App." This would put a stop to the unwanted alarm conditions. Note that the Safe App feature requires a special license from Cigent, available to premium customers upon request.

This page intentionally left blank.

Table of Contents

| 1 | Inti | roduc | ction | 1-1 |
|---|------|--------|---|-----------|
| 2 | Cig | gent I | D3E Overview | 2-3 |
| | 2.1 | D3] | BE – Software-Based Data Protection | 2-3 |
| | 2.1 | .1 | D3E Software Protection for Sensitive Data | 2-3 |
| | , | 2.1.1 | 1.1 How D3E Protects Information | 2-4 |
| | 2.1 | .2 | Triggers for D3E Dynamic Protection | 2-5 |
| | 2.1 | .3 | Deception | 2-5 |
| | , | 2.1.3 | 3.1 Deception Files | 2-5 |
| | , | 2.1.3 | 3.2 Network Manager – Cigent Deception Ports | 2-6 |
| | 2.2 | Firi | rmware-Based Data Protection | 2-6 |
| | 2.2 | .1 | Self-Encrypting SSDs | 2-7 |
| | , | 2.2.1 | 1.1 How Cigent Self-Encrypting SSDs Protect Data | 2-7 |
| | , | 2.2.1 | 1.2 Drive Types Supporting Cigent <i>Firmware Locking</i> Mode [4] [6] [7 |] [9] 2-7 |
| | - | 2.2.1 | I.3 Important Features of the Self-Encrypting SSDs [7] | 2-8 |
| | , | 2.2.1 | 1.4 Automatic Detection of Supported Self-Encrypting SSDs | |
| | 2.3 | D31 | BE Authentication (Unlocking) Methods | 2-10 |
| 3 | Fur | nction | onality Testing Highlights | |
| | 3.1 | Cig | gent Firmware Locking Mode | |
| | 3.2 | Cig | gent Secure SSD Features | |
| | 3.3 | D31 | BE Software Locking Mode | |
| | 3.4 | Ren | movable Storage Protection | |
| 4 | Co | nclus | sions and Recommendations | 4-16 |
| | 4.1 | Ove | zerall Impression | |
| | 4.2 | Dep | ployment Recommendations | |
| | 4.2 | .1 | Use Standardized Data-Protection Designations | |
| | 4.2 | 2 | Deploy a Central Management Console | |
| | 4.2 | 3 | Managing Files with Always On and Dynamic Protection | |
| | 2 | 4.2.3 | 3.1 Use File-Extension Protection Only for Uncommon File Types | |
| | 2 | 4.2.3 | 3.2 Purge Extra Copies of Sensitive Files | |
| | 4.3 | Sug | ggestions for Feature Enhancements | |
| | 4.3 | .1 | Expedite FIPS 140-2 certification for D3E Software and Cigent SSDs | |
| | 4.3 | .2 | Implement DoD CAC as a Method of D3E Authentication | |
| | 4.3 | .3 | Allow Multiple Administrator Actions per Authentication | |

| 4.3.4 I | Password and PIN Reuse | |
|------------|---|------|
| 4.3.5 | Consider Implementing File Name Protection | 4-19 |
| 4.3.6 | Alert Users to Potentially Sensitive Information in Unprotected Folders | 4-19 |
| 5 Referenc | es | 5-20 |
| Appendix A | D3E Evaluation Details | A-1 |
| A.1 Cige | ent Firmware Locking Mode | A-1 |
| A.1.1 (| Configure Cigent Secure SSD Drives | A-1 |
| A.1.1. | 1 Review Current Secure Drive Configuration | A-1 |
| A.1.1. | 2 De-Configure a D3E Secure Drive | A-4 |
| A.1.1. | 3 Reconfigure the Secure Drive | A-5 |
| A.1.1. | 4 Enable the Mini Authentication Popup | A-8 |
| A.1.1. | 5 Enable Always On File Type Protection | A-9 |
| A.1.1. | 6 Feature Evaluation Results | A-9 |
| A.1.2 | Always On and Dynamic Protection | A-9 |
| A.1.2. | 1 Accessing Always On Files | A-10 |
| A.1.2. | 2 Accessing <i>Dynamic</i> Files | A-11 |
| A.1.2. | 3 Feature Evaluation Results | A-12 |
| A.1.3 | Deception Files | A-12 |
| A.1.3. | 1 Attempt to Access the Default <i>passwords.xls Deception</i> File | A-13 |
| A.1.3. | 2 Attempt to Access User-Created <i>Deception</i> File | A-15 |
| A.1.3. | 3 Evaluation Results | A-16 |
| A.1.4 | Windows Defender and Antivirus Integration | A-17 |
| A.1.4. | 1 Evaluation Steps for Antivirus Integration | A-18 |
| A.1.4. | 2 Evaluation Results | A-21 |
| A.1.5 | Network Manager | A-22 |
| A.1.5. | 1 D3E Response to Untrusted Network Connections | A-23 |
| A.1.5. | 2 D3E Response to Port-Scanning Attempts | A-26 |
| A.1.5. | 3 Evaluation Results | A-30 |
| A.2 Cige | ent Secure SSD Features | A-30 |
| A.2.1 (| Command Log Audit | A-30 |
| A.2.1. | 1 Evaluation Steps for Command Log Audit | A-30 |
| A.2.1. | 2 Evaluation Results | A-34 |
| A.2.2 | True Erase | A-34 |
| A.2.2. | 1 <i>True Erase</i> Evaluation Steps | A-34 |

| A.2.2 | 2.2 | Evaluation Results | A-35 |
|---------|--------------|---|------|
| A.2.3 | Кеер | oAlive (Tethering) | A-35 |
| A.2.3 | 5.1 | KeepAlive Evaluation Steps | A-36 |
| A.2.3 | 5.2 | Evaluation Results | A-42 |
| A.3 D31 | E <i>Sof</i> | ftware Locking Mode | A-42 |
| A.3.1 | Fold | ler Protection | A-42 |
| A.3.1 | .1 | Establish Secure Data Locations on Win7 Laptops | A-42 |
| A.3.1 | .2 | Remove Always On and Dynamic Protection Folders | A-44 |
| A.3.1 | .3 | Assign both Dynamic and Always On Protection to a Folder | A-44 |
| A.3.1 | .4 | Win10 64-Bit Evaluation | A-45 |
| A.3.1 | .5 | Win7 32-Bit Evaluation | A-45 |
| A.3.1 | .6 | Win7 64-Bit Evaluation | A-45 |
| A.3.2 | Dyne | amic and Always On Protection | A-45 |
| A.3.2 | 2.1 | Accessing Always On Files | A-45 |
| A.3.2 | 2.2 | Accessing Dynamic Files | A-46 |
| A.3.2 | 2.3 | Win7 32-Bit Evaluation | A-49 |
| A.3.2 | 2.4 | Win7 64-Bit Evaluation | A-49 |
| A.3.3 | Dece | eption Files | A-49 |
| A.3.3 | 5.1 | Attempt to Access the Default passwords.xls Deception File | A-50 |
| A.3.3 | 5.2 | Win7 32-Bit Evaluation | A-52 |
| A.3.3 | 5.3 | Win7 64-Bit Evaluation | A-53 |
| A.3.4 | Win | dows Defender Integration | A-53 |
| A.3.4 | .1 | Evaluation Steps for Antivirus Integration | A-53 |
| A.3.4 | .2 | Win7 32-Bit Evaluation | A-56 |
| A.3.4 | .3 | Win7 64-Bit Evaluation | A-56 |
| A.3.5 | Netw | vork Manager | A-56 |
| A.3.5 | 5.1 | D3E Response to Untrusted Network Connections | A-56 |
| A.3.5 | 5.2 | D3E Response to Port-Scanning Attempts | A-59 |
| A.3.5 | 5.3 | Win7 32-Bit Evaluation | A-64 |
| A.3.5 | 5.4 | Win7 64-Bit Evaluation | A-64 |
| A.3.6 | File | Extension Protection | A-65 |
| A.3.6 | 5.1 | Evaluation Steps for File Extension Protection | A-65 |
| A.3.6 | 5.2 | Conflicts between Folder Protection and File Extension Protection | A-74 |
| A.3.6 | 5.3 | Win10 Evaluation | A-76 |

| A.3.6.4 Win7 32-Bit Evaluation | A-76 |
|--|------|
| A.3.6.5 Win7 64-Bit Evaluation | A-76 |
| A.4 Removable Storage Protection | A-76 |
| A.4.1 <i>Removable Storage Protection</i> – Evaluation Steps | A-76 |
| A.4.1.1 Win10 Evaluation | A-78 |
| A.4.1.2 Win7 32-Bit Evaluation | A-78 |
| A.4.1.3 Win 7 64-Bit Evaluation | A-78 |
| Appendix B Anomalies | B-1 |
| B.1 Password Reuse is Allowed | B-1 |
| B.2 Honeypot Files Can Be Moved, Changed, and Deleted | B-2 |
| B.2.1 Manipulation of User-Generated Honeypot Files | B-2 |
| B.2.2 Manipulation of <i>passwords.xls</i> File | B-2 |
| B.2.3 Impact of Unintended <i>Deception</i> Feature Behavior | B-2 |
| B.2.4 Issue Resolution | B-2 |
| B.3 Windows Service Host Process Tries to Access passwords.xls | B-3 |
| B.4 APPCRASH Condition at Win7 64-Bit Laptop | B-4 |
| Appendix C D3E Central Management Console | C-1 |
| C.1 Overview | C-1 |
| C.2 Notifications | C-3 |
| C.3 Security Policies | C-3 |
| C.3.1 Set the Synchronization Interval | C-3 |
| C.3.2 Safe Applications | C-4 |
| C.4 Third-Party Security Integration | C-4 |
| Appendix D Abbreviations and Acronyms | D-1 |

List of Figures

| Figure 2-1. Deception File Locations - Obfuscated and Displayed | |
|--|------|
| Figure 2-2. D3E Dashboard [4] | |
| Figure 2-3. Supported Drive Type Found | |
| Figure 2-4. Supported Drive Type Not Found | |
| Figure A-1. V2.4.4 Dashboard Indicating that Secure Drives are Installed | A-1 |
| Figure A-2. Two Physical Drives Installed | A-2 |
| Figure A-3. Total Drive Space | A-2 |
| Figure A-4. Equal Allocations for Always On & Dynamic Partitions | A-3 |
| Figure A-5. All Drives Visible in Windows Explorer | A-3 |
| Figure A-6. Always On Partitions Not Visible | A-4 |
| Figure A-7. System-Generated Backup File for Each Drive | A-4 |
| Figure A-8. Click Deconfigure for the Selected Drive | A-5 |
| Figure A-9. Enter Backup-File Location and Provision PW to Deconfigure Drive | A-5 |
| Figure A-10. Configure the Secure Drive | A-5 |
| Figure A-11. Enter D3E Secure Drive Password [8] | A-6 |
| Figure A-12. Select Location for Secure Drive Password Backup | A-6 |
| Figure A-13. Select Both Checkboxes | A-7 |
| Figure A-14. KeepAlive Feature | A-7 |
| Figure A-15. Post-Configuration L & P Secure Drives | A-8 |
| Figure A-16. Allocate Dynamic & Always On Drive Space [8] | A-8 |
| Figure A-17. Toggle D3E Settings | A-9 |
| Figure A-18. Extract Zipped Test Data to L & P Drives | A-10 |
| Figure A-19. Contents of P & L Drives with Extracted Data | A-10 |
| Figure A-20. Always On Drive Before and After Unlocking | A-11 |
| Figure A-21. Files in Always On Drive Require PIN to Unlock | A-11 |
| Figure A-22. Dynamic Files Open Without MFA | A-12 |
| Figure A-23. Locate the passwords.xls Deception File | A-13 |
| Figure A-24. D3E Threat Notifications | A-13 |
| Figure A-25. Deception Threat Detected | A-14 |
| Figure A-26. Secure Drives Locked upon Deception Event | A-14 |
| Figure A-27. Secure Drives Invisible in Windows Explorer | A-15 |
| Figure A-28. Add a Deception File. | A-16 |
| Figure A-29. Successful Attempt to Move and Inspect Deception File | A-17 |
| Figure A-30. Modified <i>Deception</i> File in Honeypot Location | A-17 |
| Figure A-31. Setting to Trigger ActiveLock for AV Tampering | A-18 |
| Figure A-32. Disable AV – Step 1 | A-19 |
| Figure A-33. Disable AV – Step 2 | A-19 |
| Figure A-34. Disable AV – Step 3 | A-20 |
| Figure A-35. Tampering with AV Triggers ActiveLock | A-20 |
| Figure A-36. ActiveLock → Always On Drives Not Visible in Explorer | A-21 |
| Figure A-37. D3E Indicates Virus Protection Disabled | A-22 |
| Figure A-38. Protection Definitions are Out of Date | A-22 |
| Figure A-39. Untrust an Existing Trusted Network Connection | A-23 |
| Figure A-40. Untrusting a Network Triggers ActiveLock [8] | A-24 |
| | |

| Figure A-41. | Try to Open File with <i>Dynamic</i> Protection | A-24 |
|--------------|---|------|
| Figure A-42. | ActiveLock Prevents Opening of File with Dynamic Protection | A-25 |
| Figure A-43. | Untrusted Connection is Lost | A-26 |
| Figure A-44. | Return the Network to a Trusted Condition [8] | A-26 |
| Figure A-45. | Locate the Port-Scanning File on the Desktop | A-27 |
| Figure A-46. | Make Sure <i>Network Deception</i> is Active | A-27 |
| Figure A-47. | Run the Attack Script | A-28 |
| Figure A-48. | Execution of Port-Scan Attack Script | A-28 |
| Figure A-49. | D3E Reaction to Port Scan | A-29 |
| Figure A-50. | ActiveLock Disengaged | A-30 |
| Figure A-51. | Click "Advanced" | A-31 |
| Figure A-52. | Click "Command Log" | A-31 |
| Figure A-53. | Command Log Audit Page | A-31 |
| Figure A-54. | SSD Scan Results | A-32 |
| Figure A-55. | Saving Scan Results to a CSV File | A-33 |
| Figure A-56. | Two CSV Files Generated | A-33 |
| Figure A-57. | Drill Down for Audit Data for Shorter Time Span | A-33 |
| Figure A-58. | Command Log Showing Unauthorized Access to File | A-34 |
| Figure A-59. | Execute the Erase Verify Procedure | A-35 |
| Figure A-60. | Erase Verification Analysis | A-35 |
| Figure A-61. | KeepAlive Provisioned on One Drive | A-36 |
| Figure A-62. | Tethering Evaluation – Step 1 | A-37 |
| Figure A-63. | Tethering Evaluation – Step 2 | A-37 |
| Figure A-64. | Tethering Evaluation – Step 3 | A-38 |
| Figure A-65. | Tethering Evaluation – Step 4 | A-38 |
| Figure A-66. | Tethering Evaluation – Step 5 | A-39 |
| Figure A-67. | Tethering Evaluation – Step 6 [8] | A-39 |
| Figure A-68. | Tethering Evaluation – Step 7 [8] | A-40 |
| Figure A-69. | Tethering Evaluation – Step 8 [8] | A-40 |
| Figure A-70. | D3E Has Been Disabled | A-41 |
| Figure A-71. | Cannot Copy Files to the Always On Drive | A-41 |
| Figure A-72. | Folder Protection – Setup Step 1 | A-43 |
| Figure A-73. | Folder Protection – Setup Step 2 | A-43 |
| Figure A-74. | New Dynamic and Always On Folders Added | A-44 |
| Figure A-75. | Removing Always On and Dynamic Protection Folders | A-44 |
| Figure A-76. | Cannot Assign Dual Protection Configurations to a Folder | A-45 |
| Figure A-77. | Browse to HighlyConfidential Folder | A-46 |
| Figure A-78. | Authentication Required to Unlock Always On Protection | A-46 |
| Figure A-79. | Browse to CompanyInternal Folder | A-47 |
| Figure A-80. | Dynamic Files Open when ActiveLock not Engaged | A-47 |
| Figure A-81. | Locate the Default Deception File | A-48 |
| Figure A-82. | D3E Locks Engages ActiveLock when Threats Are Sensed | A-48 |
| Figure A-83. | ActiveLock Must Be Cleared before Opening Dynamic Files | A-49 |
| Figure A-84. | Dynamic File Opens After ActiveLock Has Been Cleared | A-49 |
| Figure A-85. | Location of Default Deception File for This Laptop | A-50 |
| Figure A-86. | Honeypot File in Explorer | A-50 |

| Figure A-87. D3E Reaction to File Deception Event | A-51 |
|--|------|
| Figure A-88. Attempt to Open File with Dynamic Protection | A-51 |
| Figure A-89. Access Blocked to File with Dynamic Protection | A-52 |
| Figure A-90. Default Honeypot File after Editing and Return to Original Location | A-53 |
| Figure A-91. Lack of AV Protection Triggers ActiveLock | A-54 |
| Figure A-92. AV Protection Missing from Win7 Host | A-54 |
| Figure A-93. Review the PC's Security Status | A-55 |
| Figure A-94. Cannot Access File with Dynamic Protection in ActiveLock State | A-56 |
| Figure A-95. Untrust the Current Host Network | A-57 |
| Figure A-96. Untrusted Network Connection Triggers ActiveLock | A-57 |
| Figure A-97. Attempt to Open File with Dynamic Protection | A-58 |
| Figure A-98. Enter Authentication to Open Protected File | A-58 |
| Figure A-99. File Opens with Authentication | A-58 |
| Figure A-100. Return to Original Network Trust Status | A-59 |
| Figure A-101. In Network We Trust | A-59 |
| Figure A-102. Make Sure Network Deception is Active | A-60 |
| Figure A-103. Locate the Port-Scanning File on the Desktop | A-61 |
| Figure A-104. Run the Attack Script | A-62 |
| Figure A-105. Execution of Port-Scan Attack Script | A-62 |
| Figure A-106. D3E Reaction to Port Scan | A-63 |
| Figure A-107. PIN Needed to Open Dynamic File after Port Scan | A-64 |
| Figure A-108. ActiveLock Disengaged | A-64 |
| Figure A-109. Folder Protection Menu [8] | A-65 |
| Figure A-110. Remove Folder Protection [8] | A-66 |
| Figure A-111. No Folder Protection Assigned [8] | A-66 |
| Figure A-112. File Type Protection Menu [8] | A-67 |
| Figure A-113. Allow Always On File Extension Must Be Enabled | A-68 |
| Figure A-114. Enabling Always On File Protection | A-68 |
| Figure A-115. Setup Screen for Adobe File Protection | A-69 |
| Figure A-116. Choose Protection Type for PDF Files | A-69 |
| Figure A-117. Adobe Files Partially Protected | A-70 |
| Figure A-118. Custom File Type Protection | A-70 |
| Figure A-119. Add Dynamic Protection for txt Files | A-71 |
| Figure A-120. Authentication Required to Open File with Always On Protection | A-71 |
| Figure A-121. File Displayed After Authentication | A-72 |
| Figure A-122. Authentication Not Needed if ActiveLock Not Engaged | A-73 |
| Figure A-123. Under ActiveLock Text File Won't Open without Authentication | A-73 |
| Figure A-124. Text File is Accessible after Authentication | A-73 |
| Figure A-125. Folder with PDF File | A-74 |
| Figure A-126. Mark Folder for Dynamic Protection | A-74 |
| Figure A-127. Always On Protection Assigned to PDF Files | A-75 |
| Figure A-128. Untrust Removable Storage – Non-SSD Laptop | A-77 |
| Figure A-129. Post Untrust of Removable Storage - Non-SSD Laptop | A-77 |
| Figure A-130. Cannot Access File on Untrusted Removable Drive | A-77 |
| Figure A-131. "Forget" Removable Device on Cigent SSD Laptop | A-78 |
| Figure A-132. Forgotten Storage Device – SSD-Equipped Laptop | A-78 |

| Figure B-1. Host Process Triggers D3E Deception Event | B-3 |
|---|-----|
| Figure B-2. D3E Dashboard APPCRASH | B-4 |
| Figure C-1. Central Management Console Dashboard | C-1 |
| Figure C-2. Device Security Status | C-2 |
| Figure C-3. Threat History for Managed Devices | C-2 |
| Figure C-4. Security-Event Notifications | C-3 |
| Figure C-5. Central Manager Policy Screen | C-3 |
| Figure C-6. Policy – Safe Applications | C-4 |
| Figure C-7. Third-Party Integration for User Authentication | C-5 |
| | |

List of Tables

| Table 2-1. D3E Data-Protection Levels | |
|--|--|
| Table 3-1. Cigent Firmware Locking Mode Evaluation – Results | |
| Table 3-2. Cigent Secure SSD Features Evaluation – Results | |
| Table 3-3. D3E Software Locking Mode Evaluation – Results | |
| Table 3-4. Removable Storage Protection Evaluation – Results | |

1 Introduction

MITRE evaluated Cigent Technology's Dynamic Data Defense Engine (D3E) endpointprotection application at the request of the United States Air Force Cyber Resiliency Office for Weapons Systems (USAF CROWS). This report documents MITRE's D3E evaluation.

Cigent data security has two modes of operation: (1) D3E *Software Locking* mode and (2) *Firmware Locking* mode for selected types of solid-state drives (SSDs)¹¹ with D3E software running on the SSD. *Software Locking* works on any Windows 10 (Win10) or Windows 7 (Win7) installation and protects files in "user-specified folders on any non-removable storage device" [4]. Cigent's *Firmware Locking* mode works with SATA¹²- and NVMe¹³-specific APIs¹⁴ to secure dedicated partitions, which Windows view as drives. "Firmware locking mode is supported on HDDs¹⁵ and SSDs supporting TCG¹⁶ OPAL¹⁷ [5] 2.0 and Cigent Secure SSDs" [4]. Also referred to as Cigent Secure SSD Storage, the product is compatible with Windows 10, 8, and 7 operating systems [6]. D3E software locks user-specified folders, and file types on Windows computers to protect the information from unauthorized access. *Firmware Locking* provides protection to entire drives (partitions). The locking/unlocking of these partitions is under the control of the D3E administrator.

We used three personal computers (PCs) and one external Universal Serial Bus (USB) drive in our assessment, as described below.

Cigent loaned a Windows 10 64-bit laptop for the MITRE assessment. The Cigent laptop was delivered with D3E version 1.6.10. We later upgraded this to version 2.4.4. We installed the machine on the NERVE¹⁸ network, so that it would be accessible from remote locations. The Cigent PC was equipped with a CTI¹⁹ SSD drive suitable for testing the Cigent firmware-based protection feature discussed in Sections 3.1 and 3.2 and in Sections 1 and 2 of Appendix A. It was possible to test D3E's software- and firmware-locking features on this laptop. Cigent also provided a secure USB external drive for our evaluation.

MITRE provided a pair of Win7 laptops, one with a 64-bit processor, and a second with a 32-bit processor. We installed D3E version 2.4.4 on each of the Win7 machines.

The hard drives in the MITRE PCs were not compatible with Cigent firmware-based protection; i.e., they did not match any of the SSD drive types listed in Section 2.2.1.1. Consequently, only D3E software-based protection was assessed on the MITRE laptops.

Section 2 contains a brief overview of the D3E application and firmware-locking data protection, identifying the Cigent solution's important features and benefits. Section 3 summarizes results of

¹¹ Refer to Section 2.2.1.1 for a list of SSD drive types that can support Cigent firmware locking.

¹² SATA = Serial Advanced Technology Attachment

¹³ NVMe = Non-Volatile Memory Express

¹⁴ API = Application Programming Interface

¹⁵ HDD = Hard Disk Drive

¹⁶ TCG = Trusted Computing Group

¹⁷ OPAL is a TCG security standard for storage devices.

¹⁸ NERVE = Networked Experimentation, Research, & Virtualization Environment

¹⁹ CTI = Cigent Technology, Inc.

our evaluation. For brevity and ease of reading of the main document, the detailed, step-by-step examination of D3E and SSD features was deferred to Appendix A. Section 4 contains conclusions and recommendations for the D3E endpoint-security product. Appendix B contains a brief summary of the few anomalies that we encountered. Finally, Appendix C contains a brief description of D3E's central management console.

2 Cigent D3E Overview

Cigent data-protection solutions help prevent unauthorized access to sensitive files, while ensuring that authorized users can always access important data, even when the host system is already compromised.

D3E uses machine learning (ML) and user-behavior-analytics (UBA) techniques to authenticate user identity. D3E also continuously checks for malware intrusion, deploying sensors to monitor events and integrating with Windows Defender or other antivirus (AV) solutions registered with Windows Security Center. D3E feeds its sensor data and the AV-derived inputs into D3E's AI-based²⁰ Analysis Engine. When the Analysis Engine determines that the threat level is elevated, "D3E responds by securely locking files, blocking suspicious devices, or sending an alert to a SIEM²¹ or SOC²²" [4]. D3E sensors are listed in Section 2.1.1.1.

As mentioned earlier, Cigent data security has two operating modes, (1) D3E *Software Locking* mode and (2) *Firmware Locking* mode on approved SSDs. These two modes are described in Sections 2.1 and 2.2, respectively. The bulk of our assessment pertains to D3E software-based protection (for results and details, refer to Section 3.3 and Appendix Section A.3); however, we also evaluated Cigent firmware-based protection, using the Cigent loaner laptop and external USB drive, as described in Sections 3.1 and 3.2 and in Appendix Sections A.1 and A.2.

2.1 D3E – Software-Based Data Protection

D3E software-based protection employs two locking modes, *Always On* and *Dynamic*, to render sensitive information impervious to data theft or ransomware <u>when locked</u>. The D3E administrator has control over which folders and file types fall into the *Always On* and *Dynamic* protection categories.

Section 2.1.1 describes D3E data protection for different sensitivity levels.

2.1.1 D3E Software Protection for Sensitive Data

• As its name implies, the *Always On* locking mode always requires one or more unlocking techniques (Multi-Factor Authentication, or MFA²³) to access; i.e., file types, folders, and partitions²⁴ marked for *Always On* protection stay locked until a user fulfills the prescribed authentication requirements and unlocks the data. Typically, a system's most sensitive information would be marked for *Always On* protection. With *Always On* protection, "sensitive files are accessible for a very limited time and only on an as needed basis by the trusted user" [6]. Refer to Table 2-1.

²⁰ AI – Artificial intelligence

²¹ SIEM = Security Information and Event Management system

²² SOC = Security Operations Center

²³ The user's device login credentials serve as the first means of authentication; D3E authentication requirements constitute the second factor.

²⁴ Drives/partitions are marked for *Dynamic* or *Always On* protection only in *Firmware Locking* mode. With software-only protection, only folders and file types can be given *Dynamic* or *Always On* protection.

• If a file type, folder, or partition is marked for *Dynamic* protection, *ActiveLock* will engage and lock those entities whenever D3E determines that a threat has been encountered. (Refer to Section 2.1.1.1 for a discussion of the types of events that will trigger employment of *Dynamic* protection.) For file types, folders and partitions marked for *Dynamic* protection, the normal status is unlocked and accessible. *Dynamic* mode would be used to protect sensitive data that does not require the same level of privacy or security as information marked for *Always On* protection. Refer to Table 2-1.

Table 2-1 provides a brief overview of the D3E protection afforded for each data-sensitivity designation, as well as the locked status and authentication requirements for each data-protection level.

| Sensitivity of Data | Most Sensitive | Sensitive | Considered Not Sensitive |
|------------------------------------|-------------------|--|-----------------------------|
| Data-Protection Requirements | Highest | High | Protection Unnecessary |
| D3E Protection Designation | Always On | Dynamic | None |
| D3E Locked Status | Locked by Default | Locked Conditionally When D3E Detects Threat | Unlocked |
| Requires MFA/PIN to Unlock Data | Always | Under Threat Conditions | N/A |

Table 2-1. D3E Data-Protection Levels

Note: In cases of dual assignment or overlap, **Always On** protection supersedes **Dynamic** (Sometimes-On/Conditional) protection. Refer to Appendix Section A.3.6.2 for further discussion about protection overlap.

The methods for unlocking data are the same in both the *Always On* and the *Dynamic* modes: the user/administrator uses an approved means of authentication. (Refer to Section 2.3 for a brief discussion of D3E authentication.) For our evaluation, we used only the PIN²⁵ method of authentication.

D3E also supports a *Group Lock* feature that locks files on multiple PCs in a preconfigured group of devices if a threat is detected on any member of the group [7]. MITRE did not evaluate D3E's *Group Lock* feature.

2.1.1.1 How D3E Protects Information

D3E software currently does not encrypt files or folders to protect them. Instead, D3E uses "a mini-filter driver which blocks access to protected files, asking for authentication before

²⁵ PIN = Personal Identification Number

allowing access. In the near future, there will be an option in D3E to encrypt files in protected folders. These can then be shared with others in a protected manner via email/cloud file systems/etc." [2]. Cigent is seeking FIPS²⁶ 140-2 certification for the forthcoming D3E encryption [3]. Cigent should expedite the certification process so that D3E can be considered for the protection of CUI²⁷ and FOUO²⁸ information.

2.1.2 Triggers for D3E Dynamic Protection

As noted above, D3E locks information whenever a threat is detected.

In Dynamic mode, D3E uses threat-detection sensors to monitor for the following [4, 8] [7]:

- Malware
- Fileless attacks
- Privilege escalation
- Endpoint security agent, e.g., Windows Defender, disabled
- Untrusted network detected (e.g., an attached network has not been explicitly trusted in D3E)
- An untrusted network device scans the Cigent-protected machine for open ports and connects to a Cigent *Deception* port
- External-media insertion detected (e.g., unauthorized USB drive inserted)
- Network and file *Deception* engines (e.g., port-scans or attempts to access honeypot files)
- Keyboard typing cadence, network usage (User Behavior Analytics (UBA))

2.1.3 Deception

D3E includes Network and File System *Deception* engines that detect attempts to access userconfigured honeypot files or network scanning for open ports. When such attempts are detected, D3E automatically locks all file types and folders marked for *Dynamic* or *Always On* protection²⁹. Cigent claims that the D3E *Deception* engines "provide virtually zero false-positive indications of hacking activity" [1]. *Note: Care should be taken when naming and situating honeypot files, to ensure that they are not inadvertently accessed by innocent users; such accidental accesses would cause inconvenience for users and administrators*.

2.1.3.1 *Deception* Files

Deception files are honeypots that help track unauthorized access to the host system; they are intended to attract would-be attackers with enticing file names and locations. D3E creates a

 $^{^{26}}$ FIPS = Federal Information Processing Standard(s)

²⁷ CUI = Controlled Unclassified Information

²⁸ FOUO = For Official Use Only

²⁹ As noted elsewhere in this document, file types and folders marked for *Always On* protection are usually in a locked state. If they happen to be unlocked when *ActiveLock* is triggered, D3E will lock them.

default *Deception* file called *passwords.xls* in local users' **Documents** directories. D3E users can create other *Deception* files in locations of their choice. Attempts to open *Deception* files trigger *ActiveLock*, so that all file types/folders/partitions marked for *Dynamic* or *Always On* protection will be locked, and the prescribed authentication method for the device will be required to access protected information.

The D3E Dashboard hides *Deception* files for security, but D3E administrators can display their locations and file names by clicking on the *Show All* icon and using the prescribed authentication method. The left side of Figure 2-1 shows the normal, obfuscated *Deception*-file view at the D3E desktop, while the right side of the figure displays the post-authentication version.

| Deception Manage your data and network deceptions to catch attackers in the att Data Deceptions Outo Deception Outo Deceptions Outo Deception Outo Deception <t< th=""><th>Cigent D3E</th><th>- 0 ×</th><th>Cigent D3E</th><th>- D X</th></t<> | Cigent D3E | - 0 × | Cigent D3E | - D X |
|---|---|--|------------|--|
| I: Dashbaard Data Deceptions Orace interesting basing files an attacker would want to by to open. I: File Type Protection I: Add a Deception file I: File Type Protection I: File Type Protection | 9 | Deception Manage your data and network deceptions to catch attackers in the act | 9 | Deception Manage your data and network deceptions to catch attackers in the act |
| O there | Dashboard Fie Type Protection Folder Protection Secure Drives Authentication C Deception S Settings License Update Update | Data Deceptions Crade interesting looking files an attacker would want to by to open. Add a Deception file Show All Image: Show All Image: Show All and the state of the real ones are not in use by you Image: Show All and the state of the real ones are not in use by you | | Data Deceptions Section in terreting boking files an attacher would want to by to open. Image: Add a Deception file Image: Hide All Image: C:USsers\ciggent\Documents\supersecret\checkmeout.xis Image: C:Ussers\ciggent\Documents\passwords.xis Image: C:Ussers\ciggent\Documents with the state ones are not in use by you Image: C:Ussers\ciggent\Documents with the state of the rest ones are not in use by you |
| U ADOL | About | | 1 About | |

Figure 2-1. *Deception* File Locations – Obfuscated and Displayed

2.1.3.2 Network Manager – Cigent Deception Ports

Network Manager starts fake services on commonly attacked ports <u>if they are not already in use</u>. Examples include illusory copies of commonly hacked File Transfer Protocol (FTP) or Telnet³⁰ services.

If a network device scans a D3E-protected host for open ports and connects to a Cigent *Deception* port, D3E will trigger *ActiveLock* to protect sensitive information.

2.2 Firmware-Based Data Protection

D3E's robust software-based file-protection capabilities notwithstanding, software-only protection has known limitations that allow built-in protections to be bypassed [7]:

- Disabling of the endpoint's security applications, e.g., Windows Defender
- Theft of cryptographic keys
- Physical removal of the hard drive

³⁰ Telnet stands for Terminal Network.

• Bypassing the PC's OS by booting from another OS

Cigent's firmware-locking features supplement the software-locking capability cited in Section 2.1. The *Firmware Locking* mode works with SATA- and NVMe-specific APIs to secure dedicated partitions cryptographically. Section 2.2.1 below contains further information about Cigent firmware-based protection and self-encrypting SSDs.

2.2.1 Self-Encrypting SSDs

Cigent claims that its self-encrypting SSDs address the vulnerabilities of software-only protection itemized above. Self-encrypting SSDs running D3E software automatically become undetectable to attackers as soon as a threat is detected by the Analysis Engine. Files on such drives can be accessed only when the administrator uses the approved means of authentication to unlock them.

Section 2.2.1.3 provides more details about the features of Cigent's self-encrypting SSDs.

2.2.1.1 How Cigent Self-Encrypting SSDs Protect Data

Cigent secure SSDs protect data by means of encryption. "The SSD provides the encryption for every file stored on it. On top of that, the partitions are 'locked' using a key derived from the password used during configuration. To unlock a drive, D3E authenticates the user via the chosen auth method, and then unlocks the drive using the key. ... So, the PIN is not related to the key itself. That is how we can switch between PIN and other auth methods like CAC³¹ in the future" [2].

Cigent's K2 SSD is scheduled to be certified as FIPS 140-2 compliant in September 2021 [3]. Cigent should make every effort to ensure that this effort stays on track, so that the SSDs can be considered for protection of CUI and FOUO data.

2.2.1.2 Drive Types Supporting Cigent *Firmware Locking* Mode [4] [6] [7] [9]

Firmware Locking is supported on the following drive types [4]:

- HDDs and SSDs that support TCG OPAL 2.0
- Cigent Secure SSDs

The following three TCG OPAL 2.0 drive configurations currently are supported, each in sizes of 512GB, 1TB, and 2TB:

- (1) NVMe³² M.2 Internal SSD
- (2) SATA M.2 2¹/₂" Internal SSD
- (3) USB External SSD

Cigent summarizes the hardware options of their Secure SSD as follows: "Available in K2 NVMe internal and external configurations, the Cigent Secure SSD comes in three sizes —512GB, 1TB,

³¹ CAC = Common Access Card

³² NVMe = Non-Volatile Memory Express

and 2TB. It can be installed as the primary storage device on a Windows PC where the O/S runs, as secondary internal storage (such as in a desktop tower), or as external media plugged into a USB port" [6].

In each configuration, the self-encrypting SSD includes D3E's software-based functionality, as well.

2.2.1.3 Important Features of the Self-Encrypting SSDs [7]

- Custom firmware continuously checks to make sure D3E and host security agents are running. If they aren't, files marked for protection are locked.
- Data access logs are stored securely in firmware for post-breach analysis. Audit trails cannot be wiped [1]. This represents a significant Defensive Cyber Operations (DCO) capability.
- The *KeepAlive* (tethering) feature binds Cigent Secure SSDs to the D3E software running on them by means of a non-replayable heartbeat between the drive and D3E. When the feature license is turned on, Secure SSDs will enact *ActiveLock* and prevent file access if the drive fails to receive the heartbeat signal in time. The feature is intended to prevent hackers from stopping D3E protection on unlocked Secure Drives.
- Cigent's *True Erase*TM firmware feature indicates whether an erased <u>Cigent SSD hard</u> <u>drive</u> still contains data. *True Erase* supports "extended erasure verification commands to check each and every mapped and unmapped block to verify the data has been removed" [8]. Secure, verifiable data erasure from hard drives helps prevent unauthorized access to sensitive or classified information.
- With *Always On* security, secure drives are locked by default. They remain unmounted and invisible to the OS until the administrator unlocks (mounts) them by following the prescribed authentication method. Similarly, secure drives marked for *Dynamic* security "disappear" from the Windows OS when a detected threat triggers D3E to lock them [1].

2.2.1.4 Automatic Detection of Supported Self-Encrypting SSDs

D3E detects automatically whether a supported drive is installed and displays the information in the D3E Dashboard. Click on *Secure Drives* in either panel of the dashboard screen. See Figure 2-2.

| | Important Information (1 of 1) | | |
|----------------------|--------------------------------|-------------------------------------|--------------------------------|
| | PIN Setup Required | | |
| Dashboard | A PIN number m | ust be configured before using | D ³ E |
| File Type Protection | | | |
| Folder Protection | | | |
| Secure Drives | File Type Protection | Folder Protection | Secure Drives |
| Networks | Not configured | Not configured | 1 available |
| Removable Storage | 0 | 0 | 0 |
| Ceception | Ģ | 6 | ß |
| Authentication | Not connected | Removable Storage None connected | Deception 3 deception files |
| Settings | | | |
| License | | | |
| Update | | | |
| About | | | |

Figure 2-2. D3E Dashboard [4]

When D3E detects a supported drive type, clicking on *Secure Drives* yields a screen like the one in Figure 2-3. If no supported drive type is found, the display will appear as shown in Figure 2-4.



Figure 2-3. Supported Drive Type Found



Figure 2-4. Supported Drive Type Not Found

2.3 D3E Authentication (Unlocking) Methods

D3E supplements a platform's DoD CAC/login authentication, requiring the use of additional authentication to access designated sensitive information under prescribed conditions.

In our evaluation, the supplementary authentication method was PIN³³ entry. D3E also supports facial recognition and fingerprint scans as means of authentication and accommodates *Windows Hello*³⁴ and *Google Authenticator*³⁵. Cigent also is working with the Air Force to add DoD CAC as a means of MFA³⁶ for D3E.

³³ PIN = Personal Identification Number

³⁴ Windows Hello allows access to Win10 devices by means of fingerprint, facial recognition, or a secure PIN [10].

³⁵ Google Authenticator provides two-step authentication that supplements a user's password with a Google-provided one-time authentication code [11].

³⁶ The user's device login credentials serve as the first means of authentication; D3E authentication requirements constitute the second factor.

3 Functionality Testing Highlights

This section summarizes results of the D3E evaluation. A detailed, step-by-step examination of the D3E features is contained in Appendix A.

3.1 Cigent Firmware Locking Mode

The evaluation steps in this subsection were performed only on the Cigent Win10 laptop.

A high-level summary of the Cigent *Firmware Locking* Mode Evaluation is contained in Table 3-1 below.

| Feature Name | Results | Comments | ✓ / X |
|--|--|---|-------|
| SSD Config/ De-Config | Configuring and de- configuring Secure SSDs was straightforward. Performance satisfied advertised capabilities. | D3E permitted reuse of an old SSD provisioning password. We recommend that Cigent use NIST SP 800-63-3 as a guide for constructing robust digital identities. | ~ |
| <i>Always On</i> and <i>Dynamic</i> Protection | The feature performed well and met advertised capabilities. There were no issues accessing or manipulating <i>Dynamic</i> and <i>Always On</i> files on the Cigent Secure Drive. | | ~ |
| <i>Deception</i> Files | D3E File <i>Deception</i> behaved as advertised, triggering <i>ActiveLock</i> whenever an attempt was made to access a <i>Deception</i> file. | Although attempts to open user-created and system-generated <i>Deception</i> files triggered the appropriate responses, it was possible to move and edit those files and copy them back to the honeypot location. Cigent has identified a fix for the issue, which will be resolved in the next D3E build. | √/? |

 Table 3-1. Cigent Firmware Locking Mode Evaluation – Results

| AV Integration | D3E performed as expected, in that it triggered <i>ActiveLock</i> when Windows Defender was turned off. | After we ran the feature evaluation and re- activated <i>Real-time</i> <i>protection</i> in the host laptop, D3E persisted in detecting an antivirus- disabled threat, even though virus and threat- protection settings had been restored to their original state. This turned out to be appropriate behavior, because the protection definitions at the Win10 laptop were out of date. | |
|--------------------|--|---|---|
| Network Manager | The Network Manager feature functioned as advertised on the Win10 Cigent laptop equipped with Secure Drives. | | ✓ |

3.2 Cigent Secure SSD Features

The evaluation steps in this subsection were performed only on the Cigent Win10 laptop.

A high-level summary of the Cigent Secure SSD Features Evaluation is contained in Table 3-2 below.

| Feature Name | Results | Comments | ✓ / X |
|------------------------------|---|----------|-------|
| <i>Command Log Audit</i> | The Command Log Audit feature functioned as advertised on the Win10 Cigent laptop equipped with Secure Drives. | | ~ |

Table 3-2. Cigent Secure SSD Features Evaluation – Results

| True Erase | The D3E <i>True Erase</i> feature functioned as advertised on the Win10 Cigent laptop equipped with Secure Drives. | | ✓ |
|---------------------------------|--|--|---|
| <i>KeepAlive</i> (Tethering) | The <i>KeepAlive</i> SSD feature generally performed as advertised. When the heartbeat tether between the SSD and D3E was severed, firmware in the drive locked the <i>Always On</i> drive, so that it was not possible to open files or write to that drive. In other words, when the heartbeat stopped, the <i>Always On</i> drive was protected, even though the D3E service had stopped. It was possible to open the <i>Dynamic</i> Drive and write to it, but that was expected. | We did notice an anomaly in the Cigent documentation. Reference [8] states that "In less than 30 seconds, the script output will start indicating 0 files copied and you will receive a Windows error indicating Write Protect Error. Press Ctrl-C to terminate the script." In fact, Windows gave the <i>ERROR Verify</i> message shown in Figure A-69. | |

3.3 D3E Software Locking Mode

We ran *Software Locking* procedures on the two Win7 test laptops. In a few instances, we supplemented earlier testing on the Cigent SSD-equipped Win10 laptop and ran the software-locking tests on that machine, as well.

A high-level summary of the D3E *Software Locking* Mode Evaluation is contained in Table 3-3 below.

| Feature Name | Results | Comments | ✓ / X |
|--|---|---|-----------------------------|
| Folder Protection | The D3E folder- protection feature met expectations. Segregating important information into <i>Always</i> <i>On</i> and <i>Dynamic</i> folders is an excellent means of protecting sensitive data. | This feature was tested on all three evaluation laptops. | ~ |
| <i>Always On</i> and <i>Dynamic</i> Protection | The feature performed well and met advertised capabilities. | This part of the evaluation was done on the Win7 laptops. Earlier testing on the Cigent Win10 laptop yielded similar good results. (See Table 3-1.) | |
| <i>Deception</i> Files | D3E File <i>Deception</i> behaved as advertised, triggering <i>ActiveLock</i> whenever an attempt was made to access a <i>Deception</i> file. | The anomalies cited during the Cigent Win10 laptop evaluation recurred during the Win7 testing. Refer to Table 3-1. | ✓ Refer to Table 3-1. |
| AV Integration | D3E performed as expected, triggering <i>ActiveLock</i> when Windows Defender was turned off. | | ~ |
| Network Manager | The Network Manager feature functioned as advertised on the MITRE Win7 laptops. | The "untrust" and network-scanning components of the <i>Network Manager</i> feature both performed well. | ~ |
| File Extension Protection | <i>File Extension</i> <i>protection</i> worked well, performing as advertised. | We evaluated this feature on all three laptops. | ✓ |

Table 3-3. D3E Software Locking Mode Evaluation – Results

3.4 Removable Storage Protection

We tested *Removable Storage Protection* on each of the three evaluation laptops. A high-level summary of the evaluation results is contained in Table 3-4 below.

| Feature Name | Results | Comments | ✓ / X |
|---|--|--|-------|
| <i>Removable Storage Protection</i> | The feature behaved appropriately. It was possible to access files on a storage device only when the device was trusted in D3E. <i>Removable Storage</i> <i>Protection</i> prevented access to files on an untrusted removable- storage device without affecting access to files on the laptop itself. | We noticed slightly different behavior when evaluating <i>Removable</i> <i>Storage Protection</i> on the SSD-equipped Cigent Win10 laptop. The SSD-equipped laptop provides the option to "forget" a removable storage device after it has been untrusted. The next time the storage device is connected to the laptop, the user must make an explicit choice to trust the device. | |

Table 3-4. Removable Storage Protection Evaluation – Results

4 Conclusions and Recommendations

4.1 Overall Impression

Our impression of the data-protection features of Cigent's D3E software and self-encrypting SSDs was favorable. The dual firmware- and software-protection approaches combine to form a strong defense against tampering and theft of sensitive data. The *Always On* protection designation was assigned to our test systems' most sensitive information. As the name implies, file types and folders with *Always On* security were locked and inaccessible until the D3E administrator explicitly granted access to the information. Sensitive information requiring less protection than the *Always On* variety was marked for *Dynamic* protection, which locked the data only when D3E or the host detected threat conditions.

The D3E tool is flexible. The system administrator has complete control over which folders and file types are assigned *Always On* or *Dynamic* protection status. Similarly, when configuring Secure SSDs, the administrator gets to choose what percentage of each drive is given full-time, *Always On* protection.

The benefits of Secure SSDs, beyond data protection, are covered in Sections 2.2 and A.2, but the advantages of a couple of SSD features bear repeating.

- Self-encrypting SSD drives/partitions designated for *Always On* protection are unmounted and "invisible" until they are unlocked (temporarily) by the D3E administrator. This capability has obvious benefits for data security, because information on the protected drive cannot be seen, let alone accessed, by malefactors. Looking beyond data protection, the feature could yield additional cybersecurity benefits and should be investigated further.
- Among the ways Cigent SSDs protect information is the *KeepAlive* feature. *KeepAlive* tethers Cigent Secure SSDs to the D3E software running on them using a non-replayable heartbeat between the drive and D3E. Secure SSDs with the *KeepAlive* feature will enact *ActiveLock* and prevent file access if the drive fails to receive the heartbeat signal within a specified time. The feature is designed to prevent hackers from stopping D3E protection on unlocked Secure Drives.
- Cigent Secure SSDs also have a *Command Log Audit* feature that automatically stores every command sent to the drive. Commands are kept in a tamperproof location in the SSD's memory for post-breach analysis; they cannot be erased. This represents a significant DCO capability. The feature also can detect whether D3E was running at the time each command was issued, letting forensic analysts know whether the command was authorized.

In summary, MITRE recommends that Cigent D3E and Secure SSDs be considered for further evaluation. An Air Force *Innovation Pitch* event would be an excellent venue for Cigent to showcase its products. We believe that, in addition to its data-protection role, the Cigent solution could be beneficial for defensive and offensive cyber operations. We do, however, have some recommendations affecting D3E deployment, as well as a few suggestions for feature enhancements.

4.2 Deployment Recommendations

4.2.1 Use Standardized Data-Protection Designations

As noted above, the D3E tool is very flexible. That flexibility, however, could lead to inconsistencies from system to system. If D3E were deployed on a wide scale throughout the DoD, it would be wise to have a standard in place that defines how information should be categorized. This would help prevent the same data having different designations on multiple systems. The standard should:

- Identify the level of data sensitivity requiring *Always On* protection.
- Determine which level of sensitivity needs to be marked for *Dynamic* protection.
- Classify the types of data that will not require protection, i.e., files that will be afforded neither *Always On* nor *Dynamic* protection.

4.2.2 Deploy a Central Management Console

We evaluated D3E functionality separately on individual laptops to assess performance on different types of platforms. In that deployment mode, however, each laptop's administrator manages threat responses for just the individual machine. This model could lead to inconsistent and potentially unsafe threat handling. A more secure and practical mode of deployment would be to have a centralized D3E manager respond to threats across a network. D3E can be deployed with a central management console capable of monitoring and managing data security throughout a network and responding either manually or automatically. Refer to Appendix C for a brief discussion of the D3E Central Management Console.

4.2.3 Managing Files with Always On and Dynamic Protection

4.2.3.1 Use File-Extension Protection Only for Uncommon File Types

For common file extensions, such as *docx*, *pdf*, *xlsx*, and *txt*, it is preferable to segregate files needing *Always On* or *Dynamic* protection into folders marked explicitly for the desired treatment and to use D3E's *Folder Protection* feature. Use *File Extension* protection only for less common file-extension types, and only if needed. The extra administrative steps required to collect sensitive information into separate folders may be initially cumbersome, but it will avoid the potential confusion that could result from the *Folder/File Extension* conflict described in Appendix Section A.3.6.2.

4.2.3.2 Purge Extra Copies of Sensitive Files

When moving sensitive information into folders for *Dynamic* or *Always On* protection, make sure that residual copies or variants of the information do not exist in unprotected folders.

4.3 Suggestions for Feature Enhancements

4.3.1 Expedite FIPS 140-2 certification for D3E Software and Cigent SSDs

As noted in Section 2.1.1.1, D3E software does not yet provide FIPS 140-2 certified encryption, though Cigent intends to obtain that certification for their forthcoming file-encryption capability. Similarly, FIPS 140-2 certification for their K2 SSD is on Cigent's agenda. Certification for the K2 drives is expected in September 2021. Cigent should strive to keep these certification efforts on track, so that the Cigent solution can be considered for protection of FOUO and CUI information.

4.3.2 Implement DoD CAC as a Method of D3E Authentication

It was pointed out earlier that Cigent is working on adding DoD CAC as a method of D3E authentication. This is a positive development, as CAC is ubiquitous throughout the DoD and represents a proven means of MFA. Cigent should make every effort to ensure that DoD CAC is incorporated into the D3E solution as soon as possible.

4.3.3 Allow Multiple Administrator Actions per Authentication

The current D3E build requires the system administrator to enter authentication each time an unlock or other change command is issued. This method of operating is secure, and not terribly onerous; however, rather than requiring authentication prior to each administrative action, allowing the D3E administrator to perform multiple operations under a single authentication, should be considered as a time-saving device.

4.3.4 Password and PIN Reuse

As noted in the evaluation details in Appendix A, D3E permitted reuse of an old SSDprovisioning password. This was convenient for the purpose of our evaluation, but National Institute of Standards and Technology (NIST), DoD, and other agencies recommend stricter practices for reuse and strength.

- We recommend that D3E consult NIST Special Publication (SP) 800-63-3 [10] as a guide for constructing robust digital identities.³⁷
- Microsoft recommendations [11] for restricting password reuse on Win10 platforms (shown below) offer useful guidance.
 - Under *Security Settings/Account Policies*, set the **Enforce password history** parameter value to 24.
 - The Maximum password age should be set to between 60 and 90 days.

³⁷ Cigent Response: "Cigent will add the ability for password policy enforcement for both the Secure SSD password and authentication PIN in the upcoming release. It is also worth noting that that file authentication via CAC/PIV will be supported in a near term release" [19].

- The *Minimum password age* should be configured so that passwords cannot be changed immediately.
- Ideally, password policy decisions should be controlled by a single administrator at a Central Management Console, and local users/administrators should not be able to weaken the assigned policy.
- Weaker password enforcement should be allowed only in non-fielded test environments.
- At a minimum, D3E should issue a warning to the user about following DoD password guidance.
- Similar, stricter guidance should apply to setting the D3E PIN, as well.

4.3.5 Consider Implementing *File Name Protection*

MITRE believes that adding a new *File Name Protection* feature to supplement *Folder* and *File Extension Protection*, would enhance D3E. D3E administrators would be able to build an alphabetized list of files that receive either *Always On* or *Dynamic* protection. Such an implementation would avoid the *Folder/File Extension* conflict and confusion described in Appendix Section A.3.6.2.

E.g.,

- Sensitive personnel data.docx Dynamic Protection
- Attack plans 2021.pdf

Dynamic Protection Always On Protection

• In addition, use of wild-card characters would help to ensure that outdated or other variants of sensitive files receive appropriate protection.

E.g.,

| - Sensitive personnel*.* | Dynamic Protection |
|--------------------------|----------------------|
| - Attack plans 20**.* | Always On Protection |

4.3.6 Alert Users to Potentially Sensitive Information in Unprotected Folders

Section 4.2.3.2 warns users to purge extra copies of sensitive files to ensure that sensitive information is not left unintentionally in unprotected folders. Automating this warning, alerting administrators of unprotected copies or variants of sensitive files, would enhance D3E.

5 References

- [1] Cigent Technology, "Cigent D3E Layer Zero Data Protection," 2021. [Online]. Available: https://www.cigent.com/cigent-d3e.
- [2] D. Wolf, 6/17/21 email to John Mulrey: "Question about D3E FIPS 140-2 compliance", Nashua, NH: Cigent Technology, 2021.
- [3] Mulrey and Wolf, *Mulrey/Wolf Correspondence*, *16 June 2021*, Amherst, NH: Cigent Technology, 2021.
- [4] Cigent Technology, Cigent Technology Dynamic Data Defense Engine (D3E) Quick Start and Evaluation Guide, Version 2, Fort Myers, FL: Cigent Technology, 2020.
- [5] Trusted Computing Group, "TCG Storage Security Subsystem Class: Opal; Specification Version 2.01, Revision 1.00," 5 August 2015. [Online]. Available: https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_SSC_v2.01_rev1.00.pdf#page=12.
- [6] Cigent Technology, "Cigent Secure SSD Storage," Cigent Technology, 2021. [Online]. Available: https://www.cigent.com/cigent-secure-ssd.
- [7] Cigent Technology, "Cigent Solutions Overview Briefing to USAF 7/2/2020," Cigent Technology, Ft. Myers, FL, 2020.
- [8] Cigent Technology, D3E Premium Evaluation Guide, Fort Myers, FL: Cigent Technology, 2021.
- [9] Cigent Technology, "Cigent D3E Firmware Locking," Cigent Technology, 21 August 2019. [Online]. Available: https://www.youtube.com/watch?v=1-xk87LXjRs.
- [10] National Institute of Standards and Technology, "NIST Special Publication 800-63-3: Digital Identity Guidelines," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html.
- [11] Microsoft Corporation, "Enforce Password History," 19 April 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policysettings/enforce-password-history.
- [12] Cigent Technology / Dave Wolf, Zoom Presentation on D3E Central Management Console, D. Wolf, Ed., Nashua, NH: Cigent Technology, 2021.
- [13] Microsoft, "Microsoft Update Catalog (KB4474419)," Microsoft Corporation , 2021. [Online]. Available: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4474419.
- [14] Microsoft Corporation, "Microsoft Update Catalog (KB976932)," Microsoft Corporation, 2021.[Online]. Available: https://www.catalog.update.microsoft.com/Search.aspx?q=KB976932.
- [15] Cigent Technology, "Cigent D3E Locking All Connected Drives," Cigent Technology, 19 April 2020. [Online]. Available: https://www.youtube.com/watch?v=SEJfuSZ7nFo.
- [16] S. Park and J. Lee, "Analysis of the K2 Scheduler for a Real-Time System with an SSD," 6 April 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/7/865/htm.
- [17] Microsoft Corporation, "Learn about Windows Hello and set it up," Microsoft Corp., 2021. [Online]. Available: https://support.microsoft.com/en-us/windows/learn-about-windows-helloand-set-it-up-dae28983-8242-bb2a-d3d1-87c9d265a5f0.

- [18] Google, "Get verification Codes with Google Authenticator," Google, 2021. [Online]. Available: https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=en.
- [19] Mulrey and Wolf, *Correspondence Dave Wolf and John Mulrey, 6 June 2021*, Nashua, NH, 2021.

Haec pagina vacua intentione restat³⁸.

³⁸ This page is intentionally blank.
Appendix A D3E Evaluation Details

Result summaries from the evaluation are contained in Section 3 of this report. Details have been moved to this appendix for ease of reading.

The D3E functional testing described below largely follows the outline provided in references [4] and [8].

D3E *Software Locking* mode was tested for each of the three laptop configurations. *Firmware Locking* and Secure Solid-State Drive (SSD) features, however, were evaluated only on the Cigent loaner Win10 machine and the loaner USB drive.

A.1 Cigent Firmware Locking Mode

The evaluation steps in this subsection were performed only on the Cigent Win10 laptop.

| Cigent D3E | | | | _ | | × |
|----------------------|---|---|--------------------------------------|----------------|----------|------|
| Ø | Standing Guard We are looking out for yo | d ur sensitive data | | | | |
| Dashboard | | | | | | |
| File Type Protection | | | ັດ | | | |
| Folder Protection | | Folder Protection | Secure Drives | | | |
| Secure Drives | Custom | 4 Always On folders 1 Dynamic folder | CTI SSD: 1 P: CTI SSD: 1 H: | | | |
| Q Networks | | | | | | |
| Nemovable Storage | ° _ | ~ | S (| | | |
| S Deception | | Removable Storage | Deception | | | |
| Ruthentication | Trusted | New (1) | 2 deception files | | | |
| Settings | | | | | | |
| License | | | | | | |
| C Update | | | | | | |
| i About | | | | | | |
| | | | Cigent D ³ E v2.4.4 © 202 | 21 Cigent Tech | nnology, | Inc. |

Figure A-1. V2.4.4 Dashboard Indicating that Secure Drives are Installed

The D3E Dashboard shown in Figure A-1 indicates that the computer has at least one secure SSD drive. Therefore, the steps in Sections A.1 and A.2 can be executed.

A.1.1 Configure Cigent Secure SSD Drives

In this evaluation step, we will configure the secure drive labeled E55907071F7900000081.

A.1.1.1 Review Current Secure Drive Configuration

Figure A-1 through Figure A-3 show that the Cigent laptop under evaluation has two physical drives. Note that each drive has a distinct serial number (S/N). Note also that each physical drive

has two partitions, L & P for the ...81 drive, and G & H³⁹ for the ...82 drive. Each partition is mounted as a separate drive in Windows. D3E protection was turned off temporarily, so that the *Always On* drives L & G could be seen in the dashboard and in Windows Explorer, as shown in Figure A-2 and Figure A-5.

Drives L & P represent the *Always On* and *Dynamic* drives (partitions), respectively, for the Cigent laptop's internal drive (E55907071F790000081), while G and H are the *Always On* and *Dynamic* partitions for the external USB drive attached to the Cigent laptop.

Figure A-3 shows that each physical drive has been allocated 447 GB. The 223 GB allocation for the *Dynamic* partition of the ...81 drive (Drive P in Figure A-4) indicates that equal space has been given to the *Always On* and *Dynamic* partitions. The same allocation applies to the ...82 external drive. The D3E administrator can change drive-space allocations, as will be shown in Section A.1.1.3 below.



Figure A-2. Two Physical Drives Installed



Figure A-3. Total Drive Space

³⁹ Labels for the external USB drives can change if the external drive is ejected and later reinstalled.

| ReadyBoost | Prev | ious Versions | Quota | Customia |
|--------------|-----------|-------------------|---------|--------------|
| General | Tools | Hardware | Sharing | Secur |
| ~ | CIGENT | DYNAMIC | | |
| Туре: | Local Dis | k | | |
| File system: | NTFS | | | |
| Used spa | ce: | 105,377,792 b | ytes | 100 MB |
| Free spac | e: | 239,867,527,168 b | ytes | 223 GB |
| Capacity: | | 239,972,904,960 b | ytes | 223 GB |
| | | O | | Disk Cleanur |

Figure A-4. Equal Allocations for Always On & Dynamic Partitions



Figure A-5. All Drives Visible in Windows Explorer

In the *Secure Drives* window, click on the *Always On* drives for the two physical drives to reactivate protection. Note that <u>it is not necessary</u> to enter a PIN or other authentication type to turn protection back on, though authentication <u>is required</u> when disabling protection.

Figure A-6 shows the results of turning on protection for the partitions. Protection has rendered the two *Always On* partitions, L & G, invisible both in the D3E Dashboard and in Windows Explorer. Had Dynamic partitions P & H been similarly protected (locked), they, too, would have become invisible in Windows. (This attribute applies only to secure SSDs.)

| Dashboard | Standing Guara We are looking out for your se | ensitive data | | Image: Application of the state of the |
|---|--|---|---|---|
| File Type Protection Folder Protection Secure Drives Nature 1 | File Type Protection | Colder Protection 4 Aways On folders 1 Dynamic folder | Secure Drives CTI SSD: P: CTI SSD: H: | Clipboard ← → ← ↑ → → This PC → Documents → > ≪ C on RCAT-JUMP > ≪ D on RCAT-JUMP > ← D exitop > ← D ocuments > ↓ D Documents > ↓ ↓ D Documents > ↓ ↓ D Documents |
| Pretworks | Networks nerve.mitre.org Trusted | Removable Storage New (1) | Contemption Section 2 deception files | |
| < | | , | | V V Network |

Figure A-6. Always On Partitions Not Visible

To demonstrate D3E's ability to reconfigure existing drives, it first was necessary to deconfigure a Secure Drive. The ...81 Secure Drive will be de-configured in Section A.1.1.2 below.

A.1.1.2 De-Configure a D3E Secure Drive

After making the Secure Drives visible, we copied their file contents to a Backup folder. (It was necessary to enter the authentication PIN each time a secure file was moved.) For the sake of convenience, if not security, a backup folder was located on the Cigent laptop. We also copied the Backup folder to the H: partition of the USB drive, because that drive was not being reconfigured. Note that this Backup folder contains only user-generated files, which we may want to use after the Secure Drive has been reconfigured.

Separate from our backup of user-generated data files, D3E generates a backup file (*.d3e) containing system configuration data for each Secure Drive. In our case, the files were located on the desktop, as shown in Figure A-7. The .d3e backup file will play a role in the de-configuration steps below.

| > 🥩 C on RCAT-JUMP | NEW BUILD_GUIDE FOR 2.4.4 | 4/19/2021 10:02 AM | File folder | |
|--------------------|---------------------------------|--------------------|---------------|------|
| > 🥪 D on RCAT-JUMP | E55907071F7900000081_backup.d3e | 8/1/2020 8:40 AM | D3E File | 1 KB |
| > Desktop | E55907071F790000082_backup.d3e | 8/1/2020 8:39 AM | D3E File | 1 KB |
| > 🖻 Documents | i readme.txt | 9/14/2020 2:30 PM | Text Document | 1 KB |

Figure A-7. System-Generated Backup File for Each Drive

- Deconfiguration Step 1:
 - Select the appropriate Secure Drive. For our evaluation, select the81 internal drive with partitions L & P.
 - Click the **Deconfigure** button to de-configure the internal Secure Drive of the Cigent laptop. Refer to Figure A-8.

| Cigent D3E | | 16 * | 10.206.161.214 _ 8" × | \$ 💥 4 | |
|--|--|-------------------|-----------------------|----------|----------------------|
| | Secure Drives Protect files with firmware locking, the highest left | vel of protection | | | |
| Dashboard File Type Protection | Name: <u>CTI SSD</u> S/N: ES5907071F7900000081 FW: ECFM1379 | [447 68] | | / | 🖻 P: |
| Folder Protection Secure Drives | Secure Drives | Dynamic (P:) | | Deconfig | gure Change Password |
| P ➡ Networks Removable Storage C Deception | Name: CTI SSD s/II: ESS907071F79000000082 FW: ECFM13T9 | [447 GB] | | | <mark>∂</mark> H: |

Figure A-8. Click Deconfigure for the Selected Drive

- Deconfiguration Step 2:
 - Browse to the desktop location of the desired .d3e backup file, as shown in Figure A-9.

| Cigent D3E | * Return to Secure Drives |) |
|----------------------|--|--------|
| | Deconfigure | |
| Dashboard | CTI SSD S/N: E55907071F790000081 | |
| File Type Protection | WAAUDIG: Deconfiguring will cause all data stored on your D'4 Secure Drives to be permanently erased. | |
| | Please ensure that you have backed up all data before proceeding. Once started, this process cannot be stopped. | |
| Folder Protection | O Backup File C:/Users/cigent/Desktop/E55907071F7900000081_backup.d3e | Browse |
| Secure Drives | Password Essaveration | - |
| Networks | Type the following line, exactly as shown, in the confirmation box to proceed: IUURESTAND THAT ALL DATA ON MY SECURE DRIVES WILL BE ERASED | _ |
| Removable Storage | LUNDERSTAND THAT ALL DATA ON MY SECURE DRIVES WILL BE EXISED | Save |
| of Deception | | |

Figure A-9. Enter Backup-File Location and Provision PW to Deconfigure Drive

- Enter the provisioning password for the Secure Drives.
- Type the prescribed line in the confirmation box to proceed.
 - Click **Save** to Configure, then execute the prescribed authentication step. (For this system, simply enter the PIN at the D3E prompt.)

A.1.1.3 Reconfigure the Secure Drive

After a successful de-configuration, a screen such as the one in Figure A-10 will be displayed. The internal Secure Drive can now be configured.

| Cigent D3E | 🖮 📶 10205151214 💷 🖉 🗙 | \$ 🗰 🖌 🏠 | () |
|----------------------|--|----------|------------------------------|
| | Secure Drives | | |
| Dashboard | Protect hies with himware locking, the highest level of protection | | |
| File Type Protection | Name: CTI SSD s/it: ESS9070715790000001 FW: ECM1319 [447 GB] | / | |
| Folder Protection | | | Configure |
| Secure Drives | | | Advanced |
| P. Networks | Name: CTI SSD s/ii: E559070717900000002 IW: ECIML3T9 [447 GB] | | 🖻 H: |
| 🔗 Removable Storage | | | |
| J Deception | | | |

Figure A-10. Configure the Secure Drive

- Configuration Step 1:
 - Click on the **Configure** Button shown in Figure A-10.
- Configuration Step 2:
 - Create/enter password for the Secure Drive d3e configuration file. Refer to Figure A-11.



Figure A-11. Enter D3E Secure Drive Password [8]

• When you click the checkbox to create a password backup file, a screen like the one in Figure A-12 will be displayed.

| Save Backup File | | | | | | | |
|--|--------------------------------|--------------------|-------------|------|------|------------------|-------|
| \rightarrow \checkmark \uparrow \blacksquare > This PC | > Desktop > | | | ~ | Ö | 🔎 Search Desktop | |
| rganize • New folder | | | | | | (EE | - (|
| A Na | ame | Date modified | Туре | Size | | | |
| | Backupfiles_20 April | 4/20/2021 3:55 PM | File folder | | | | |
| DneDrive | NEW BUILD_GUIDE FOR 2.4.4 | 4/19/2021 10:02 AM | File folder | | | | |
| This PC | E55907071F790000081_backup.d3e | 8/1/2020 8:40 AM | D3E File | | 1 KB | | |
| 3D Objects | E55907071F790000082_backup.d3e | 8/1/2020 8:39 AM | D3E File | | 1 KB | | |
| A on RCAT-JUMF | Backupfiles_21 April | 4/21/2021 10:06 AM | File folder | | | | |
| C on RCAT-JUMF | | | | | | | |
| D on RCAT-JUMF | | | | | | | |
| E Desktop | | | | | | | |
| Documents 🗸 | | | | | | | |
| File name: E55907071 | F790000081_backup.d3e | | | | | | |
| Save as type: *.d3e | | | | | | | |
| | | | | | | | |
| Hide Folders | | | | | | Open C | ancel |

Figure A-12. Select Location for Secure Drive Password Backup

• After selecting the backup-file location for the Secure Drive password, click the **Save** button shown in Figure A-11.

- Configuration Step 3:
 - The screen in Figure A-13 will be displayed.

| 🎸 Cigent D3E | | - [| X C |
|----------------------|--|---|-------------------------------|
| | Return to Secure Drives | | |
| | Configure | | |
| Dashboard | CTI SSD S/N: E55907071F7900000081 | | |
| File Type Protection | Enter and save your D ³ E Secure | Drive password. | |
| Folder Protection | Password | Password Requirement At least one number [0-9] At least one symbol [1@#\$%^1 | s: &*] |
| Secure Drives | | At least one lower case letter [2 At least one upper case letter [Password length must be 8 to 3 | a-z] A-Z] 12 characters |
| Networks | ✓ I have saved my password in a safe place. | | |
| Removable Storage | Show Advanced Options | | Save |
| 3 Deception | | | |

Figure A-13. Select Both Checkboxes

• Select both checkboxes and click on the **Save** button. D3E displays a notification of the *KeepAlive* security feature. *KeepAlive* protects data if a malware event occurs; the feature is discussed further in Section A.2.3.



Figure A-14. KeepAlive Feature

- Enter the appropriate authentication (PIN) at the prompt.
- The post-configuration screen is displayed in Figure A-15.



Figure A-15. Post-Configuration L & P Secure Drives

- Configuration Step 4:
 - Allocate Drive Space
 - i. Because we intentionally did not erase database files from the C:\users\public\cigent directory, pre-existing configuration data, including drive-space allocations, were carried over from the previous configuration. Consequently, D3E did not prompt us to allocate space for the *Dynamic* and *Always On* partitions. Had we been prompted, a screen like the one in Figure A-16 would have been displayed. To change allocations, simply adjust the *Dynamic/Always On* slider.

| Cigent D3E | | |
|----------------------|---|--|
| - | Return to Secure Drives | |
| | Configure | |
| Dashboard | PCIe SSD S/N: 288E07080B5300002941 | |
| Ele Turne Protection | Enter and save your D ³ E See | cure Drive password. |
| File Type Protection | Password Password | Password Requirements: |
| Folder Protection | Confirm Password Password | At least one number [0-9] At least one symbol [1@#\$%^&*] |
| Secure Drives | □ Click the checkbox to create a backup of you password before continuing (required). | At least one lower case letter [A-2] r Password length must be 8 to 32 characters |
| Networks | ⊗ Hide Advanced Options | Save |
| 🔗 Removable Storage | Adjust the Dynamic/Always Total Size: | On drive proportions 894 GB |
| J Deception | Dynamic Size 447.0 GB | Always On Size 447.0 GB |
| | Enable KeepAlive Feature | |
| Authentication | | |
| Settings | | |
| License | | |
| C Update | | |
| i About | | |
| | Cigent | t D ³ E v2.0.9 © 2020 Cigent Technology, Inc. |

Figure A-16. Allocate Dynamic & Always On Drive Space [8]

A.1.1.4 Enable the Mini Authentication Popup

• At the *Settings* Menu of the D3E Dashboard, toggle the slider and enter the appropriate authentication (PIN) to enable the *Use Mini Authentication Popup* feature. See Figure A-17.

A.1.1.5 Enable Always On File Type Protection

• At the *Settings* Menu of the D3E Dashboard, toggle the slider and enter the appropriate authentication (PIN) to enable *Allow Always on File Type Protection*. See Figure A-17.



Figure A-17. Toggle D3E Settings

A.1.1.6 Feature Evaluation Results

- The configuration of the Cigent Secure Drive was accomplished according to plan. There were no problems or issues. When a password was created, however, as part of the Secure Drive Configuration (in Section A.1.1.3 above), D3E permitted reuse of the old provisioning PW. This was convenient for the purpose of our evaluation, but Air Force password guidance recommends stricter practices.
 - **Recommendation**: We recommend that Cigent use NIST SP 800-63-3 as a guide for constructing robust digital identities.

A.1.2 Always On and Dynamic Protection

- Preliminary Steps: Make sure that the recently configured L & P drives contain data files. If the drives are empty, they can be populated with data from the Evaluation Kit that accompanied the D3E build, or from the G & H drives that were not reconfigured. Figure A-18 shows the contents of the *EvaluationKitAuxFiles* folder, while Figure A-19 shows the L & P drives with the extracted data.
 - Extract *CompanyInternal.zip* files to the P drive.
 - Extract *HighlyConfidential.zip* files to the L drive.

| This PC | ^ | Name | Type | Compressed size | Password prot | Size | | Ratio |
|-------------------|---|------------------------------|----------------------------|-----------------|---------------|------|-----------|-------|
| 3D Objects | | CompanyInternal.zip | Compressed (zipped) Folder | 1,306 KB | No | | 1,306 KB | 0% |
| A on RCAT-JUMP | | 1 HighlyConfidential.zip | Compressed (zipped) Folder | 16,149 KB | No | | 16,149 KB | 0% |
| C on RCAT-JUMP | | network_recon_local_only.zip | Compressed (zipped) Folder | 1,289 KB | No | | 1,289 KB | 0% |
| S D on RCAT-JUMP | | | | | | | | |
| Desktop | | | | | | | | |
| 🗎 Documents | | | | | | | | |
| 🐥 Downloads | | | | | | | | |
| Music | | | | | | | | |
| E Pictures | | | | | | | | |
| 📕 Videos | | | | | | | | |
| 👟 Local Disk (C:) | | | | | | | | |

Figure A-18. Extract Zipped Test Data to L & P Drives

| • _ | | ^ | | | |
|---|---|--|---|---|---|
| A on RCAT-JUMP | ^ | Name | Date modified | Type | Size |
| 🔮 C on RCAT-JUMP | | cr2e047.pdf | 3/18/2019 12:59 PM | PDF File | 560 KB |
| 🔮 D on RCAT-JUMP | | 📴 Form 2464 - Annual Franchisor Cert.pdf | 3/18/2019 12:59 PM | PDF File | 217 KB |
| Desktop | | InternalMemos.txt | 8/6/2019 3:51 PM | Text Document | 1 KB |
| Documents | | Ransomware_Trifold_e-version.pdf | 8/6/2019 3:41 PM | PDF File | 803 KB |
| 🕹 Downloads | | | | | |
| Music | | | | | |
| E Pictures | | | | | |
| 📕 Videos | | | | | |
| Local Disk (C:) | | | | | |
| CIGENT DYNAMIC (H:) | | | | | |
| | | | | | |
| CIGENT ALWAYS ON (L:) | | | | | |
| CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P:) | | | | v ð ♀ Searc | :h CIGENT AL |
| CIGENT ALWAYS ON (L) CIGENT DYNAMIC (P;) ✓ | ^ | Name | Date modified | ✓ Ŏ Time | th CIGENT AL |
| CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P;) → | ^ | Name | Date modified | ✓ ð | th CIGENT AL |
| CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P;) ✓ ↑ → This PC > CIGENT ALWAYS ON (L:) ✓ C on RCAT-JUMP ✓ C on RCAT-JUMP ✓ D on RCAT-JUMP | | Name ^ | Date modified 8/6/2019 3:52 PM | V & Searce Type Office Open XML | ch CIGENT ALL Size 385 K |
| CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P;) A on RCAT-JUMP C on RCAT-JUMP C on RCAT-JUMP Deckno | | Name ^ Annual Report - draft - confidential.docx billing.xix Confidential.bt | Date modified 8/6/2019 3:52 PM 8/6/2019 3:51 PM | ✓ Ŏ P Searce Type Office Open XML XLSX File Text Document | Size 385 K 15 K |
| CIGENT ALWAYS ON (L:) CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P;) A on RCAT-JUMP C on RCAT-JUMP C on RCAT-JUMP D on RCAT-JUMP D on RCAT-JUMP Doments | | Name ^ Annual Report - draft - confidential.docx billing.xtsx Confidential.xtx Confidential.xtx | Date modified 8/6/2019 3:52 PM 8/6/2019 3:51 PM 8/6/2019 3:51 PM 8/23/2018 10:33 PM | V 0 P Searc Type Office Open XML XLSX File Text Document PDF File | ch CIGENT ALI Size 385 K 15 K 1 K 7.317 K |
| CIGENT ALWAYS ON (L) ⊂ CIGENT DYNAMIC (P;) ⇒ → ↑ → This PC → CIGENT ALWAYS ON (L) S ^A A on RCAT-JUMP S ^C C on RCAT-JUMP S ^C D on RCAT-JUMP Desktop Bootenets Desktop | Î | Name Annusl Report - draft - confidential.docx billing.xtx Confidential.bt Confidential.bt Confidential.bt | Date modified 8/6/2019 3:52 PM 8/6/2019 3:51 PM 8/6/2019 3:51 PM 8/23/2018 10:33 PM 3/18/2019 1:55 PM | V O P Searc Type Office Open XML XLSX File Text Document PDF File PDF File | ch CIGENT ALI Size 385 K 15 K 1 K 7,317 K 124 K |
| CIGENT ALWAYS ON (L:) ⊂ CIGENT DYNAMIC (P;) ⇒ ~ ↑ → This PC > CIGENT ALWAYS ON (L:) ⇒ A ~ ↑ → This PC > CIGENT ALWAYS ON (L:) ⇒ C on RCAT-JUMP ⇒ D on RCAT-JUMP ⇒ Documents ↓ Documents ↓ Downloads | | Name Annual Report - draft - confidential.docx billing.xlsx Confidential.txt corporate_info.pdf comfort_pdf comfort_pdf | Date modified 8/6/2019 3:52 PM 8/6/2019 3:51 PM 8/6/2019 3:51 PM 8/23/2018 10:33 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM | ✓ O Type Office Open XML XLSX File Text Document PDF File PDF File | ch CIGENT ALV Size 385 K 15 K 1 K 7,317 K 124 K 128 K |
| CIGENT ALWAYS ON (L) ⊂ CIGENT DYNAMIC (P;) ⇒ · · ↑ · → This PC > CIGENT ALWAYS ON (L) ** A on RCAT-JUMP ** C on RCAT-JUMP ** C on RCAT-JUMP © Desktop © Desktop © Documents ↓ Downloads >* Music | Î | Name ^ Annual Report - draft - confidential.docx billing.xtsx Confidential.txt corporate_info.pdf confidential.txt corporate_info.pdf confidential.txt corporate_info.pdf confidential.txt confidential.txt corporate_info.pdf confidential.txt confidentia | Date modified 8/6/2019 3:53 PM 8/6/2019 3:51 PM 8/23/2018 1:033 PM 3/18/2019 1:259 PM 3/18/2019 1:259 PM 3/18/2019 1:259 PM | V Ö P Searc Type Office Open XML XLSX File Test Document PDF File PDF File PDF File PDF File | ch CIGENT ALD Size 385 K 15 K 7,317 K 124 K 128 K 148 K |
| CIGENT ALWAYS ON (L:) CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P;) A on RCAT-JUMP C on RCAT-JUMP C on RCAT-JUMP O osktop Downents Ownents Ownents | Î | Name ^ Annual Report - draft - confidential.docx billing.xix corporate_info.pdf corporate_info.pdf corporate_info.pdf corporate_info.pdf corporate_info.pdf corporate_info.pdf corporate_info.pdf corporate_info.pdf corporate_info.pdf | Date modified 8/6/2019 3:52 PM 8/6/2019 3:53 PM 8/23/2018 10:33 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM 8/6/2019 3:89 PM | Image: Constraint of the second sec | ch CIGENT AL Size 385 K 15 K 7,317 K 128 K 128 K 148 K 148 K |
| CIGENT ALWAYS ON (L) ⊂ CIGENT DYNAMIC (P;) → → ↑ → This PC → CIGENT ALWAYS ON (L) ☆ A on RCAT-JUMP ☆ C on RCAT-JUMP ☆ D on RCAT-JUMP @ Doesktop @ Documents ↓ Downloads ↓ Music ₩ Pictures ₩ Videos | Î | Name Annusl Report - draft - confidential.docx biling.xtx Confidential.bxt conste.info.pdf why.pdf fw9.pdf m Ansomware Prevention and Resp.pdf fansomware_Executive_One-Page.pdf | Date modified 8/6/2019 3:52 PM 8/6/2019 3:51 PM 8/6/2019 3:51 PM 8/3/2018 10:33 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM 8/6/2019 3:50 PM | ♥ 0 P Searc Type Office Open XML XLSX File Text Document PDF File PDF File PDF File PDF File PDF File | ch CIGENT AL ¹ Size 385 K 15 K 7,317 K 124 K 124 K 128 K 148 K 148 K 154 K |
| CIGENT ALWAYS ON (L:) CIGENT ALWAYS ON (L:) CIGENT DYNAMIC (P;) → · | | Name Annual Report - draft - confidential.docx billing.xlcx Confidential.txt corporate_info.pdf w0.pdf w0.pdf consortial experiments and Resp.pdf consortial and Resp.pdf | Date modified 8/6/2019 3:52 PM 8/6/2019 3:51 PM 8/3/2018 10:33 PM 8/3/2019 12:59 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM 8/6/2019 3:39 PM 8/6/2019 3:50 PM 8/6/2019 3:46 PM | ♥ ♥ Search Type Office Open XML XLSX File Text Document POF File PDF File PDF File PDF File PDF File PDF File PDF File PDF File PDF File PDF File PDF File | 5 CIGENT AL Size 385 K 15 K 7,317 K 124 K 128 K 128 K 148 K 154 K 783 K 9,342 K |

Figure A-19. Contents of P & L Drives with Extracted Data

A.1.2.1 Accessing Always On Files

- Recap of *Always On* Behavior:
 - As we described in Section 2.1 of this paper, files on *Always On* drives remain locked under all conditions, until they are made accessible when a D3E administrator enters the prescribed authentication to unlock the drive temporarily.
 - In other words, step-up authentication is always required to access *Always On* files.
 - Locked Always On Secure Drives are not visible in Windows Explorer.
 - If a threat is detected while an *Always On* drive is temporarily unlocked, D3E unmounts (locks) the drive.

• Browse to L:\HighlyConfidential in Windows Explorer. If the drive and file are not visible, simply click on the green portion of the Secure Drive icon in the D3E Dashboard and use the prescribed authentication method. Figure A-20 shows the locked and unlocked states of the *Always On* drive.

| Cigent D3E | 10206-161214 - 🔮 × 🗖 - X | Cipert Dit | |
|--|---|--|---|
| Dashboard | Secure Drives Protect files with firmware locking, the highest level of protection | Dashboard | Secure Drives Protect files with firmware locking, the highest level of protection |
| File Type Protection | Name: <u>CTI SSD</u> P: | File Type Protection | Name: <u>CTI SSD</u> ▲ CTI <u>SSD</u> → CTI <u>SSD</u> ▲ CTI <u>SSD</u> → |
| Folder Protection Secure Drives | Secure Drives Secure Drives Drynamc (Pr) Deconfigure Change Passaord Advanced | Folder Protection Secure Drives | Secure Drives Aways to (L.) Dynamic (P.) Deconfigure Change Password Advanced |
| ♀ Networks ♦ Removable Storage ♀ Deception | Name: CTI SSD | Networks Removable Storage Deception | Name: CTI SSD s/π: ESS9027072179000000002199: ECHLI3T9 [447 68] |

Figure A-20. Always On Drive Before and After Unlocking

• Once the Secure Drive has been unlocked, file names will be visible in Windows Explorer. Click on the *Confidential* text file. Regardless of the *ActiveLock* status, the file will appear empty until the appropriate authentication is entered. See Figure A-21.

| Detted-Hongai Pair Reporting 0 | |
|---|--|
| | Hyphyconderdat-Nampat - D X No tat found Yee Hug Buth Phopole of the hultad States, in Order to fore a more perfect Union, establish Justice, insure deset - provide for the common defects, promote the general Maifere, and accure the Elessings of Liberty to corsolv do ordain and establish this Constitution for the United States of America. |
| Che Annue C | e e Lol Cert 5 100% Weedeer (DRJ) UT-4 |
| Pre PIN | Post PIN |
| | |

Figure A-21. Files in Always On Drive Require PIN to Unlock

• The triggering of ActiveLock to secure the *Always On* drive when a threat is detected is demonstrated and evaluated in Section A.1.3.1 below.

A.1.2.2 Accessing Dynamic Files

- Recap of *Dynamic* Behavior:
 - *Dynamic* data normally are unlocked and accessible; however, if a filetype, folder, or partition is marked for *Dynamic* protection, the *Dynamic* locking mode will activate and lock these entities whenever D3E determines that a threat has been encountered. Step-up authentication then will be required to access the information.
 - o Locked Dynamic Secure Drives are not visible in Windows Explorer.
- Refer to Section 2.1 for further details.

• Browse to P:*cr2e047.pdf* in Windows Explorer. Because the file is on a drive with *Dynamic* protection, second-factor authentication (PIN) will not be required to open it, unless *ActiveLock* has been triggered by a security event. See Figure A-22.



Figure A-22. Dynamic Files Open Without MFA

• The triggering of ActiveLock to secure the *Dynamic* files when a threat is detected is demonstrated and evaluated in Section A.1.3.1 below.

A.1.2.3 Feature Evaluation Results

There were no issues accessing or manipulating *Dynamic* and *Always On* files on the Cigent Secure Drive. The feature performed as advertised.

A.1.3 Deception Files

As noted earlier, *Deception* files track unauthorized access attempts to the host system by enticing prospective attackers with interesting file names and folders. D3E creates a default *passwords.xls Deception* file in local users' **Documents** directories, and D3E users can create other *Deception* files in locations of their choice. Attempts to open *Deception* files trigger *ActiveLock*.

The test cases below demonstrate D3E's response to attempts to access the default and usercreated honeypot files.

A.1.3.1 Attempt to Access the Default passwords.xls Deception File

• In Windows Explorer, browse to the location of the *passwords.xls* default *Deception* file (C:\Users\cigent\Documents).

| 👔 🖓 📴 🖛 Documents | lin ++ | 10.206.161.214 | _ 8 × |
|--|---------------|--------------------|-------------|
| File Home Share View | | | |
| ← → → ↑ 🗎 → This PC → Local Disk (C:) → Users → cigent → Documents | • | | |
| > 🕹 Downloads | Name | Date modified | Type Size |
| > 🎝 Music | supersecret | 9/16/2020 11:51 AM | File folder |
| > E Pictures | which_setting | 9/28/2020 2:32 PM | File folder |
| > 📕 Videos | passwords.xls | 8/1/2020 8:34 AM | XLS File |
| V Local Disk (C:) | | | |
| AlwaysOn | | | |
| > Backup | | | |
| Dynamic | | | |
| > 🦲 Intel | | | |
| PerfLogs | | | |
| > Program Files | | | |
| > Program Files (x86) | | | |
| Share | | | |
| 🗸 🗸 🔄 Users | | | |
| ✓ cigent | | | |
| 3D Objects | | | |
| I Contacts | | | |
| Desktop | | | |
| > 😥 Documents | | | |
| 🕹 Downloads | | | |

Figure A-23. Locate the passwords.xls Deception File

- Double-click on the *passwords.xls* file. Note the following results:
 - o A Windows pop-up message informs you that you cannot access the file.
 - The D3E Dashboard displays a *Threats Detected* notification.
 - The Cigent task-tray icon turns red.



Figure A-24. D3E Threat Notifications

• The D3E Dashboard indicates that a *Deception* event has occurred. See Figure A-25.



Figure A-25. Deception Threat Detected

• The Secure Drives have been locked as a result of the *Data-Deception* attempt.

| Cigent D3E | | | х |
|----------------------|---|----------|---------|
| ļ | Secure Drives Protect files with firmware locking, the highest level of protection | | |
| Dashboard | CTI SSD | | 6 |
| File Type Protection | S/N: E55907071F7900000081 | | _ |
| Solder Protection | CTI SSD S/N: E55907071F7900000082 | | Ô |
| Secure Drives | | | |
| Networks | | | |
| Ruthentication | | | |
| 9 Deception | | | |
| Settings | | | |
| License | | | |
| C Update | | | |
| 1 About | | | |
| ActiveLock Engaged | Cigent D ³ E v1.6.10 © 2020 Cigent Te | chnology | /, Inc. |

Figure A-26. Secure Drives Locked upon Deception Event

• Finally, note that the Secure Drives (G, H, L & P) are no longer visible in Windows Explorer.



Figure A-27. Secure Drives Invisible in Windows Explorer

- Click on **Dashboard**. Then click on the *Clear Threat* button and enter the prescribed authentication method to clear the Cigent warnings and return to normal operation.
 - After the threat has been cleared, note that the *Always On* partitions remain locked (and invisible in Windows Explorer), while the *Dynamic* partitions are visible and unlocked.

A.1.3.2 Attempt to Access User-Created Deception File

- To conduct this evaluation, we created a *Documents Company Confidential* folder, because we want the *Deception* file to reside here. (This choice is arbitrary and at the administrator's discretion.)
- Click *Add a Deception File* at the D3E Dashboard *Deception* menu.
 - Browse to the folder where you will create the *Deception* file, and thin click **Open**.
 - If you don't wish to use the default *passwords.xls* file name, simply enter the name of a non-existing file (we chose *Ooh lala.txt*), click *Save*, and implement the prescribed authentication method at the prompt. See Figure A-28.



Figure A-28. Add a *Deception* File

- In Windows Explorer, browse to the location of the user-created *Deception* file; then click on the file to access it.
- Note that warnings similar to those shown in Figure A-24 are displayed, and that the D3E Dashboard displays the notification shown in Figure A-25.
- Click on *Clear Threat* and use the prescribed authentication method to clear the Cigent warnings.

A.1.3.3 Evaluation Results

Our evaluation demonstrated that D3E File *Deception* behaved as advertised, triggering *ActiveLock* whenever an attempt was made to access a *Deception* file.

We did, however, note the following anomalous behavior:

- Although attempts to open user-created *Deception* files triggered the appropriate responses, it was possible to delete those files from within Windows Explorer. The files also could be moved to another location and subsequently opened/edited.
 - While the *Deception* file is merely a honeypot, and the ability to delete, copy/move, or open it with impunity will not immediately harm the host, such behavior provides an attacker with a means of analyzing and eventually circumventing D3E defenses.
- Moreover, while it was not possible to permanently delete the system-generated *passwords.xls* file, that file could similarly be moved and subsequently opened/examined. See Figure A-29 below. Note that the system-generated *Deception* file has been moved from the *Documents* folder to the desktop prior to opening.

| 👔 🔜 🛃 📕 🖛 Desktop | | | | | | - 🗆 🗙 |
|--|---------------------------------|--------------|----------------------|---|----------------|---------------|
| File Home Share View | | | | | | ~ 🕜 |
| Pin to Quick Copy access Copy Paste Paste shor | tcut Move Copy to Delete Rename | New item • | Properties | Select all Select none | | |
| Clipboard | Organize | New | Open | Select | | |
| $\leftarrow \rightarrow \neg \uparrow \blacksquare$ > This PC > Desk | top | | | | v ŭ ,> s | earch Desktop |
| Quick access | | ^ Name | ^ | Date modified | Туре | Size |
| • On - Drive | | Backupfiles_ | 20 April | 4/20/2021 3:55 PM | File folder | |
| OneDrive | | Backupfiles_ | 21 April | 4/21/2021 10:08 AN | File folder | |
| 💻 This PC | | E55907071E7 | 900000081 backup d3e | 4/19/2021 10:02 AIV 8/1/2020 8-40 ΔΜ | D3F File | 1 KB |
| 3D Objects | | E55907071F7 | 900000082 backup.d3e | 8/1/2020 8:39 AM | D3E File | 1 KB |
| A on RCAT-JUMP | | ooh lala.txt | | 4/22/2021 1:31 PM | Text Document | 1 KB |
| 🛫 C on RCAT-JUMP | | readme.txt | | 9/14/2020 2:30 PM | Text Document | 1 KB |
| 🛫 D on RCAT-JUMP | | passwords.xl | ls | 4/22/2021 1:29 PM | XLS File | 1 KB |
| Cesktop | Descriver de vie - Notenad | | | | | - n x |
| Documents | File Edit Format View Help | | | | | |
| 🕹 Downloads | The care rounde new risp | | | | | ^ |
| Music | 1 | | | | | |
| E Pictures | | | | | | |
| 🙀 Videos | | | | | | |
| 🏪 Local Disk (C:) | | | | | | |
| CIGENT DYNAMIC (H:) | | | | | | |
| CIGENT DYNAMIC (P:) | | | | | | |
| CIGENT DYNAMIC (H:) | < | | | | | > |
| international In | | | Ln 1, | Col 1 100% | Windows (CRLF) | UTF-8 |
| DESKTOR-0000964 | | | | | | |

Figure A-29. Successful Attempt to Move and Inspect Deception File

• D3E also allowed us to modify the system-generated *passwords.xls* file and replace the default file. Figure A-30 shows the contents of the *passwords.xls* file after moving the file to the desktop, editing the file, and copying it back into the original folder.

| | | r r | 1 👗 Cut | | | |
|--------------------|-------------|----------|----------------|-------|----------|------|
| passwords.xls - | Notepad | | | - 🗆 | \times | |
| File Edit Format | View Help | | | | | ken: |
| New stuff | | | | | ^ | |
| | | | | | | nt |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | \sim | |
| < | | | | | > | |
| | Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8 | | |
| CTI W SSD_20210 | INZIP | supersec | ret | | | |

Figure A-30. Modified *Deception* File in Honeypot Location

A.1.4 Windows Defender and Antivirus Integration

D3E works with Windows Defender antivirus (AV) and other AV solutions registered with Windows Security Center; D3E will lock files if Defender detects a threat or if the AV software has been disabled [8].

The subsections below evaluate D3E's integration with Windows' AV protection.

A.1.4.1 Evaluation Steps for Antivirus Integration

• At the D3E Dashboard Settings screen, make sure that *Trigger Active Lock if your Antivirus becomes disabled* is turned on. If it is not enabled, push the slider to the right and enter the appropriate authentication. (See Figure A-31.)



Figure A-31. Setting to Trigger ActiveLock for AV Tampering

- In the Windows start menu, search for Virus & threat protection.
 - Click on Windows Security.
 - Then click on *Virus & threat protection*. (See Figure A-32.)
 - o Click Manage settings. (See Figure A-33.)

| Best match | | |
|--|---|---------------------------|
| Virus & threat protection System settings | | • |
| Settings | | Virus & threat protection |
| r Check security status | > | System settings |
| Windows Security | > | |
| Search the web | | 📑 Open |
| ✓ virus - See web results | > | |
| | | |
| | | |

Figure A-32. Disable AV – Step 1



Figure A-33. Disable AV – Step 2

• Turn off *Real-time protection* by pushing the slider to the left. Then click **Yes** to put the action into effect. (See Figure A-34.)



Figure A-34. Disable AV – Step 3

• D3E detects the threat and engages *ActiveLock* (Figure A-35). Note that *Dynamic* drives P & H are visible, but locked, in the D3E Dashboard. *Always On* drives G and L are not visible in the Dashboard or in Windows Explorer. (Refer to Figure A-36.)



Figure A-35. Tampering with AV Triggers ActiveLock



Figure A-36. ActiveLock → Always On Drives Not Visible in Explorer

- Although *Dynamic* drives P & H are visible under *ActiveLock*, files on those drives require PIN authentication to access.
- Repeat earlier steps to manage *Windows Security* settings.
 - Turn *Real-time protection* back on.
 - The *ActiveLock* condition should clear.⁴⁰
- After *ActiveLock* has been cleared, *Always On* drives L & G can be unlocked and made visible in the usual way:
 - Click on *Secure Drives*.
 - Select either Secure Drive.
 - Toggle the slider from the locked (Green) position and enter the appropriate authentication.

A.1.4.2 Evaluation Results

D3E performed as expected, triggering *ActiveLock* when Windows Defender was turned off. We also noted that D3E properly detected out-of-date virus definitions.

• After we ran the evaluation steps in Section A.1.4.1 and re-activated *Real-time protection* at the host laptop, D3E persisted in detecting an antivirus-disabled threat, even though

⁴⁰ As we discovered, D3E will indicate a threat condition if virus protection definitions are not up to date.

virus and threat-protection settings had been returned to normal. (Refer to **Error! Reference source not found.**.) At first we thought that this was an error, so we notified Cigent about the issue. Cigent's response: "D3E uses the Windows Security Center APIs to determine the state and health of the properly registered Anti-Virus applications. In addition to state (enabled/disabled), the APIs will indicate a threat state if the virus definitions are out of date by more than a week (typically)." It turned out that Cigent's suspicion was, in fact, correct. Refer to **Error! Reference source not found.**, which shows that virus protection definitions at the Win10 laptop were out of date.



Figure A-37. D3E Indicates Virus Protection Disabled



Figure A-38. Protection Definitions are Out of Date

A.1.5 Network Manager

Network Manager is designed to prevent unauthorized devices from connecting to the D3E-protected host.

As we stated in Section 2.1.3.2, the D3E *Network Manager* starts fake services on commonly attacked ports <u>if they are not already in use</u>. If a network device scans a D3E-protected host for open ports and connects to a Cigent *Deception* port, D3E will trigger *ActiveLock* to protect sensitive files. *ActiveLock* also is triggered if an unauthorized device tries to connect to the system on any port, or if the system joins a network that has not been previously trusted.

The following two subsections describe the steps we performed to evaluate D3E *Network Manager* functionality.

A.1.5.1 D3E Response to Untrusted Network Connections

- Untrust the Current Network
 - Untrusting an existing network connection will have the same effect as trying to connect the D3E-protected host to an untrusted network.
 - Select *Networks* at the D3 Dashboard.
 - Click on a trusted network.
 - Click the Untrust button. Refer to Figure A-39.



Figure A-39. Untrust an Existing Trusted Network Connection

Clicking Untrust triggers ActiveLock. See Error! Reference source not found..



Figure A-40. Untrusting a Network Triggers ActiveLock [8]

• Show that files with *Dynamic* protection cannot be opened under *ActiveLock* condition.

(*ActiveLock*'s attributes have been demonstrated elsewhere in this report; however, for the sake of completeness, we'll show how D3E protects data after detection of an untrusted-network connection.)

• Try to open a file that has been assigned *Dynamic* protection. Refer to Figure A-41 below.

| to Quick Copy Paste Resternation Paste shortcut | Move Copy Delete Rename to to to | New folder | Properties | Belect none | | | | |
|---|-------------------------------------|---------------|------------|-------------|-----------------|-----|--------------|-----------------|
| Clipboard | Organize | New | Open | Select | | | | |
| - → × ↑ 📜 > This PC > Docun | nents > Company Confidential | | | | ~ | υ | , P Search C | ompany Confiden |
| | | ^ Name | ^ | D | ate modified | Typ | pe | Size |
| OneDrive This PC 3 D Objects Desktop Documents Downloads Music Pictures Videos Local Disk (C.) | | | iala.txt | 4, | 22/2021 1:31 PM | Tex | xt Document | 1 KB |

Figure A-41. Try to Open File with *Dynamic* Protection

• Figure A-42 shows that *ActiveLock* prevents the opening of the file unless the prescribed authentication is used.



Figure A-42. ActiveLock Prevents Opening of File with Dynamic Protection

• Clicking **Untrust** also causes the network connection to drop. Refer to Figure A-43.



Figure A-43. Untrusted Connection is Lost

• To clear the *ActiveLock* condition and restore the network connection, return to the *Networks* page at the D3E Dashboard and click **Trust** for the network you previously untrusted. Refer to Figure A-44.



Figure A-44. Return the Network to a Trusted Condition [8]

A.1.5.2 D3E Response to Port-Scanning Attempts

- Scan Network Ports
 - To perform the network-scanning evaluation, we used a port-scanning program provided by Cigent. That file is included on the laptop, as described below and depicted in Figure A-45.
 - The desktop of the evaluation laptop contains a folder called **NEW BUILD_GUIDE FOR 2.4.4.** Open the folder.
 - Next, open the folder called 16 April Cigent Stuff for hard drive and laptops.
 - Open the **EvaluationKitAuxFiles** folder, which contains the *EvaluationKitAuxFiles* zipped file.

 Clicking on the *EvaluationKitAuxFiles.zip* zipped file reveals the network_recon_local_only.zip file, which we will use to scan network ports.

| Organize * Include in library * Share with * New folder Image: Comparize * Include in library * Share with * New folder Name * Date modified Type Size Image: Comparize * Include in library * Share with * New folder Image: Comparize * Include in library * Share with * New folder Image: Comparize * Include in library * Share with * New folder Image: Comparize * Include in library * Share with * New folder Image: Comparize * Include in library * Share with * New folder Image: * Include in library * Share with * New folder Image: * Include in library * Share with * New folder Image: * Include in library * Share with * New folder Image: * Include in library * Share with * New folder Image: * Include in library * Share with * New folder Image: * Include in library * Share with * New folder Image: * | NEW BUILD_GUIDE FOR 2.4.4 + | | | | • 😰 Search N 💋 |
|---|--|--|--|----------------------------------|---------------------------------------|
| Parorites Date modified Type Size | Organize 👻 Include in library 👻 Share with 👻 New | w folder | | | i · · 🗈 🔞 |
| Desktop Develoads Develoads Is 16 April Cigent Stuff for hard drive and la 4/19/2021 10:03 AM PIF File folder Becent Places Is 6 April Cigent Stuff for hard drive and laptops Is 6 April | ☆ Favorites | Name * | Date modified | Type 5 | Size |
| iii Courreladds iii 6 April Cigent Stuff for hard drive and laptops e 06b102aaf/2d3e66cd99219c_Cigent_D3 4/16/2021 10:50 AM PDF Fie 8,555 KB iii 6 April Cigent Stuff for hard drive and laptops iiii 6 April Cigent Stuff for hard drive and laptops e 06b102aaf/2d3e66cd99219c_Cigent_D3 4/16/2021 10:50 AM PDF Fie 8,555 KB iii 6 April Cigent Stuff for hard drive and laptops iiiiiiiiiiiiiiiiiiiiiiiiiiiii | Nesktop |) 16 April Cigent Stuff for hard drive and la. | 4/19/2021 10:03 AM | File folder | |
| | Downloads | 606b102aaf2d3e68cd99219c_Cigent_D3. | 4/16/2021 10:50 AM | PDF File | 8,555 KB |
| Compressed (zpped) Folder C | Organize Include in library Share with New BuiltD_GUIDE FOR 2.4.4 16 April Organize Include in library Share with New Yevorites Desktop | Cigent Stuff for hard drive and laptops - w folder Name ^ Setup Guide 2.0.x for version 2.4.4 code | Date modified 4/19/2021 10:03 AM | Type : | • • • • • • • • • • • • • • • • • • • |
| | Downloads 10 Recent Places | 🎉 v2.4.4 software 🚹 EvaluationKitAuxFiles (3) | 4/19/2021 10:03 AM 4/16/2021 11:42 AM | File folder Compressed (zippe | 18,743 KB |
| Image: Search E Image: Search E Organize • Extract all Files Image: Search E Image: Search E Image: Search E Imag | EvaluationKitAuxFiles (3) | | | | _ 🗆 × |
| Organize ▼ Extract all files Image: Compressed size Password p Size ■ Desktop ■ Downloads ■ Recent Places ■ Manue ^ Type Compressed (siped) Folder 1,306 KB No No | G C + NEW BUILD_GUIDE FOR 2.4.4 + 16 Apri | Cigent Stuff for hard drive and laptops + Evaluation | KitAuxFiles (3) | | 🝷 🎦 Search E 💋 |
| Image: Second | Organize 👻 Extract all files | | | | 8= • 📑 🔞 |
| Desktop CompanyInternal Compressed (zipped) Folder 1,306 KB No Downloads HighlyConfidential Compressed (zipped) Folder 16,149 KB No Pacent Places Intervert_recon_local_only Compressed (zipped) Folder 1,289 KB No | - 🔶 Favorites | Name ^ T | /pe | Compressed size | Password p Size |
| Downloads Image: HighlyConfidential Compressed (zipped) Folder 16,119 KB No Sign Recent Places Image: I | E Desktop | CompanyInternal C | ompressed (zipped) Folder | 1,306 KB | No 1 |
| Recent Maces | Downloads | HighlyConfidential C | ompressed (zipped) Folder | 16,149 KB | No 16 |
| | E Recent Maces | hetwork_recon_local_only C | ompressed (zipped) Folder | 1,289 KB | No 1 |

Figure A-45. Locate the Port-Scanning File on the Desktop

• Go to the D3E *Deception* menu and make sure *Network Deception* is turned on.



Figure A-46. Make Sure Network Deception is Active

- Copy network_recon_local_only.zip to C:\ directory. (The file can be run from anywhere, but it seemed easier to us to execute the command from this location.)
- Open a command prompt; set the current directory to C:\; and run the attack script. Refer to Figure A-47 and Figure A-48.
 - Note that the script attacks ports 3389, 445, 139, and 135. These ports are used for Remote Desktop Protocol (RDP), Transmission Control Protocol

(TCP), Server Message Block (SMB), and Remote Procedure Call (RPC), respectively.

| C:\>dir | | | |
|-------------|--------------|---------------|------------------------------|
| Volume in | drive C has | no label. | |
| Volume Ser | ial Number i | s 7657-FF82 | |
| Volume oct | iai Namber i | | |
| Directory | of C·\ | | |
| bill cocory | 0. 0. (| | |
| 09/15/2020 | 09:46 AM | <dir></dir> | AlwaysOn |
| 04/13/2021 | 03:16 PM | <dir></dir> | Backup |
| 09/15/2020 | 09:49 AM | <dir></dir> | Dynamic |
| 08/01/2020 | 08:32 AM | <dir></dir> | Intel |
| 08/20/2019 | 11:13 AM | 2,648,576 | network_recon_local_only.exe |
| 08/01/2020 | 08:51 AM | <dir></dir> | PerfLogs |
| 04/19/2021 | 10:10 AM | <dir></dir> | Program Files |
| 08/01/2020 | 08:32 AM | <dir></dir> | Program Files (x86) |
| 09/14/2020 | 02:18 PM | <dir></dir> | Share |
| 08/01/2020 | 08:25 AM | <dir></dir> | Users |
| 04/19/2021 | 09:56 AM | <dir></dir> | Windows |
| | 1 File(s |) 2,648,57 | 6 bytes |
| | 10 Dir(s) | 94,684,778,49 | 6 bytes free |
| | | | |
| C+\>natwork | necon local | only eve | |

Figure A-47. Run the Attack Script



Figure A-48. Execution of Port-Scan Attack Script

- D3E's reaction to the *Network Deception* is shown in Figure A-49.
 - *ActiveLock* is engaged.
 - The D3E icon turns red.
 - The user is prompted to enter authentication to clear the threat.



Figure A-49. D3E Reaction to Port Scan

• Enter the D3E PIN to clear the threat.

• *ActiveLock* is now disengaged, as shown in Figure A-50.



Figure A-50. ActiveLock Disengaged

A.1.5.3 Evaluation Results

D3E *Network Manager* functioned as advertised on the Cigent laptop equipped with Secure Drives.

A.2 Cigent Secure SSD Features

A.2.1 Command Log Audit

A.2.1.1 Evaluation Steps for Command Log Audit

Cigent Secure SSDs store every command sent to the drive automatically. The commands are kept in a tamperproof location in the SSD's memory. "Cigent D3E also periodically writes markers to the log to indicate the activity was performed with D3E running and that the activity was properly authorized. Commands are stored for all partitions, including unsecured locations should the user have configured a portion of the drive as a normal NTFS⁴¹ partition. ... This command log can be used to audit drive activity to capture attempts to read information from the drive without D3E possibly indicating attempts to circumvent file protection. Further, the command log can be used to report on files accessed with or without D3E running by mapping the accessed locations to the current file system layout. This can reveal important information to investigators attempting to understand what was accessed or at least attempted to be accessed." [8].

⁴¹ NTFS = New Technology File System

- Open *Secure Drives* at the D3E Desktop.
 - Select the top $(\dots 81)$ SSD drive.
 - Click on the Advanced icon, as indicated by the red arrow in Figure A-51.

| 8 10.206.161.214 - Remote E | lesktop Connection | | | | - 🗆 × |
|-----------------------------------|---|--------------|---|-----------------|-------------|
| V | Secure Drives Protect files with firmware locking, the highest level of protecti | on | | | ^ |
| Dashboard File Type Protection | Name: CTI SSD 8/II: ESS907071F7900000081 FW: ECFM13T9 [447 68] | | | _/ | 💼 P: |
| Folder Protection | E Secure Drives | | _ | | |
| Secure Drives | Always On (locked) | Dynamic (P:) | | econfigure Chan | ge Password |
| Removable Storage | Name: CTI SSD s/fi: E55907071F7900000082 FW: ECFM13T9 [447 GB] | | | | â H: |
| Deception | | | | | _ |
| | | | | | |

Figure A-51. Click "Advanced"

• Click the Command Log Button. See Figure A-52. This will cause the *Command Log Audit* page (shown in Figure A-53) to be displayed.

| 🈼 10.206.161.214 - Remote I | Desktop Connection | | | | | - | o × |
|-----------------------------------|---|---------------|--|------|-------------|-----------|--------------------|
| v | Secure Drives Protect files with firmware locking, the highest level | of protection | | | | | |
| Dashboard File Type Protection | Name: CTI SSD s/n: E55907071F7900000081 FW: ECFM13T9 [44 | 7 68] | | | / | | ê P: |
| Folder Protection | Secure Drives | | | | | | |
| Secure Drives | Always On (locked) | Dynamic (P: | | | Deconfigure | Change Pa | assword Ivanced |
| Networks | | | | | Command | Log Erase | e Verify |

Figure A-52. Click "Command Log"

| Cigent D3E | Return to Secure Drives Command Log Audit CTI SSD | 16206.19314 - ð * | \$ 🗰 • 🔝 🗐 🖥 |
|---|---|------------------------------|--------------|
| Dashboard File Type Protection | S/N: E55907071F7900000081 | Read Unauthorized R/W | |
| Folder Protection | | | |
| Networks Removable Storage | | | |
| ປັ Deception | | | |
| | | | |
| Authentication | | | |
| Settings | | 44 44 Unauthorized R/W >> >> | |
| Dicense | Affected File Report | | |
| C Update | From 01/01/2000 ~ 12:00 AM C 01/01/2000 ~ 12:00 AM C | | Generate |
| 1 About | File reports are based on file locations at the time the report was generated | | |

Figure A-53. Command Log Audit Page

- When we ran the *Command Log Audit* evaluation, the SSD had not yet been scanned, so it was necessary to scan the drive.
 - Click the **Scan** button. (Our initial scan took about 15 minutes.)

- The log provides start and end times to indicate the time window covered by the scan, i.e., the time elapsed from the previous scan to the current scan.
- The log shows the volume of authorized reads and authorized writes, as well as the combined unauthorized reads and writes (indicated below the x-axis in red on the bar chart).



Figure A-54. SSD Scan Results

- Note that our sample report covers approximately the 10 days leading up to the scan.
- Note also that scan results can be saved to comma-separated values (CSV) files. Refer to Figure A-55.
 - Two csv files, of type *csv_files* and *csv_ranges*, can be generated per scan. See Figure A-56 below. The csv files can be opened in Excel or in a text editor.
 - To generate csv reports:
 - o Click Generate.
 - Save the file to the desired location.
 - Enter the prescribed authentication code (PIN).
 - Csv_files identify scan Time, Monitored status, Volumes, Letters, File IDs, Parent File IDs, and File Names.
 - Csv_ranges identify scan Time, Monitored status, Reads, Writes, and Ranges within memory.
- Administrators can drill down into specific scan timeframes by clicking on individual bars within the chart. Figure A-57 displays bar-chart data for a 48minute span on 4/20/21. *Csv_file* and *csv_range* reports can be generated for these ranges, as well.

| ← → · ↑ | ? Size |
|---|-----------|
| Organize New folder Name Date modified Type | ? Size |
| This PC Name Date modified Type | Size |
| | |
| 3D Objects Company Confidential 4/22/2021 1:31 PM File folder | |
| A on RCAT-JUMF supersecret 4/15/2021 2:26 PM File folder | |
| C on RCAT-JUMF which_setting 9/28/2020 2:32 PM File folder | |
| 🖋 D on RCAT-JUMF | |
| E Desktop | |
| Documents | |
| Downloads | |
| h Murie V K | > |
| File name: CTI SSD_20210419_1011-20210428_1609.csv | ~ |
| Save as type: *.csv | ~ |
| ∧ Hide Folders Save Cance | el |





Figure A-56. Two CSV Files Generated



Figure A-57. Drill Down for Audit Data for Shorter Time Span

- After the initial scan completes, clicking the **Scan** button again simply (and promptly) retrieves the existing scan log. To obtain a fresh scan after some time has passed, press the **Full Rescan** button.
- Using Command Logs:
 - Cigent points out that the values in the csv_files of greatest importance are found in the *Time*, *Monitored*, and *File Name* columns.
 - Permissible values for *Monitored* are *Yes* and *No*. A *Monitored* value of *Yes* indicates that the file access was authorized (because the administrator entered the correct authentication code before the access attempt), while a value of *No* means that the file access was unauthorized.
 - Knowing the names of sensitive files can be beneficial when scanning audit logs. Recall that the file *Confidential.txt* resides on drive L and has *Always On* protection. Figure A-58 below shows that an unauthorized attempt was made to access the file on 20 April at 19:29:43 UTC, or ~3:30 PM local time.

| III SSD_20210420_0907-20210429_1115.csv_files.csv - Notepad | | | | | |
|--|-------------------------|-------------|--|--|--|
| File Edit Format View Help | | | | | |
| 2021-04-20 18:14:06 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,40,5,Annual Report - draft - confi | dential.docx | | | | |
| 2021-04-21 18:54:23 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,40,5,Annual Report - draft - confidential.docx | | | | | |
| 2021-04-21 18:59:23 UTC, Yes, {ef8e5bcc-9594-4065-a399-159bea0b0d1},L,40,5,Annual Report - draft - confidential.docx | | | | | |
| 2021-04-21 19:33:10 UIC,Yes,{ef8e5bcc-9594-4065-a399-159bea000dd1},L,40,5,Annual Report - draft - confidential.docx | | | | | |
| 2021-04-21 18:54:23 UIC,YES,{ef8e50CC-9594-4065-8399-1590E800041},L,44,5,01111ng.XISX | | | | | |
| 2021-04-21 19:55:10 UIC, YES, {eroesocc-9594-4005-8599-1590e8000041;j_L,41,5,01111ng.x15x | Find | × | | | |
| 2021-04-20 15:25:45 OFC, NO, (e18e5bcc-0554-4005-a559-159bea0b0441), L, 42, 5, confidential txt | | | | | |
| 2021-04-21 18:31:20 UTC Yes {ef8e5hcc.9594.4065-s.399.159haa0hd041}; 1.35 Confidential tvt | Find what: confidential | Find Next | | | |
| 2021-04-21 18:32:20 UIC Yes (ef8e5brc-9594-4065-a399-159bea0b0d41) L.42.5.Confidential.txt | Direc | tion Cancel | | | |
| 2021-04-21 18:54:23 UTC.Yes./ef8e5bcc-9594-4065-a399-159bea0b0d41\.L.42.5.Confidential.txt | 0 | | | | |
| 2021-04-21 18:59:23 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,42,5,Confidential.txt | Match gase | p @ gom | | | |
| 2021-04-21 19:02:55 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,42,5,Confidential.txt | Wrap around | | | | |
| 2021-04-21 19:08:07 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,42,5,Confidential.txt | | | | | |
| 2021-04-21 19:26:09 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,42,5,Confidential.txt | | | | | |
| 2021-04-21 19:33:10 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,42,5,Confidential.txt | | | | | |
| 2021-04-20 17:34:05 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,43,5,corporate_info.pdf | | | | | |
| 2021-04-20 17:51:05 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,43,5,corporate_info.pdf | | | | | |
| 2021-04-20 18:14:06 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,43,5,corporate_info.pdf | | | | | |
| 2021-04-21 18:54:23 UTC,Yes,{ef8e5bcc-9594-4065-a399-159bea0b0d41},L,43,5,corporate_info.pdf | | | | | |
| 2021-04-21 18:59:23 UTC, Yes, {ef8e5bcc-9594-4065-a399-159bea0000441}, L, 43, 5, corporate_info.pdf | | | | | |
| 2021-04-21 19:33:10 UTC,Yes,{e+8e5bcc-9594-4065-a399-159bea0b0d41},L,43,5,corporate_info.pdf | | | | | |

Figure A-58. Command Log Showing Unauthorized Access to File

A.2.1.2 Evaluation Results

D3E *Command Log Audit* functioned as advertised on the Cigent laptop equipped with Secure Drives.

A.2.2 True Erase

Secure, verifiable data erasure from hard drives helps prevent unauthorized access to sensitive or classified information. Cigent SSDs provide a *True Erase* feature that supports "extended erasure verification commands to check each and every mapped and unmapped block to verify the data has been removed" [8]. The *Erase Verify Secure Drive* commands described below will result in **Failure** if any blocks in memory show un-erased data.

A.2.2.1 True Erase Evaluation Steps

• Select the detached SSD (S/N ...82) to check whether there are un-erased data blocks on the drive. Since we're using the internal SSD (S/N ...81) to conduct our *True Erase* evaluation, we know in advance that our SSD has not been erased. If it had been, D3E

wouldn't be installed and we couldn't conduct the evaluation. We can, however, check the detached drive.

- Open *Secure Drives* at the D3E Desktop.
 - \circ Select the detached (...82) SSD drive.
 - Click on the *Advanced* icon.
 - Then click on the Erase Verify button. Refer to Figure A-59.



Figure A-59. Execute the Erase Verify Procedure

The results of the *Erase Verify* procedure are shown in Figure A-60. Because the detached SSD has not been erased, the *Erase Verify* action appropriately reports *Device Not Erased*. The Erasure Verification Analysis shows that no blocks on the drive have been erased.



Figure A-60. Erase Verification Analysis

A.2.2.2 Evaluation Results

The D3E *True Erase* feature functioned as advertised on the Cigent laptop equipped with Secure Drives.

A.2.3 KeepAlive (Tethering)

The *KeepAlive* feature binds Cigent Secure SSDs to the D3E software running on them by means of a non-replayable heartbeat between the drive and D3E. When the feature is activated, Secure SSDs will enact *ActiveLock* and prevent file access if the drive fails to receive the heartbeat

signal in time. The feature prevents attackers from stopping D3E protection on unlocked Secure Drives.

If *KeepAlive* tethering has been provisioned for an SSD, there will be a small blue heart next to the drive icon in the Dashboard's *Secure Drive* panel. Figure A-61 indicates that the internal (...81) SSD has been provisioned with the *KeepAlive* feature, while the external (...82) drive has not.



Figure A-61. KeepAlive Provisioned on One Drive

A.2.3.1 KeepAlive Evaluation Steps

- Make sure both the *Always On* and *Dynamic* partitions on the internal SSD are unlocked.
- Enter "services" in the Windows search box.


Figure A-62. Tethering Evaluation – Step 1

- Open the **Services** application and find the Cigent D3E Service.
- Right-click on the CigentD3E row and click *Properties*.

| 🖁 Services | | | | | the H | |
|--------------------|---------------------|---------------------------|---------------|---------|--------------|---------------|
| File Action View | Help | | | | | |
| Þ 🔿 📅 🏟 d | à 🗟 🛛 📰 🕨 🗰 H 🕩 | | | | | |
| 🐊 Services (Local) | Services (Local) | | | | | |
| | Cigent D3E | Name | Description | Status | Startup Type | Log On As |
| | | BranchCache | This service | | Manual | Network S |
| | Stop the service | Capability Access Manager | Provides fac | Running | Manual | Local Syste |
| | Restart the service | CaptureService_f8544 | Enables opti | Running | Manual | Local Syste |
| | | 🔍 Cellular Time | This service | - | Manual (Trig | Local Service |
| | Description: | Certificate Propagation | Copies user | Running | Manual (Trig | Local Syste |
| | Cigent D3E | Cigent D25 | Cigent D3E | Running | Automatic | Local Syste |
| | | Cli Start | Provides inf | | Manual (Trig | Local Syste |
| | | 🔍 Cli Stop | This user ser | Running | Manual | Local Syste |
| | | CN Pause | The CNG ke | Running | Manual (Trig | Local Syste |
| | | CC Resume | Supports Sy | Running | Automatic | Local Service |
| | | CC Pertart | Manages th | | Manual | Local Syste |
| | | Q Co | This service | Running | Automatic (| Local Service |
| | | 🔍 Co All Tasks > | This user ser | Running | Automatic | Local Syste |
| | | Co Refrech | The Connec | Running | Automatic | Local Syste |
| | | Q Co | Allows Con | | Manual | Local Syste |
| | | Co Properties | Indexes con | | Manual | Local Syste |
| | | Co Hele | Manages co | Running | Automatic | Local Service |
| | | Cn | Provides se | Running | Manual | Local Syste |
| | | CredentialEnrollmentMana | Credential E | | Manual | Local Syste |
| | | Cryptographic Services | Provides thr | Running | Automatic | Network S |
| | | Data Sharing Service | Provides da | Running | Manual (Trig | Local Syste |
| | | 🖾 Data Usage | Network da | Running | Automatic | Local Service |

Figure A-63. Tethering Evaluation – Step 2

• At the *Recovery* tab, change all failure options to **Take No Action** and then click **OK**. See Figure A-64.

| Name | Description | Status | Startup Type | Log On As | | |
|-------------------------------|---------------|---------|--------------|--------------------------------|--|------------|
| 🥋 BranchCache | This service | | Manual | Network S | | |
| 🧠 Capability Access Manager | Provides fac | Running | Manual | Local Syste | | |
| CaptureService_f8544 | Enables opti | Running | Manual | Local Syste | | |
| 🔍 Cellular Time | This service | | Manual (Trig | Local Service | | |
| Certificate Propagation | Copies user | Running | Manual (Trig | Circuit D25 Descertion (Local | Commuted | × |
| 🥋 Cigent D3E | Cigent D3E | Running | Automatic | Cigent D3E Properties (Local | Computer) | ^ |
| Client License Service (ClipS | Provides inf | | Manual (Trig | General Log On Recovery | Dependencies | |
| Clipboard User Service_f8544 | This user ser | Running | Manual | | | |
| 🆏 CNG Key Isolation | The CNG ke | Running | Manual (Trig | Select the computer's response | se if this service fails. <u>Help me set u</u> | o recovery |
| 🧠 COM+ Event System | Supports Sy | Running | Automatic | delions. | | |
| 🖏 COM+ System Application | Manages th | | Manual | First failure: | Take No Action | ~ |
| 🧠 Connected Devices Platfor | This service | Running | Automatic (| Second failure: | Take No Action | ~ |
| 🧠 Connected Devices Platfor | This user ser | Running | Automatic | | Take the Platent | |
| 🤹 Connected User Experience | The Connec | Running | Automatic | Subsequent failures: | Take No Action | ~ |
| 🥋 ConsentUX_f8544 | Allows Con | | Manual | Reset fail count after: | 0 davs | |
| 🆏 Contact Data_f8544 | Indexes con | | Manual | | | |
| 🆏 CoreMessaging | Manages co | Running | Automatic | Restart service after: | 0 minutes | |
| 🥋 Credential Manager | Provides se | Running | Manual | | NI | |
| 🥋 CredentialEnrollmentMana | Credential E | | Manual | Enable actions for stops w | Restart Computer Op | otions |
| 🥋 Cryptographic Services | Provides thr | Running | Automatic | Run program | | |
| 🖏 Data Sharing Service | Provides da | Running | Manual (Trig | Program: | | |
| 🆏 Data Usage | Network da | Running | Automatic | | Brow | se |
| 🖏 DCOM Server Process Laun | The DCOML | Running | Automatic | | | |
| Delivery Optimization | Performs co | | Automatic (| Command line parameters: | | |
| Device Association Service | Enables pair | Running | Automatic (T | Append fail count to en | d of command line (/fail=%1%) | |
| 🖏 Device Install Service | Enables a c | | Manual (Trig | | d of continiarid line (/fail= % 1%) | |
| 🧠 Device Management Enroll | Performs D | | Manual | | | |
| Q Device Management Wirele | Routes Wire | | Manual (Trig | | OK Cancel | Apply |
| 🖏 Device Setup Manager | Enables the | Running | Manual (Trig | | Gunder | . 444.0 |
| DeviceAssociationBroker f8 | Enables app | - | Manual | Local System | | |

Figure A-64. Tethering Evaluation – Step 3

• Create a batch file called *keepalivetest.bat*, with contents as shown in Figure A-65 below. Note: Make sure that the drive letter in the "copy test" line matches that of the *Dynamic* partition on the Secure Drive.

| | | | 183 | | | - |
|---------------|------------|----------------|-------|---|----------|---|
| keepalivetes | t.bat - No | tepad | _ | | \times | |
| File Edit For | mat View | w Help | | | | |
| echo off | | | | | ^ | ł |
| echo "This | is a te | est">>test.txt | | | | |
| conv test.t | xt P:\ | IV | | | | t |
| timeout 5 | | | | | | |
| goto start | | | | | | f |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | I |
| | | | | | | ĺ |
| | | | | | | I |
| | | | | | | Î |
| | | | | | | ł |
| < | | | | | > ~ | ł |
| Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8 | 3 | | 1 |

Figure A-65. Tethering Evaluation – Step 4

• Save the batch file to the *Documents* folder on the C:\ drive⁴², as shown in Figure A-66.

⁴² We saved the file to the user's *Documents* directory on the C:\ drive.

| 🗟 🖓 📙 🖛 Documents | | | | | - | o x |
|--|-------------|-----------------|--------------------|-------------------|-----------------|------------|
| File Home Share View | | | | | | ~ 0 |
| The share view | | | - | | | • |
| 🖈 🖹 📋 🕹 Cut 🛛 📃 🖳 🗶 🛋 | New item * | V Open - | Select all | | | |
| Rin to Quick Conv. Parta | Easy access | Propertier Edit | Select none | | | |
| access Paste shortcut to v to v | folder | • History | 🔡 Invert selection | | | |
| Clipboard Organize | New | Open | Select | | | |
| ← → ∽ ↑ 🗄 → This PC → Local Disk (C:) → Users → cigent → Docum | ents | | | ~ Ō | Search Document | 5 |
| | | ^ | | | | |
| > E Pictures | Name | | Date modified | Туре | Size | |
| > 🚼 Videos | Company C | onfidential | 4/22/2021 1:31 PM | File folder | | |
| Y 🏪 Local Disk (C:) | supersecret | | 4/15/2021 2:26 PM | File folder | | |
| AlwaysOn | which setti | na | 9/28/2020 2:32 PM | File folder | | |
| Backup | keepalivete | t.bat | 4/30/2021 11:45 AM | Windows Batch Fil | le 1 KB | |
| | passwords. | ls | 4/22/2021 1:29 PM | XLS File | 1 KB | |
| Dynamic | | | | | | |
| > intel | | | | | | |
| PerfLogs | | | | | | |
| > 🧧 Program Files | | | | | | |
| > Program Files (x86) | | | | | | |
| Share | ~ | | | | | |
| 5 itans | | | | | | 800 80 |
| Sitems | | | | | | 8 E |

Figure A-66. Tethering Evaluation – Step 5

- Run the batch file, as described below and shown in Figure A-67:
 - Open a command-prompt window.
 - Navigate to the *Documents* directory.
 - Start the batch file (type "keepalivetest.bat").
 - Leave the batch file running.



Figure A-67. Tethering Evaluation – Step 6 [8]

- Open a command prompt and navigate to C:\.
 - Run as administrator the command: "taskkill /IM cigentservice.exe /F"; this will shut down the Cigent Service. See Figure A-68.



Figure A-68. Tethering Evaluation – Step 7 [8]

- Within 30 seconds the script output from the batch job will display an **ERROR Verify** message.
 - Press Ctrl-C to terminate the batch job.

```
Waiting for 0 seconds, press a key to continue ...
ERROR Verify - P:\test.txt
    1 file(s) copied.
Waiting for 0 seconds, press a key to continue ...
ERROR Verify - P:\test.txt
    1 file(s) copied.
Waiting for 0 seconds, press a key to continue ...
ERROR Verify - P:\test.txt
    1 file(s) copied.
Waiting for 4^CTerminate batch job (Y/N)? ynue ...
C:\Users\cigent\Documents>
```

Figure A-69. Tethering Evaluation – Step 8 [8]

- Open Windows Explorer and Navigate to the L *Always On* drive.
 - Killing the D3E process severs the *KeepAlive* tether between D3E and the SSD. The drive's firmware locks the drive when no D3E heartbeat is detected.
 - The D3E Dashboard informs you that the service has been disabled. See Figure A-70.



Figure A-70. D3E Has Been Disabled

 Verify that it is impossible to open files or copy files to the drive. See Figure A-71.

| \leftarrow \rightarrow \checkmark \uparrow \checkmark This PC \rightarrow CIGENT ALWAYS ON (L:) \rightarrow | |
|---|---|
| Interrupted Action — — X | Name Date |
| - Interopeet inter | secret subfolder 4/30/2 |
| Invalid MS-DOS function. | Annual Report - draft - confidential.docx 8/6/2 |
| keepalivetest.txt | billing.xlsx 8/6/2 |
| Size: 94 bytes | Confidential.txt 8/6/2 |
| Date modified: 4/30/2021 11:39 AM | corporate_info.pdf 8/23/2 |
| Try Again Skip Cancel | fw4.pdf 3/18/2 |
| ing righting only concer | 🔤 fw9.pdf 3/18/3 |
| | iw9.pdf 3/18/ |
| More details | Ransomware Prevention and Resp.pdf 8/6/2 |
| Local Disk (C:) | Ransomware_Executive_One-Page.pdf 8/6/2 |
| Elements (E:) | sans ransomeware.pdf 8/6/2 |
| CIGENT DYNAMIC (H:) | |
| CIGENT ALWAYS ON (L:) | |
| secret subfolder | |
| CIGENT DYNAMIC (P:) | ~ |

Figure A-71. Cannot Copy Files to the Always On Drive

- Return to normal operating mode by doing the following:
 - Turn the Cigent Service back on.
 - Return to the Cigent *Services Properties* page shown in Figure A-64 and change failure options at the *Recovery* tab back to **Restart the Service**.

A.2.3.2 Evaluation Results

The *KeepAlive* SSD feature performed as advertised. When the heartbeat tether between the SSD and D3E was severed, firmware in the drive locked the *Always On* drive, so that it was not possible to open files or write to that drive. In other words, when the heartbeat stopped, the *Always On* drive was protected, even though the D3E service had stopped. It was possible to open the *Dynamic* Drive and write to it, but that was expected.

We did notice an anomaly in the Cigent documentation. Reference [8] states that "In less than 30 seconds, the script output will start indicating 0 files copied and you will receive a Windows error indicating Write Protect Error. Press Ctrl-C to terminate the script." In fact, Windows gave the *ERROR Verify* message shown in Figure A-69.

A.3 D3E Software Locking Mode

The evaluation procedures below are described in reference [8] as pertaining to D3E software on Windows computers without SSD Secure Drives. Each of the procedures was run on our two Win7 test laptops. In a few instances, we supplemented earlier testing on the Cigent SSD-equipped Win10 laptop and ran D.3 software-locking tests on that machine, as well.

A.3.1 Folder Protection

Folder Protection for Cigent Secure SSD Drives was tested in Section A.1.2. The steps below demonstrate D3E *Folder Protection* for Windows PCs that are not equipped with Secure SSD Drives. For our evaluation, the two MITRE Win7 laptops were used to validate this Cigent capability.

A.3.1.1 Establish Secure Data Locations on Win7 Laptops

- At <u>both Win7 laptops</u>, perform the following steps. (The *CompanyInternal* and *HighlyConfidential* zipped files can be found in the desktop folder named EvaluationKitAuxFiles.)
 - Create a directory C:\Cigent.
 - Unzip *CompanyInternal* into C:\Cigent.
 - Unzip HighlyConfidential into C:\Cigent.
 - Select *Folder Protection* at the D3E Dashboard.
 - Click Add a Dynamic Protection Folder.

| Cigent D3E | | _ 🗆 × |
|----------------------|--|-------|
| v | Folder Protection | |
| Dashboard | Dynamic Protection Folders | |
| File Type Protection | Files in Dynamic protection folders only require authentication to access when ActiveLock is or Add a Dynamic Protection Folder | n |
| Folder Protection | C:\Users\RCAT\Documents | |
| Secure Drives | C:\Users\RCAT\Pictures | |
| L Networks | C:\Users\RCAT\Videos | |
| Removable Storage | Always On Protection Folders | |
| J Deception | Files in Always On protection folders always require authentication to access Add an Always On Protection Folder | |
| | C:\Users\RCAT\Documents\HighlyConfidential | |
| authentication | | |



Browse to C:\Cigent\CompanyInternal and click the Select Folder button.

| Select a Folder | | | × |
|---------------------------------------|--------------------|---------------------|----------|
| 🔄 🕞 - 📕 - Cigent - CompanyInternal | ▼ 65 | Search CompanyInter | nal 😥 |
| Organize 🔻 New folder | | |)III 🔻 🔞 |
| 🍌 Sample Music 🔺 Name 🗠 | | Date modified | Туре |
| E Pictures | | | |
| E My Pictures | No items match you | ur search. | |
| E 🎍 Public Pictures | | | |
| Jample Picture | | | |
| 🗉 🛅 Videos | | | |
| | | | |
| I I I I I I I I I I I I I I I I I I I | | | |
| Cinent | | | |
| CompanyInter | | | |
| HighlyConfider | | | |
| PerfLogs | | | |
| 🗄 🍌 Program Files | | | |
| E 🎍 SOFTWARE | | | |
| 🗄 🌗 Users 🔤 📲 | | | |
| | | | <u> </u> |
| Folder: CompanyInternal | | | |
| | | Select Folder | Cancel |
| | | | |

Figure A-73. Folder Protection – Setup Step 2

- Enter your PIN at the D3E prompt.
- Click Add an Always On Protection Folder.
 - Browse to C:\Cigent\HighlyConfidential and click the Select Folder button.
 - Enter your PIN at the D3E prompt.
- Results of these setup procedures are seen in Figure A-74.

| Cigent D3E | _ . × |
|----------------------|---|
| I | Folder Protection Protect files by folder location |
| Dashboard | Dynamic Drotaction Foldors |
| File Type Protection | Files in Dynamic protection folders only require authentication to access when ActiveLock is on Add a Dynamic Protection Folder |
| Folder Protection | C:\Users\RCAT\Documents |
| Secure Drives | C:\Users\RCAT\Pictures |
| L Networks | C:\Users\RCAT\Videos |
| 🔗 Removable Storage | C:\Cigent\CompanyInternal |
| 3 Deception | Always On Protection Folders Files in Always On protection folders always require authentication to access Add an Always On Protection Folder |
| Ruthentication | C:\Users\RCAT\Documents\HighlyConfidential |
| Settings | |

Figure A-74. New Dynamic and Always On Folders Added

A.3.1.2 Remove Always On and Dynamic Protection Folders

• To remove an *Always On* or *Dynamic* protection folder, simply click on one of the displayed folders, and then click the **Remove** button and use the appropriate authentication method (PIN).



Figure A-75. Removing Always On and Dynamic Protection Folders

A.3.1.3 Assign both Dynamic and Always On Protection to a Folder

- Any attempt to assign both *Dynamic* and *Always On* protection to the same folder simultaneously should fail.
- Try to assign *Always On* protection to the C:\Cigent\CompanyInternal folder. (Note that the folder already has been assigned *Dynamic* protection.)
- Repeat the procedure described in Section A.3.1.2 for assigning *Always On* protection, browse to the C:\Cigent\CompanyInternal directory, and click **Select Folder**.

• The attempted double-assignment fails, as expected and desired.

| | Folder Protection | ו | | | |
|----------------------|--|---------------------------------------|-----------------------------|--|--|
| | Protect files by folder locatio | n | | | |
| Dashboard | Dynamic Protection Fold | lers. | | | |
| File Type Protection | Files in Dynamic probaction folders of | rdy migure authentication to an | cass other Activation is or | | |
| Folder Protection | ED Add a Dynamic Protec | tion Polder | | | |
| | C./Users/eCAT/Dooun | nents | | | |
| Secure Drives | C:\Users\ACAT\Picture | 6 | | | |
| Networks | C:\Livers\RCAT\Video | | | | |
| Removable Storage | C:\Cigent\CompanyInternal | | | | |
| Deception | Always On Protection | This folder is already configured. | | | |
| Authentication | C:\Cigent\HighlyConfi | dential | | | |
| Settings | | | | | |
| License | | | | | |
| Update | | | | | |
| About | | | | | |

Figure A-76. Cannot Assign Dual Protection Configurations to a Folder

A.3.1.4 Win10 64-Bit Evaluation

(Verify Add & Delete Folder Protection for Secure SSD Drives)

• Always On and Dynamic protection features for Cigent Secure SSD Drives were covered as part of Firmware Locking in Section A.1.2 above, but the Adding and Deleting Folder Protection capability was omitted from that evaluation, because that functionality is considered software-only protection. Therefore, we revisited our earlier testing and tried to add and delete folder protection for the Cigent Win10 SSD-equipped machine. The D3E folder-protection feature met expectations, segregating important information into Always On and Dynamic folders to protect sensitive data.

A.3.1.5 Win7 32-Bit Evaluation

• Folder protection performed well and as expected for the MITRE Win7 32-bit laptop.

A.3.1.6 Win7 64-Bit Evaluation

• Folder protection performed well and as expected for the MITRE Win7 64-bit laptop.

A.3.2 Dynamic and Always On Protection

A.3.2.1 Accessing Always On Files

Perform the following steps at **both Win7 laptops**.

• Browse to C:\Cigent\HighlyConfidential in Windows Explorer.

| | - | viM228134-PC | | x / | |
|---------------------------------|---|----------------------|--------------------|----------|------------|
| HighlyConfidential | | | | | |
| C→ → MM228134-PC 32 | bit 🔹 Local Disk (C:) 🔹 Cigent 👻 HighlyConfider | ntial | | 👻 🚱 Sea | arch Hig 😥 |
| Organize 👻 Include in library 👻 | Share with 👻 New folder | | | 8== | • 🔟 🔞 |
| E 🛧 Favorites | Name * | Date modified | Туре | Size | |
| Nesktop | 📄 Annual Report - draft - confidential | 8/6/2019 3:52 PM | Office Open XML Do | 385 KB | |
| Downloads | billing.xlsx | 8/6/2019 3:51 PM | XLSX File | 15 KB | |
| E Recent Places | Confidential | 8/6/2019 3:51 PM | Text Document | 1 KB | |
| 🗆 🥽 Libraries | corporate_info.pdf | 8/23/2018 10:33 PM | PDF File | 7,317 KB | |
| Documents | fw4.pdf | 3/18/2019 12:59 PM | PDF File | 124 KB | |
| 🗉 🌙 Music | fw9.pdf | 3/18/2019 12:59 PM | PDF File | 128 KB | |
| 🕀 🔛 Pictures | iw9.pdf | 3/18/2019 12:59 PM | PDF File | 148 KB | |
| Videos | Ransomware Prevention and Resp.p | df 8/6/2019 3:39 PM | PDF File | 154 KB | |
| | Ransomware_Executive_One-Page. | odf 8/6/2019 3:50 PM | PDF File | 783 KB | |
| □ 1 mm228134-PC 32 bit | sans ransomeware.pdf | 8/6/2019 3:46 PM | PDF File | 9,342 KB | |
| Cigent | | | | | |
| CompanyInternal | | | | | |
| lighlyConfidential | | | | | |
| PerfLogs 💌 | | | | | |
| 10 items | | | | | |

Figure A-77. Browse to HighlyConfidential Folder

• Double-click on the *Confidential.txt* to open the file. Regardless of the *ActiveLock* state, it will be necessary to use an approved authentication method to open the file, because the folder has *Always On* protection. See Figure A-78. After the correct PIN has been entered, opening/editing the file is possible.

| 1 | HighlyConfidential | | | | | _ 0 × | F 🕫 | ् । 🏦 🔍 | |
|----------------------------|--|---|--|--|--|---------------------------|--|---------------------------|----|
| old cigent builds et al | O I + MM228134-PC 32 bit + Local Disk (C:) | Cigent • HighlyConfidential | | | 👻 🚺 Sea | rch Hig 😥 | | | |
| | Organize 🝷 🧾 Open 🝷 Print New Folder | | | | 388 | - 🗆 0 | | | |
| | Name - | 1 | Date modified | Туре | Size | | | | |
| File Edit Format Wew Help | | iort - draft - confidential | 8/6/2019 3:52 PM 8/6/2019 3:51 PM 8/6/2019 3:51 PM | Office Open XM, Do XLSX File Text Document | 385 KB 15 KB 1 KB | | Protection by folder location | | |
| | | info.pdf | 8/23/2018 10:33 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM 3/18/2019 12:59 PM | PDF File PDF File PDF File PDF File | 7,317 KB 124 KB 128 KB 148 KB | | Protection Folders c protection folders only require authentication to Dynamic Protection Folder | access when ActiveLock is | on |
| | | re Prevention and Resp.pdf re_Executive_One-Page.pdf meware.pdf | 8/6/2019 3:39 PM 8/6/2019 3:50 PM 8/6/2019 3:46 PM | PDF File PDF File PDF File | 154 KB 783 KB 9,342 KB | | ers\RCAT\Documents | | |
| | | | | | | | ers\RCAT\Pictures ers\RCAT\Videos | | |
| | | | 010 0 51 54 | | | | gent\CompanyInternal | | |
| | | M Date created: 8(6)2 | U193:51 PM | 0 Deception | | Files in Always Add an | n Protection Folders On protection folders always require authenticate Always On Protection Folder | on to access | |
| | | | | 🛞 Authentica | tion | C:\Ci | gent\HighlyConfidential | | |
| | | | | Settings | | | | | |
| | | | | License | | | | 🚧 Authorize 🗖 | |
| | | | | C Update | | | | File Access | |
| | | | | About | | | | Enter PIN | _ |
| | | | |] | | | Cigent D ³ E v2 | Enter your PIN | |

Figure A-78. Authentication Required to Unlock Always On Protection

A.3.2.2 Accessing *Dynamic* Files

Perform the following steps at **both Win7 laptops**.

- Make sure *ActiveLock* is not engaged. The shield at the D3E Desktop should be green.
- Browse to C:\Cigent\CompanyInternal in Windows Explorer.

| | H MM2 | 28134-PC | _ 8 > | × | | | | |
|---------------------------------|---|--------------------|---------------|-----------------|--|--|--|--|
| 🕌 CompanyInternal | | | | | | | | |
| 🕞 🕞 🗸 🖌 🗸 MM228134-PC | 32 bit 🝷 Local Disk (C:) 🝷 Cigent 🝷 CompanyInternal | | | 👻 🔯 Search Co 💋 | | | | |
| Organize 🔻 Include in library 🔻 | Organize 🔻 Include in library 👻 Share with 💌 New folder 🛛 😥 😧 | | | | | | | |
| 🖃 🜟 Favorites | Name ^ | Date modified | Туре | Size | | | | |
| 🧮 Desktop | cr2e047.pdf | 3/18/2019 12:59 PM | PDF File | 560 KB | | | | |
| Downloads | Form 2464 - Annual Franchisor Cert.pdf | 3/18/2019 12:59 PM | PDF File | 217 KB | | | | |
| 🕍 Recent Places | InternalMemos | 8/6/2019 3:51 PM | Text Document | 1 KB | | | | |
| 🗆 🥽 Libraries | Ransomware_Trifold_e-version.pdf | 8/6/2019 3:41 PM | PDF File | 803 KB | | | | |
| E Documents | | | | | | | | |
| 🕀 🎝 Music | | | | | | | | |
| E Pictures | | | | | | | | |
| 🛨 📷 Videos | | | | | | | | |
| 🖂 🌉 MM228134-PC 32 bit | | | | | | | | |
| 🖃 💒 Local Disk (C:) | | | | | | | | |
| 🖃 🍌 Cigent | | | | | | | | |
| CompanyInternal | | | | | | | | |
| PerfLogs | | | | | | | | |
| 4 items | | | | | | | | |

Figure A-79. Browse to CompanyInternal Folder

• Double-click on *InternalMemos* to open the text file. Because *ActiveLock* is not engaged, the file will open without the need for authentication.



Figure A-80. Dynamic Files Open when ActiveLock not Engaged

- To demonstrate that D3E locks access to *Dynamic* files when *ActiveLock* is engaged, we will jump ahead and show that attempting to open a *Deception* file triggers *ActiveLock*, which, in turn, blocks access to *Dynamic* files and requires authentication to unlock. The topic of *Deception* Files is covered in greater detail in Section A.3.3 below.
 - Navigate to the *passwords.xls Deception* file in the *Documents* folder. See Figure A-81.

| | H | MM228134-PC | _ 8 > | × |
|--|--|--------------------|-------------|----------------------|
| Documents | | | | _ _ _ _ _ |
| COV 🖹 🗸 Libraries 🗸 Docum | ents 🔻 | | | 👻 🛃 Search Do 👂 |
| Organize 🔻 Share with 🔻 New | folder | | | = - 🗊 😧 |
| Favorites | Documents library Includes: 2 locations | | | Arrange by: Folder 🔻 |
| Becent Places | Name * | Date modified | Туре | Size |
| | 퉬 CompanyInternal | 4/28/2021 11:13 AM | File folder | |
| 🖃 🥽 Libraries | \mu HighlyConfidential | 4/28/2021 11:13 AM | File folder | |
| Documents Music Pictures Videos | passwords.xls | 3/10/2021 11:42 AM | XLS File | 1 KB |

Figure A-81. Locate the Default Deception File

• Double-click on the file and attempt to open it. Note that trying to open the honeypot file triggers *ActiveLock* and access to the file is denied.



Figure A-82. D3E Locks Engages ActiveLock when Threats Are Sensed

- Ignore the *Data Deception Event* for now.
- Attempt to open *InternalMemos.txt* before clearing the alarm. Note that the D3E administrator must use authentication before the *Dynamic* file can be opened. See Figure A-83 and Figure A-84.

| CompanyInternal | | | | - | _ 🗆 🗙 | F → P | • • • |
|---------------------------------------|--|----------------------|---------------------|----------------|-------|-------|------------------------|
| 🌀 🕞 - 🕌 + ММ228134-РС 32 Ы | t 🔹 Local Disk (C:) 👻 Gigent 👻 CompanyInternal | | | 🔹 🔯 🛛 Search C | 0 🙋 | | |
| Organize 💌 🧾 Open 💌 Print | New folder | | | 800 - | | | |
| | Name ~ | Date modified | Туре | Size | | | |
| MM228134-PC 32 bit Local Disk (C:) | Cr2e047.pdf | 3/18/2019 12:59 PM | PDF File | 560 KB | | | |
| 🔒 Cigent | Form 2464 - Annual Franchisor Cert.pdf | 3/18/2019 12:59 PM | PDF File | 217 KB | | | |
| CompanyInternal | InternalMemos Reprozemana Trifold examples off | 8/6/2019 3:51 PM | Text Document | 1 KB | | | |
| Devil are | E carsonware_nrou_e-version.pu | 0/0/2019 3.41 PM | POLITIK | 005 KB | | | |
| Ele Edit Format View Help | | | | _ 0 > | S | | |
| | | | | | 1 1 | | |
| | | | | | 1 1 | | |
| | | | | | 1 1 | | |
| | | | | | 1 1 | | |
| | | | | | 1 1 | | |
| 1 | | | | | 1 1 | | |
| | | | | | | | |
| | | | | | 1 1 | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Authentica | ation | • | | | | | |
| | Networks | Domourbl | - Charman | | | | |
| Settings | | | Court Technology | | | (4) | Authorize File Access |
| ActiveLock E | ingageoj Ogi | ent Dre v2.4.4 © 202 | I Ugent Technology, | Inc. | | | THE FREEDO |
| | | | | | | | here and |
| | | | | | | | Enter PIN |
| | | | | | | | |
| | | | | | | | Enter your PIN |

Figure A-83. ActiveLock Must Be Cleared before Opening Dynamic Files



Figure A-84. Dynamic File Opens After ActiveLock Has Been Cleared

• Return to the D3E Dashboard to clear the *Data Deception Event* by using the prescribed authentication.

A.3.2.3 Win7 32-Bit Evaluation

• The evaluation of D3E *Dynamic* and *Always On* file protection on the MITRE Win7 32bit laptop went as expected. All advertised features were demonstrated successfully.

A.3.2.4 Win7 64-Bit Evaluation

• The evaluation of D3E *Dynamic* and *Always On* file protection on the MITRE Win7 64bit laptop went well and as expected.

A.3.3 Deception Files

The evaluation steps below were performed on the two MITRE Win7 laptops. They echo those conducted in Section A.1.3 for the Cigent SSD-equipped laptop and demonstrate D3E's response to attempts to access default and user-created honeypot *Deception* files.

A.3.3.1 Attempt to Access the Default passwords.xls Deception File

- Find the location of the D3E default *Deception* file, *passwords.xls*.
 - Click ³ Deception</sup> at the D3E Dashboard.
 - Then click Show All at the *Deception* panel and enter appropriate authentication (PIN). Figure A-85 shows the results of these actions.



Figure A-85. Location of Default Deception File for This Laptop

- In Windows Explorer, browse to the location of the *passwords.xls* default *Deception* file (C:\Users\RCAT\Documents\passwords.xls).
- Try to open the honeypot file by double-clicking on *passwords.xls* in Windows Explorer.



Figure A-86. Honeypot File in Explorer

• The attempt to open the honeypot file triggers *ActiveLock* and the alarms shown in Figure A-87.

| S. Her | 10.1 ····· |
|--|---|
| <u>F</u> | - |
| 1000 | All ALL THE ALL AND A |
| | |
| 1 | |
| 0 | Deception Nexpricer data and retrain deceptions to add attackers in the act |
| S Derbort | Fails Deceptions |
| Pile Type Phalentine | ID AM a Deceptor Rei ID Inde AD |
| Cottac Protection | Cliner/IO/T0cometh/peevonb.ds |
| Concer Down | C Creation St Dataset and Street and the |
| La barrente | Hermonic Deception Les notes ance with Droch to name in the archive and |
| La contra c | |
| A. conten | |
| - | |
| O failings | |
| D Literate | |
| C types | |
| • +0-+1 | |
| B Dart 18 | In the second seco |
| 0 | Threats Detected (1 of 1) |
| Centered . | Parts Deception Count |
| The Type Protection | · ···································· |
| Follor Protection | · • • • |
| Decum Trees | The Trave Protection Faller Protection |
| R months | Nerved Uter Sec. 1. Sec. 1. March 1. Sec. 1. March 1. Sec. 1. |
| 🖉 Annostin Tarap | |
| d beater | • • • • • |
| 0.1000 Atr | Networks Winnersteiner Hereinersteiner Hereinersteiner |
| O Settings | |
| Q | |
| (Prome | |
| 0 | |
| · internet lagent | Open CR (2014 & 2023 Open Technology, Sec. |

Figure A-87. D3E Reaction to File Deception Event

• When *ActiveLock* is engaged, it is not possible to open files with *Dynamic* protection unless the administrator uses an appropriate authentication method to clear the alert. Try to open *InternalMemos.txt*. See Figure A-88.

| CompanyInternal | | | * | | MM228134-PC | _ @ × 🖊 |
|---|---|--------------------|---------------|--------|-------------|---------|
| 🕤 🕞 - MM228134-PC 32 | bit + Local Disk (C:) + Users + RCAT + My Documents | CompanyInternal | | | | |
| Organize 💌 Include in library 💌 | Share with 👻 New folder | | | | | |
| 🔛 Recent Places 💻 | T Name - | Date modified | Туре | Sce | | |
| 🧊 Ubraries | cr2e047.pdf | 3/18/2019 12:59 PM | PD# Ne | 560 KB | | |
| Documents | Form 2464 - Annual Franchisor Cert.pdf | 3/18/2019 12:59 PM | PDF File | 217 KB | | |
| Music | internalMemos | 8/6/2019 3:51 PM | Text Document | 1 KB | | |
| Notures | Ransonware_Trifold_e-version.pdf | 8/6/2019 3:41 PM | PDF File | 803 KB | | |
| 🗑 Woleos | | | | | | |
| Hel2005HPC 3258 Gont Call (C) Fold: Fold: Gont Call (C) Gon | | | | | | |

Figure A-88. Attempt to Open File with Dynamic Protection

• Note that D3E prompts the administrator to use authentication. See Figure A-89. Entering the correct PIN allows access to the file and clears the *ActiveLock* status.

| | | | | | * | MM220154.PC _ # X | |
|--|---|---|-----------------------|----------|--------|-------------------|----------------------------|
| | C • M452813 | 6 PC 32 bit + Local Dbk (Cr) + Users + RCAT + My Docume | nts + ConpanyOnternal | | | | i 🐨 🔍 🔝 |
| | panice * 💽 Open * | Share with * Print new folder | | | | | iii • 0 |
| Lawrence and a subset of call | 1 Recent Places | ≜ F Name - | Date modified | Type | See | | |
| | a designed as | 0/20047.pdf | 3/18/2019 12:59 PM | PDF File | 560 80 | | |
| | Concents | Form 2464 - Annual Franchisor Cert.pdf | 3/18/2019 12/59 PM | FOF File | 217 68 | | |
| | Intitled - Netepad | | | | | | |
| | Edit Format View H | dp. | | | | | |
| Generatives P Protein P Protein | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Generatives P Addorfer P Add | | | | | | | |
| Autore | | | | | | | |
| Concentrate Concentra | | | | | | | |
| Cessestimut P Prior P Prior P Athone P Ath | | | | | | | |
| Author | | | | | | | |
| A December of the former | | | | | | | |
| Cessestimut P Addonée P Addonée | | | | | | | |
| Autor A | | | | | | | |
| Production and a state of the state of | | | | | | | |
| Conscience: P Addonées P Add | | | | | | | |
| Comparison C | | | | | | | |
| Constanting Constanti | | | | | | | |
| Seventimet 9 Photos 9 Ph | | | | | | | |
| Augustation Augustati | | | | | | | |
| Consistent of the second | | | | | | | |
| For Addance For Addan | | | | | | | |
| Autor A | Company Inter | na | | | | | |
| te febre te actives te acti | Company System | end . | | | | | |
| A status Parada A accluster The product of the constant of | Company Inte Highly Confide Phy Pluse | nul. | | | | | |
| sector | Company Seta Highly Condus Phy Physic Phy Physic | nd i | | | | | |
| Annolations and a solution (1) in the research (solution (1)) | Company bris Highly Coulds Prip Music Prip Pluzes Prip Valees | nd I | | | | | |
| Andhore A | Company Shite Highly Coulde Phy Phare Phy Phare Phy Phares Phy Velaces Saved Games | nd | | | | | |
| <pre>c end/system = in access c end/system = in access percentance (source) system = in access</pre> | Companyanta Highly/Confide Phy Nuac Phy Phytawas Phy Valence Searches Searches | nd | | | | | |
| Cardital and Annual Annua | Company bits Highly Contide Phy Nusc Phy Nusc Phy Valence Saved Galance Saved Galance Mindees | He I | | | | | Kuthote |
| Concisional Section 20 | Company John Highly Coulded Phy Nazes Phy Pictures Served Games Physics Served Games Physics A en IICA1 (JUPP) | neal | | | | | S Authorite |
| Thermalities Date worked (MUXTP 35) PM Determanded (MUXTP 35) PM Technology 10 (MUXTP | Company Series Program Constant Program Constant Program Constant Program Constant Series Constant Series Constant Series Constant Series Constant | nd . | | | | | € Autorite Reviews □ |
| International pre-ended (00/007933) PM Dee-overad (00/00793) PM Dee-overad (00/007933) PM Dee-overad (00/00793) PM Dee-overad (00/007933) PM Dee-overad (00/007933) PM Dee-overad (00/007933) PM Dee-overad (00/00793) PM Dee-overad (00/007933) PM Dee-overad (00/007933) PM Dee-overad (00/00793) | Company Intel Triply Could Pry Nucle Pry Nucle Pry Veloci Served Games Previous Medides A con RCA1 OUPP C con RCA1 OUPP | nd i | | | | | S Authorize C |
| Text Counset Sex 327 bess | Company Shin Heijihi, Chinda Heijihi, Chinda Heijihi, Chinda Heijihi, Chinda Services Heidens | | | | | | € Authorite File Access |
| | Company Setti Inspire Curified In Pri Nuc In Pri P Patanes In Pri Videns Inserted Gamer Secret Gamer Secret Gamer Can ICCA1 OUP Can ICCA1 OUP | ne | Jacov 2.51 per | | | | Anthone File Access |



A.3.3.2 Win7 32-Bit Evaluation

- D3E's *Deception Files* feature performed as advertised on MITRE's Win7 32-bit laptop. We did, however, notice some anomalous behavior⁴³. Cigent is investigating the anomalous *Deception*-file behavior.
 - Although attempts to open <u>user-created</u> *Deception* files triggered the appropriate response, it was possible to delete those files from within Windows Explorer. The files also could be moved to another location and subsequently opened and edited.
 - While it was not possible to permanently delete the <u>system-generated</u> <u>passwords.xls</u> file, that file also could be moved and subsequently opened/edited. We moved the system-generated *Deception* file from the *Documents* folder to the Desktop prior to opening. We then edited the file and copied it back to its original honeypot location. See Figure A-90, which displays the new contents of the system-generated *passwords.xls* file.

⁴³ The anomalies cited here also were encountered on the SSD-equipped Cigent Win10 64-bit laptop and on the MITRE Win7 64-bit laptop.

| passwords.xls - Notepad | | range 🔏 Cut | | | × | |
|-----------------------------|-------|---------------|---------|-------|---|------|
| File Edit Format View Help | | | | | | ken: |
| New stuff | | | | | 1 | ~ |
| | | | | | | nt |
| | | | | | | |
| | | | | | | |
| | | | | | | L |
| | | | | | | h |
| | | | | | | / |
| < | | | | | > | |
| Ln 1, Col 1 | 10 | 00% Windows (| CRLF) U | ITF-8 | | |
| CTI WINZIP SSD_20210 SSI | 📕 Kei | ersecret | | | | |

Figure A-90. Default Honeypot File after Editing and Return to Original Location

A.3.3.3 Win7 64-Bit Evaluation

• D3E's *Deception Files* feature performed as advertised on MITRE's Win7 64-bit laptop. The anomalies cited above were seen on this machine, as well.

A.3.4 Windows Defender Integration

The evaluation steps below were performed on the two MITRE Win7 laptops. They mirror the steps conducted in Section A.1.4 for the Cigent SSD-equipped laptop.

The subsections below evaluate D3E's integration with Windows' AV protection.

A.3.4.1 Evaluation Steps for Antivirus Integration

- At the D3E Dashboard Settings screen, make sure that *Trigger Active Lock if your Antivirus becomes disabled* is turned on. If it's not enabled, push the slider to the right and enter the appropriate authentication. (See Figure A-31.)
- As soon as this feature was enabled at the MITRE Win7 32-bit and 64-bit laptops, D3E triggered *ActiveLock*. See Figure A-91. There was no need to disable the host's AV software, because that software had not been installed. See Figure A-92. (To display the screen shown in Figure A-92, type "antivirus" at the search window and select "*Review your computer's status and resolve issues*." See Figure A-93.)



Figure A-91. Lack of AV Protection Triggers ActiveLock

| la. | | | |
|---|---|--|-----------------|
| Center Action Center | | | _ 0 × |
| Control Panel + All | Control Panel Items Action Center | | 👻 🔯 Search Co 😥 |
| Control Panel Home Change Action Center settings | Review recent messages and resolve problems Action Center has detected one or more issues for you to review. | | @_ |
| Change User Account Control settings | Security | • | |
| View performance information | Spyware and unwanted software protection (Important) Windows Defender is out of date. | Update now | |
| | Turn off messages about spyware and related protection | Get a different antispyware program online | |
| | Virus protection (Important) Windows did not find antivirus software on this computer. Turn off messages about virus protection | Find a program online | |
| | Windows Update (Important) Windows Update is not set up for this computer. Turn off messages about Windows Update | Change settings | |
| | Maintenance | • | |
| See also Backup and Restore | Set up backup Your files are not being backed up. Turn off messages about Windows Backup | 😚 Set up backup | _ |
| Windows Update Windows Program Compatibility Troubleshooter | If you don't see your problem listed, try one of these: | | |

Figure A-92. AV Protection Missing from Win7 Host

| My Documents | | |
|--|--|----------------|
| | bit ▼ Local Disk (C:) ▼ Users ▼ RCAT ▼ M | 4y Documents 👻 |
| Organize 👻 Include in library 👻 | Share with 🔻 New folder | |
| ★ Favorites ■ Desktop > Downloads > Recent Places > Libraries > Documents > Music > Pictures | CompanyInternal CompanyInternal HighlyConfidential | |
| Videos MM228134-PC 32 bit Local Disk (C:) Cigent Coced Coced | | |
| Control Panel (3) Review your computer's status a Check security status Scan for spyware and other potr | and resolve issues entially unwanted software | |
| ♀ See more results | | |
| antivirus | 🔀 Log off 🕨 | |
| Start 🔗 [] 🖸 | | |

Figure A-93. Review the PC's Security Status

- The lack of AV protection on the host triggered *ActiveLock*. Ensure that it's not possible to access files with *Dynamic* protection when *ActiveLock* is engaged.
 - Repeat steps from the *Deception* Files evaluation and try to access the *InternalMemos.txt* file. Ensure that D3E yields results identical to those encountered in the *Deception* test. See Figure A-94.

| | 1 | | MA228135 PC _ | õ x | \$ 🗰 📢 🏦 🕺 📱 |
|---------------------|----------------------------|--------------------|---|---|--------------------------|
| ROAT USER Del_E7470 | old cigent builds et al | Cigent DOE | | | |
| UREBed - Notestal | | 0 | Folder Protection | | |
| | | | Ic Protection Folders name patients folder only require authentication to acces a Dynamic Protection Folder | is when ActivaLack is on | |
| | | | Companyinternal A silvers x D'AL x McDonments x Companyinternal | * (1) Sauth (2) (1) | |
| | | | Constant a Constant a State with a first from Inform | | |
| | | Settings | Constant Constan | Detection of the provided set of the provided | |
| | | C Update | Prett.op Program Files SOFFWARE | | K Authorize Kile Access |
| | | ActiveLock Engaged | InternalMerrinas Date noodfied Sky(2021 10/51 AM Date oread Text Document Sizer 327 bytes | ed: 0/62019 3/51 PM | Enter PDV |
| | | | | | Enter your PIN |

Figure A-94. Cannot Access File with Dynamic Protection in ActiveLock State

- Return D3E settings to their original status and turn off the ActiveLock condition.
 - Go to the D3E Dashboard's *Settings* menu and deactivate the *Trigger Active Lock if your Antivirus becomes disabled* setting. Push the slider to the left and use the appropriate authentication.

A.3.4.2 Win7 32-Bit Evaluation

• D3E's *Windows Defender Integration* feature performed as advertised on MITRE's Win7 32-bit laptop.

A.3.4.3 Win7 64-Bit Evaluation

• D3E's *Windows Defender Integration* feature performed as advertised on MITRE's Win7 64-bit laptop.

A.3.5 Network Manager

The evaluation steps below were performed on the two MITRE Win7 laptops. They repeat those executed in Section A.1.5 for the Cigent SSD-equipped laptop and demonstrate D3E's response to attempts by unauthorized devices to access the D3E-protected host.

A.3.5.1 D3E Response to Untrusted Network Connections

- Untrust the current network to simulate the effects of connecting the D3E-protected host to an untrusted network.
 - Select *Networks* at the D3 Dashboard.
 - Click on a trusted network.
 - Click the **Untrust** button. Refer to Figure A-95.

| Cigent D3E | |
|----------------------|--|
| | Networks Manage the trust level of networks you connect |
| Dashboard | Manage Known Networks |
| File Type Protection | rerve.mitre.org |
| Folder Protection | Details Untrust |
| Secure Drives | |
| L Networks | |



• *ActiveLock* is engaged. Refer to Figure A-96.

| 🍕 Cigent D3E | |
|----------------------|---|
| • | Networks Manage the trust level of networks you connect |
| Dashboard | Manage Known Networks |
| File Type Protection | reve.mitre.org |
| Folder Protection | Details |
| Secure Drives | |
| ☐ Networks | |
| Removable Storage | |
| J Deception | |
| Real Authentication | |
| 🗱 Settings | |
| ActiveLock Engaged | Cigent D ³ E v2.4.4 Constraints Detected object of threads Detected object of the set of |

Figure A-96. Untrusted Network Connection Triggers ActiveLock

- Show that files with *Dynamic* protection cannot be opened under *ActiveLock* condition.
 - Attempt to open *InternalMemos.txt* while D3E is in *ActiveLock*. See Figure A-97.



Figure A-97. Attempt to Open File with Dynamic Protection

 D3E Requires Authentication to Open file, as shown in Figure A-98 and Figure A-99.



Figure A-98. Enter Authentication to Open Protected File



Figure A-99. File Opens with Authentication

• Clicking **Untrust** also causes the network connection to drop. To clear the *ActiveLock* condition and restore the network connection, return to the *Networks*

page at the D3E Dashboard, click **Trust** for the network you previously untrusted, and use the prescribed authentication method. Refer to Figure A-100 and Figure A-101.

| 🍕 Cigent D3E | | | |
|----------------------|--|------------------|-------|
| 0 | Networks Manage the trust level of networks you connect | | |
| Dashboard | Manage Known Networks | | |
| File Type Protection | 🛜 nerve.mitre.org | | |
| Folder Protection | Details | | Trust |
| Secure Drives | | | |
| D Networks | | | |
| Removable Storage | | | |
| J Deception | | 🏅 Trust Network | |
| Authentication | | • | |
| Settings | | Enter PIN | |
| ActiveLock Engaged | Cigent D ³ E | V2 Enter your PI | N |

Figure A-100. Return to Original Network Trust Status



Figure A-101. In Network We Trust

A.3.5.2 D3E Response to Port-Scanning Attempts

• Before starting the network-scanning evaluation, go to the D3E *Deception* menu and make sure *Network Deception* is turned on.



Figure A-102. Make Sure Network Deception is Active

Note that separate scanning applications were used for the 32-bit and 64-bit Win7 laptops.

- To perform the network-scanning evaluation, we used a port-scanning program provided by Cigent. That file is included on the laptop, as described below and shown in Figure A-103.
 - The desktop of the evaluation laptop contains a folder called **NEW BUILD_GUIDE FOR 2.4.4.** Open the folder.
 - Next, open the folder called *16 April Cigent Stuff for hard drive and laptops*.
 - For the Win7 64-bit laptop, click on the *EvaluationKitAuxFiles.zip* folder, within which you'll see *network_recon_local_only.zip*. Unzip that file. We will use *network_recon_local_only.exe* to scan network ports of the 64-bit laptop.
 - For the Win7 32-bit laptop, use the *local-netscan-32.exe* file contained within the *16 April Cigent Stuff for hard drive and laptops* folder.

| NEW BUILD_GUIDE FOR 2.4.4 | | | | | _ 0 |
|---|---------------------|---|--------------------------|-------------------|------------------------------|
| NEW BUILD_GUIDE FOR 2.4. | 4 • | | | | Search N |
| Organize 👻 Include in library 👻 Share wi | th 🔻 Ne | w folder | | |)= • 🔳 🖲 |
| 🔆 Favorites | - | Name ^ | Date modified | Туре | Size |
| Nesktop | | 16 April Cigent Stuff for hard drive and la | . 4/19/2021 10:03 AM | File folder | |
| Downloads Recent Places | | 606b102aaf2d3e68cd99219c_Cigent_D3 | . 4/16/2021 10:50 AM | PDF File | 8,555 KB |
| 16 April Cigent Stuff for hard drive and la | ptops 4 + 16 Apr | I Cigent Stuff for hard drive and laptops 🔹 | | | - 🗆 |
| Organize • Include in library • Share wi | th 🕶 Ne | w folder | | |)= • 🔟 🖲 |
| 🔆 Favorites | - | Name ^ | Date modified | Туре | Size |
| 🧮 Desktop | | Setup Guide 2.0.x for version 2.4.4 code | 4/19/2021 10:03 AM | File folder | |
| bownloads | | 퉬 v2.4.4 software | 4/19/2021 10:03 AM | File folder | |
| Mecent Maces | | EvaluationKitAuxFiles (3) | 4/16/2021 11:42 AM | Compressed (zippe | 18,743 KB |
| EvaluationKitAuxFiles (3) | | | | | _ 0 |
| GOO IN . NEW BUILD_GUIDE FOR 2.4 | .4 🕶 16 Apr | il Cigent Stuff for hard drive and laptops 👻 Evaluation | KitAuxFiles (3) | | 👻 🛃 Search E |
| Organize 🔻 Extract all files | | | | | 8= • 🖬 🔞 |
| 🗉 🔆 Favorites | - | Name - Ty | pe | Compressed size | Password p Size |
| E Desktop | | CompanyInternal Co | mpressed (zipped) Folder | 1,306 KE | 3 No |
| | | HighlyConfidential Co | mpressed (zipped) Folder | 16,149 KE | 3 No |
| Downloads | | | | | |

Figure A-103. Locate the Port-Scanning File on the Desktop

- Copy *network_recon_local_only.exe* (<u>or *local-netscan-32.exe* for</u> <u>the 32-bit machine</u>) to C:\ directory. (The file can be run from anywhere; we chose that location arbitrarily.)
- Open a command prompt; set the current directory to C:\; then run the attack script. Refer to Figure A-104 and Figure A-105.
 - Note that the script attacks ports 21, 3389, 445, 139, and 135. These ports are used for File Transfer Protocol (FTP), Remote Desktop Protocol (RDP), Transmission Control Protocol (TCP), Server Message Block (SMB), and Remote Procedure Call (RPC), respectively.

| C:\>dir | | | |
|-------------|--------------|--------------|------------------------------------|
| Volume in | drive C has | no label | |
| Volume Ser | ial Number | is 7657-FF8 | 2 |
| VOLUME SET | | 13 7037 220. | |
| Directory | of C:\ | | |
| í í | | | |
| 09/15/2020 | 09:46 AM | <dir></dir> | AlwaysOn |
| 04/13/2021 | 03:16 PM | <dir></dir> | Backup |
| 09/15/2020 | 09:49 AM | <dir></dir> | Dynamic |
| 08/01/2020 | 08:32 AM | <dir></dir> | Intel |
| 08/20/2019 | 11:13 AM | 2,64 | 8,576 network_recon_local_only.exe |
| 08/01/2020 | 08:51 AM | <dir></dir> | PerfLogs |
| 04/19/2021 | 10:10 AM | <dir></dir> | Program Files |
| 08/01/2020 | 08:32 AM | <dir></dir> | Program Files (x86) |
| 09/14/2020 | 02:18 PM | <dir></dir> | Share |
| 08/01/2020 | 08:25 AM | <dir></dir> | Users |
| 04/19/2021 | 09:56 AM | <dir></dir> | Windows |
| | 1 File(| s) 2,6 | 48,576 bytes |
| | 10 Dir(s |) 94,684,7 | 78,496 bytes free |
| | | | |
| C+\\network | r recon loca | l only eve | |

Figure A-104. Run the Attack Script

| G. C:\Windows\system32\cmd.exe | _ 0 |
|---|-----|
| Directory of C:\ | |
| 04/28/2021 10:28 AM (DIR) AlwaysOn supersensitive 05/04/2021 08:41 AM (DIR) Cigent 08/20/2019 11:13 AM 2,648,576 network_recon_local_only.exe 09/13/2009 11:20 PM (DIR) Perflogs 09/13/2019 01:59 PM (DIR) Program Files 03/23/2021 09:33 AM (DIR) Program Files 03/23/2021 09:19 AM (DIR) SOFTWARE 03/23/2021 10:48 AM (DIR) Users 05/10/2021 10:48 AM (DIR) Users 05/10/2021 01:52 PM (DIR) Users 05/10/2021 01:62 PM (DIR) Users 05/10/2021 01:62 PM (DIR) Users 05/10/2021 01:62 PM 216.948,576 bytes 1 File(s) 2.648,576 bytes 9 | |
| C:\>network_recon_local_only.exe Starting Alpha RECOM IP: 10.206.161.198 Recon Report for host: 10.206.161.198 Boom - Open port: 21 Boom - Open port: 3389 Boom - Open port: 445 Boom - Open port: 139 Boom - Open port: 135 | |

Figure A-105. Execution of Port-Scan Attack Script

- D3E's reaction to the *Network Deception* is shown in Figure A-106.
 - *ActiveLock* is engaged.
 - The D3E icon turns red.

• You are prompted to enter authentication to clear the threat.



Figure A-106. D3E Reaction to Port Scan

• For completeness, after initiating port scanning, we attempted to open a file that had been assigned *Dynamic* protection. D3E appropriately protected the file and prompted the administrator to enter authentication. See Figure A-107.





- Go to the Security Status tab and enter a PIN to clear the test threat.
 - *ActiveLock* is now disengaged, as shown in Figure A-108.

| 💐 Cigent D3E | | | - 🗆 × |
|-------------------------------|--|---|--------------------------------|
| Dashboard | Standing Guar We are looking out for yo | d ur sensitive data | |
| File Type Protection | S | © | ۵ ۲ |
| Folder Protection | File Type Protection | Folder Protection | Secure Drives |
| Secure Drives | Custom | 4 Always On folders 1 Dynamic folder | CTI SSD: DP: CTI SSD: DH: |
| Removable Storage | S | | O |
| Deception | 모 | o | J |
| | Networks nerve.mitre.org Trusted | Removable Storage New (1) Trusted (1) | Deception 2 deception files |
| Authentication | | | |

Figure A-108. ActiveLock Disengaged

A.3.5.3 Win7 32-Bit Evaluation

- The "untrust" portion of the *Network Manager* evaluation performed well and as expected on the MITRE Win7 32-bit laptop.
- Results of the network-scanning evaluation on the MITRE Win7 32-bit laptop went well.

A.3.5.4 Win7 64-Bit Evaluation

- The "untrust" portion of the *Network Manager* evaluation performed well and as expected on the MITRE Win7 64-bit laptop.
- The network-scanning evaluation went well and as expected on the MITRE Win7 64-bit machine.

A.3.6 File Extension Protection

In addition to the drive/partition and folder protection documented earlier, D3E also lets administrators assign *Always On* and *Dynamic* protection to files based on the files' extension. This feature was added to D3E to spare administrators from having to reorganize files into designated protection folders. Instead, global protection is given to files with the designated extension(s), regardless of their location within the PC's directories. Cigent cautions that, because this protection-assignment method is global, it could have unintended consequences. Cigent advises users to "implement File Extension protection on files that are used only for a particular application, for example, PDF" [8]. Section A.3.6.2 examines in more detail the potential for conflict between *Folder Protection* and *File Extension Protection*.

The *File Extension Protection* demonstration was conducted on all three evaluation laptops. Following reference [8], we opted to assign *Always On* protection to files with *.pdf* extension and *Dynamic* protection to files with *.txt* extensions. Prior to starting the exercise, we removed existing folder protections, so that the effects of *File Extension Protection* would not be masked.

A.3.6.1 Evaluation Steps for File Extension Protection

Execute the following steps on all three evaluation laptops.

- Remove Folder Protection.
 - Click the *Folder Protection* menu at the D3E Dashboard.



Figure A-109. Folder Protection Menu [8]

• Remove *Folder Protection* by selecting the folder and then clicking the **Remove** button. Use the prescribed authentication method to enact the removal. Repeat this step for each *Dynamic* and *Always On* folder. Refer to Figure A-110.

| Folder Protection Protect files by folder location Protect files by folder location Protection Protection < | Cigent D3E | |
|---|----------------------|---|
| Protect files by folder location II Dashboard Dynamic Protection Folders IF ler Type Protection I Add a Dynamic Protection Folder IF her Type Protection I Add a Dynamic Protection Folder IF folder Protection I C:\Users\dave\Documents IF her Type Protection I C:\Users\dave\Documents | | Folder Protection |
| Image: Dashbaard Dynamic Protection Folders File: Type Protection File: n Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folder Image: Add a Dynamic Protection Folders Image: Add a Dynamic Protection Folders Image: Add a Dynamic Protection Folders Image: Add a Dynamic Protection Folders Image: Add a Dynamic Protection Folders Image: Add a Dynamic Protection Folders Image: Add an Always On Protection Folders Image: Add an Always On Protection Folder Image: Add an Always On Protection Folders Image: Add an Always On Protection Folder Image: Add an Always On Protection Folders Image: Add an Always On Protection Folder Image: Add an Always On Protection Folders Image: Add an Always On Protection Folder Image: Add an Always On Protection Folders Image: Add an Always On Protection Folder Image: Add an Always On Protection Folders Image: Add an Always On Protection Folder | V | Protect files by folder location |
| File Type Protection Files n Dynamic Protection Folder of main authentication to access when ActiveLock is on | Dashboard | Dynamic Protection Folders |
| ■ Folder Protection □ C:\Users\\dave\Documents ■ Secure Drives □ C:\Users\\dave\Dickures ■ Networks □ C:\Users\\dave\Dickures ● Removable Storage □ C:\Users\\dave\Dickures ③ Deception Always On Protection Folders Fits n Aways On protection Folders ■ Add an Always On Protection Folder ● Authentication □ C:\Users\User\User | File Type Protection | Files in Dynamic protection folders only require authentication to access when ActiveLock is on |
| Secure Drives C:\Users\dave\Pictures C:\Users\dave\Pictures Networks C:\Users\dave\Pictures C:\Users\dave\Pictures Deception Always On Protection Folders Fites n Aways On protection Folder Add an Always On Protection Folder Add an Always On Protection Folder C:\Users\Logent\HighlyConfidential Lcense C:\Users\Ligent\HighlyConfidential Update C:\Users\Ligent\HighlyConfidential C:Update C:\Users\Ligent\HighlyConfidential | Folder Protection | C:\Users\dave\Documents |
| Networks C:\Users\dave\Pictures C:\Users\dave\Pictures C:\Users\dave\Videos C:\Users\dave\Videos Always On Protection Folders Add an Always On Protection Folder C:\UsersLegent\HighlyConfidential C:\UsersLegent\HighlyConfidential C:\UsersLegent\HighlyConfidential C:\UsersLegent\HighlyConfidential Cogent PE v2.0.9 & 2020 Ogent Technology. In Cogent PE v2.0.9 & | Secure Drives | Remove |
| C:USersVideos C:USers\dave{Videos C:USers\dave{Videos C:USers\dave{Videos C:USers\dave{Videos C:USers\dave{Videos Advays On Protection Folder Advays On Protection Folder Add an Always On Protection Folder Add an Always On Protection Folder C:USers\HighlyConfidential C:USers C:USers\HighlyConfidential C:USers C:USERCERS C:USERCERS C:USERS C:USERCERS C:USERCERS C:USERCERS C:USERCERS | Q Networks | C:\Users\dave\Pictures |
| Image: C_C_Gent\CompanyInternal Image: Deception Always On Protection Folders Fless in Always On protection Folders Image: Authentication Image: Authentication Image: Authentication Image: C_C_Gent\HighlyConfidential Image: C_C_C_Gent\HighlyConfidential Image: C_C_C_C_Gent\HighlyConfidential Image: C_C_C_C_C_C_C_C_C_C_C_C_C_C_C_C_C_C_C_ | + | C:\Users\dave\Videos |
| Deception Always On Protection Folders Files in Navays On protection Folders Add an Always On Protection Folder Add an Always On Protection Folder Add an Always On Protection Folder C:\Gigent\HighlyConfidential C:\Gigent\HighlyConf | Removable Storage | C:\Cigent\CompanyInternal |
| Auways on Protection Folders Here Navays On Protection Folders Add an Always On Protection Folder Add an Always On Protection Folder Authentication C:\Cigent\HighlyConfidential C:\Cigent\HighlyConfidential C:\Cigent\HighlyConfidential About Cogent DF: v2.0.0 © 2020 Opent Technology. In Cogent DF: v2.0.0 © 2020 Opent Technology. In Enter PM | of Deception | |
| Add an Always On Protection Folder Authentication C:\Ggent\HighlyConfidential | | Always On Protection Folders Files in Always On protection folders always require authentication to access |
| Authentication C:\Gigent\HighlyConfidential Settings C:\Gigent\HighlyConfidential C:\Gigent | | Add an Always On Protection Folder |
| Setings Loense Othote About Copent DPE v2.0.9 © 2020 Opent Technology, In Copent DPE v2.0.9 © 2020 Opent Technology, In Enter PN Enter PN | Authentication | C:\Cigent\HighlyConfidential |
| Cipent D'E v2.0.0 C 2020 Cipent Technology, In Cipent D'E v2.0 C 2020 Cipent Technology, In C | Settings | |
| C Update About Cgent D*E v2.0.9 © 2020 Ggent Technology, In Cgent | () License | |
| About Cigent D*E v2.0.9 © 2020 Ogent Technology, In Cigent D*E v2.0.9 © 2020 Ogent | C Update | |
| Cgent D ^{re} v2.8.9 © 2020 Cgent Technology. In Modify Folder Protection Enter PM | About | |
| Kontexton Enter PN | | Cigent D ^a E v2.0.9 © 2020 Cigent Technology, In |
| Enter PIN | | K Modify Folder |
| | | Enter PIN |

Figure A-110. Remove Folder Protection [8]

• At the conclusion of the previous step, the *Folder Protection* menu should look like Figure A-111 below. In other words, no *Folder Protection* should be assigned.



Figure A-111. No Folder Protection Assigned [8]

• Assign File Extension Protection

Full *Always On* or *Dynamic* protection may be assigned to Microsoft Office files, as well as to Adobe files. In addition, D3E lets administrators customize the *File Extension Protection* feature by designating other file extensions for protection.

In this exercise, we assign *Always On* protection to files with a .pdf extension, and *Dynamic* protection to files with .txt extension.

• Select the *File Type Protection* menu at the D3E Dashboard.



Figure A-112. File Type Protection Menu [8]

- o Click Adobe Files.
 - It may be necessary to enable the *Allow Always On File Extension* feature at the Dashboard's *Settings* screen. If the message "Enable 'Allow Always On File Extension' option to add Always On extensions" appears at the top of the Adobe Files screen (as shown in Figure A-113), simply enable the feature at the *Settings* screen.
 - Move the slider to the right and use the prescribed authentication. See Figure A-114.

| Cigent D3E | | |
|------------------------------------|--|---|
| I | Return to File Type Protection Adobe Files | |
| Dashboard Eile Type Protection | Enable 'Allow Always On File Extension' o Acrobat | ▶ pption to add Always On extensions. |
| Folder Protection | pdf Photoshop | None Dynamic Always On |
| Secure Drives | abr | None Dynamic Always On |
| L Networks | csh | None Dynamic Always On |
| 🔗 Removable Storage | psb | None Dynamic Always On |
| of Deception | psd | None Dynamic Always On |
| | u3d | None Dynamic Always On |
| Authentication | Photoshop Elements | |
| Settings | pse | None Dynamic Always On |
| License | Illu strator ai | None Dynamic Always On |
| C Update | Premiere | |
| (i) About | prproi | None Dynamic Always On |
|] | | Cigent D ³ E v2.4.4 © 2021 Cigent Technology, Inc. |

Figure A-113. Allow Always On File Extension Must Be Enabled



Figure A-114. Enabling Always On File Protection

 After Always On File Protection has been enabled, clicking Adobe Files will display the screen shown in Figure A-115 below.

| Cigent D3E | | | | 00 | |
|----------------------|--|-----------|--------------|-----------------|------|
| | Return to File Type Protection | | | | |
| v | Adobe Files | | | | |
| Dashboard | Acrobat | | | | |
| File Type Protection | pdf | None | Dynamic | Always On | |
| Folder Protection | Photoshop | | | | |
| Secure Drives | abr | None | Dynamic | Always On | |
| Networks | csh | None | Dynamic | Alwayrs On | |
| 🔗 Removable Storage | psb | None | Dynamic | Always On | |
| of Deception | psd | None | Dynamic | Always On | |
| | u3d | None | Dynamic | Always On | |
| | Photoshop Elements | | | | |
| Authentication | pse | None | Dynamic | Always On | |
| Settings | Illustrator | | | | |
| License | ai | None | Dynamic | Always On | |
| C Update | Premiere | | | | |
| () About | prproj | None | Dynamic | Alwayrs On | |
| | | Casak DIF | 0.0.0.0.2020 | Gaaab Tashaalaa | . In |

Figure A-115. Setup Screen for Adobe File Protection

- Note that multiple Adobe file-extension types may be assigned D3E protection. For this exercise, select *Always On* protection for PDF files, as shown in Figure A-116.
 - Click the **Save** button.
 - Then use the prescribed authentication method to enact your selection.

| Cigent D3E | | | |
|----------------------|--|------------------------------------|-----------------------------|
| | Return to File Type Protection | | |
| | Adobe Files | | Save Cancel |
| - | | | ^ |
| Dashboard | Acrobat | | |
| File Type Protection | pdf | None Dyna | mic Always On |
| Folder Protection | Photoshop | | |
| Secure Drives | abr | None Dyna | mic Always On |
| Networks | csh | None Dyna | mic Always On |
| Y Networks | psb | None Dyna | mic Always On |
| Removable Storage | psd | None Dyna | mic Always On |
| J Deception | u3d | None Dyna | mic Always On |
| | Photoshop Elements | | |
| Authentication | pse | None Dyna | mic Always On |
| - | Illustrator | | |
| Settings | ai | None Dyna | mic Always On |
| Dicense | | | |
| C Undata | Premiere | | |
| O opuace | prproj | None Dyna | mic Always On |
| About | | | ~ |
| | | Cigent D ^a E v2.0.9 © 2 | 020 Cigent Technology, Inc. |

Figure A-116. Choose Protection Type for PDF Files

Click on return to File Type Protection at the top of the screen to display the screen below.

| Cigent D3E | | - | × |
|----------------------|--|---|---|
| V | File Type Protection Protect files by type, across all drives | | |
| Dashboard | Microsoft Office Files | | |
| File Type Protection | No protection | | |
| Folder Protection | Adobe Files < Partally protected | | |
| Secure Drives | Custom 🤡 | | |
| L Networks | Fully protected | | |

Figure A-117. Adobe Files Partially Protected

- Note that Adobe Files are marked "Partially protected." This reflects the fact that PDF files have been given D3E protection, but other Adobe file types have not been assigned protection.
- Click *Custom* to display the screen shown in Figure A-118 below.

| Cigent D3E | | | | - 🗆 | × |
|---------------------------------|--|------|---------|-----------|---|
| | Return to File Type Protection | | | | |
| | Custom | | | | |
| Dashboard | | | | | |
| File Type Protection | cad | None | Dynamic | Always On | |
| Folder Protection | | | | | |
| Secure Drives | | | | | |
| L Networks | | | | | |
| Nemovable Storage | | | | | |
| of Deception | | | | | |
| ♂ Removable Storage ⑦ Deception | | | | | |

Figure A-118. Custom File Type Protection

- Note that, if text files are not listed in the Custom File Extension list, we'll have to add the .txt extension.
 - Click Add File Type to display the screen shown in Figure A-119
 - Type *txt* in the space provided.
 - Make sure *Dynamic* protection is assigned.
 - Click Save.
 - Use the prescribed authentication method.
 - Click on Return to File Type Protection at the top of the screen.

| Cigent D3E | | - 🗆 X |
|----------------------|--|------------------------|
| | Return to File Type Protection | |
| | Custom | Save Cancel |
| Dashboard | ⊕ Add File Type | |
| File Type Protection | txt | None Dynamic Always On |
| Folder Protection | | Remove |
| Secure Drives | cad | None Dynamic Always On |
| ➡ Networks | | |
| Removable Storage | | |
| J Deception | | |



• Test File Extension Protection for PDF extensions.

Files with pdf extensions have just been given *Always On* protection, so authentication should be required to access the information in the file, regardless of the *ActiveLock* status.

- Browse to C:\Cigent\HighlyConfidential. (Actually, any path to a pdf file will work.)
- Click on *fw4.pdf* (or any other pdf file on the laptop) to open the file.
- Note that authentication is required to open this file. See Figure A-120.

| ă di ,;; file;//C)Ggeet/he4pcl × + ∨ | H al toronation | - 6 × | - 0 |
|--------------------------------------|-----------------|-------|----------------------------|
| ← → X @ 0 files///Cigent/fin/pdf | | | 日本 本 & ビ |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | K Authorize File Access |
| | | | 0 |
| | | | Triter PIN |
| | | | Enter your PIN |

Figure A-120. Authentication Required to Open File with Always On Protection

• The contents of the file can be accessed after the appropriate authentication has been used. See Figure A-121.



Figure A-121. File Displayed After Authentication

• Test File Extension Protection for txt extensions.

Files with txt extensions have just been assigned *Dynamic* protection. Authentication should be required to access such files <u>only when *ActiveLock* is engaged</u>.

- Browse to C:\Cigent\Confidential.txt. Figure A-122 demonstrates that, when ActiveLock is not engaged, it is not necessary to use authentication to access the file.
- Demonstrate that authentication is required to access .txt files when *ActiveLock* is engaged.
 - Trigger ActiveLock by attempting to access *passwords.xls*. Ignore D3E warnings for now.
 - Try to open C:\Cigent*Confidential.txt*. Note that the file will not open until authentication has been employed. See Figure A-123 and Figure A-124.
 - At the D3E Dashboard, enter authentication to clear the *Data Deception Event* threat.
 - After clearing the threat, note that the *Confidential.txt* file opens without authentication.
| 🚺 🕑 📜 🔻 Cigent | | | | | **** | |
|---|------------------|-----------------------|-------------------------------|---|--------------|--------------------|
| File Home Share View | | | | | | ~ (|
| Image: Pin to Quick access Copy Paste Image: Copy path Pin to Quick access Paste Paste shortcut | Move Copy to to | New folder | Properties | Select all Select none Invert selection | | |
| Clipboard | Organize | New | Open | Select | | |
| \leftrightarrow \rightarrow \checkmark \Uparrow $\stackrel{]}{\longrightarrow}$ This PC \rightarrow Local Disk | (C:) → Cigent | | | ~ | ō ,≏ se | earch Cigent |
| 🐚 This PC | | ^ Name | ^ | Date m | odified | Type |
| 3D Objects | | Annual Rep | ort - draft - confidential.do | ex 8/6/201 | 9 3:52 PM | Office Open XML Do |
| A on RCAT-JUMP | | billing.xlsx | | 8/6/201 | 9 3:51 PM | XLSX File |
| C on RCAT-JUMP | | Confidentia | il.txt | 8/6/201 | 9 3:51 PM | Text Document |
| D on RCAT-JUMP | Confid | Install but . Natanad | nfa ndf | 9/32/30 | 10 10-22 DA4 | PDF File |
| Desktop | Ella Esta | Essent View Male | | | | PDF File |
| Documents | We the f | People of the Uni | ted States. in Ord | er to form a more | perfe of | PDF File |
| Downloads | | | | | | PDF File |
| Music | Cigent D3E | | | | | - 🗆 🗙 |
| Pictures | | | | | | |
| H Videos | | Ctops | ling Cuard | | | |
| 🐛 Local Disk (C:) | | Stand | ing Guard | | | |
| AlwaysOn | 1 | We are lo | oking out for your s | ensitive data | | |
| 📜 Backup | Dashboard | | | | | |
|] Cigent | | S | | | | |
| 10 items 1 item selected 327 bytes | File Type Protei | ction | | | | 2 1 |

Figure A-122. Authentication Not Needed if ActiveLock Not Engaged

| 📕 🕑 📕 🖛 Cigent | | | | | | - | 0 × | |
|-------------------------------------|------------------------------------|--------------------------------|--------------------------------|------------|-----------------|----------------------|---------------|----|
| File Home Share View | | | | | | | ~ 👩 | |
| Pinto Copiedo Copy Paste Secreto | More Copy to * to * | New Item • | Properties | Select all | | | | |
| Clipboard | Organize | New | Open | Select | | | | |
| ← → ← ↑ 🖡 > This PC > Local Disk | (C:) > Cigent | | | | ~ õ | 🥬 Search Cigent | | |
| This PC | | Name | ^ | 0 | ate modified | Type | | |
| I Untitled - Notepad | - D X | 🖹 Annual Repo | t - draft - confidential.do | α 8 | /6/2019 3:52 PI | M Office | Open XML Docu | |
| File Edit Format View Help | | billing.xlsx | | | /6/2019 3:51 Pt | VI XLSX F | le | |
| | | Confidential | xt | 8 | /6/2019 3:51 PM | M Text D | ocument | |
| | | corporate_int | o.pdf | 8 | /23/2018 10:55 | PM PDFH | e . | |
| | | twiptr | | | /18/2019 12:59 | PM PDFH | e . | |
| | | in in a cell | | 3 | /18/2019 12:59 | PM PDFFi PM PDFFi | | |
| | | Ransermaare | Prevention and Resp. off | | /M/2019 3-39 Pt | M PDE FI | | |
| | | Renormante | Executive One-Reas off | | (6/2010 3-50 04 | 4 PDF Fi | | |
| | | Sans ransome | ware.pdf | | /6/2019 3:46 Pt | M PDF Fi | le l | |
| | | | | | | | | |
| Cigent D3E | | | | | | | | |
| E Ba | | | | | | | | |
|). CK | Decention | | | | | | > | |
| 10 items | Deception | | | | | | 100 100 | |
| | Manage your data and n | etwork deceptions t | o catch attackers in | the act | | | | |
| Dashboard | | | | | | | | |
| | Data Deceptions | | | | | | Authorize | |
| File Type Protection | Create interesting looking files a | in attacker would want b le | i try to open. | Show A | | | File Access | |
| Folder Protection | 0 | and the second second | white the second second second | 6100 | | | Enter P | 9N |
| Secure Drives | D | | | | | | | |

Figure A-123. Under ActiveLock Text File Won't Open without Authentication

| Image: Second | Move Copy to Organize | New item * | Properties Qpen Properties QPen | Select all Select none Invert selection Select | | | × ^ 0 |
|---|---|--|---|---|--|--|---|
| ← → ~ ↑ 📕 → This PC → Local Disk | C:) > Cigent | | | | ~ | ð P | Search Cigent |
| Cenfidentiabet - Notepad File Edit Format Vere Halp Vere | I BORB PERFE | Name Annual Report Mining xita Confidential La Confidential La Conporte_info Mx-pdf Mx-pdf Ranscenware [sans ranscenee] | - draft - confidential.doo t t t revention and Resp.pdf Scecutive_One-Page.pdf ware.pdf | CX 8 | Date mod (/6/2019 : (/1/2021 (/18/2019 (/18/2019 (/18/2019 (/18/2019 (/6/2019 : (/6/2019 : | ified is2 PM is1 PM 9:14 AM 10:33 PM 12:39 PM 12:39 PM is39 PM is39 PM is30 PM is46 PM | Type Office Open JAM. Decu XLS: File Test Document PDF File PDF File PDF File PDF File PDF File |
| Backup | 10- | | | | | | |
| Copen Copen Copen Copen Copen Copen Co | Manage your data and n Data Deceptions Create interesting boking files Add a Deception fil D D | etwork deceptions to an attacker would want to le | catch attackers in try to open. | the act ⊙ Show A | л | | |

Figure A-124. Text File is Accessible after Authentication

• At the conclusion of this evaluation, clear *ActiveLock*, remove *File Extension Protection* for TXT files and mark PDF files for *Dynamic* protection.

A.3.6.2 Conflicts between Folder Protection and File Extension Protection

- Before we ran the *File Extension Protection* evaluation described above, we removed *Folder Protection*, so that the latter's effects would not mask the D3E's *File Extension Protection* performance. After our baseline checkout of the feature, we wanted to go back and see whether the simultaneous use of *File Extension* and *Folder* protections could lead to conflicts. (The following test was conducted only on the Win10 64-bit laptop.)
 - We marked a folder for *Dynamic* protection and made sure that the folder contained a PDF file.
 - We then assigned *Always On* protection to files with the PDF extension.
 - Finally, we tried to access the *fw4.pdf* file:
 - (1) when *ActiveLock* was engaged and
 - (2) when *ActiveLock* was not engaged.
- Evaluation steps are depicted below in Figure A-125 through Figure A-127.



Figure A-125. Folder with PDF File



Figure A-126. Mark Folder for *Dynamic* Protection

• Before turning on *File Extension Protection*, we verified (again) that *Dynamic Folder Protection* behaved appropriately under *ActiveLock* and non-*ActiveLock* conditions.

| Cigent D3E | | | | - 0 | × |
|----------------------|--|--------------|--------------|----------------|-----------|
| Ø | Return to File Type Protection Adobe Files | | | | |
| Dashboard | Acrobat | | | | ~ |
| File Type Protection | pdf | None | Dynamic | Always On | |
| Folder Protection | Photoshop Elements | | | | |
| Secure Drives | pse | None | Dynamic | Always On | |
| Networks | Illustrator | | | | |
| Removable Storage | ai | None | Dynamic | Always On | |
| Posentian | Photoshop | | | | |
| 0 Deception | abr | None | Dynamic | Always On | |
| | csh | None | Dynamic | Always On | |
| Ruthentication | psb | None | Dynamic | Always On | |
| 💠 Settings | psd | None | Dynamic | Always On | |
| License | u3d | None | Dynamic | Always On | |
| C Update | Premiere | | | | |
| () About | prproj | None | Dynamic | Always On | |
| | | Cigent DªE v | 2.4.4 © 2021 | Cigent Technol | ogy, Inc. |

Figure A-127. Always On Protection Assigned to PDF Files

- <u>With ActiveLock not engaged</u>, we tried to access the PDF file in the folder marked for *Dynamic* protection. When we tried to access the *fw4.pdf* file, we saw that the *Always On* protection assigned to the PDF file extension had precedence over the protection level assigned to the folder. This behavior does not constitute a problem, but it could be confusing to users encountering *Always On* treatment for a file in a folder marked explicitly for *Dynamic* protection. Recall Cigent's caution that "because this protection-assignment method is global, it could have unintended consequences unless care is taken" [8].
- To bolster our conclusion, we reran the test, assigning *Always On* Protection to the folder, and *Dynamic* protection to PDF files. As expected, behavior followed *Always On* rules when we tried to access the PDF file. This behavior echoes what we saw through our earlier *Always On/Dynamic* tests.

Key Takeaway: If a dual assignment of *Folder Protection* and *File Extension Protection* causes a file to be assigned both *Always On* and *Dynamic* protection, *Always On* treatment will prevail.

- Recommendations:
 - For common file extensions, such as *docx*, *pdf*, *xlsx*, and *txt*, it is preferable to segregate files needing *Always On* or *Dynamic* protection into folders marked explicitly for the desired treatment and to use D3E's *Folder Protection* feature. Use *File Extension Protection* only for less common file-extension types, and only if needed. The extra administrative steps required to collect sensitive information into separate files may be cumbersome, but it will avoid the potential confusion that could result from the *Folder/File Extension* conflict described above.

- 2. When moving sensitive information into folders for *Dynamic* or *Always On* protection, make sure that residual copies or variants of the information do not exist in unprotected folders.
- 3. MITRE believes that the addition of a new *File Name Protection* feature, supplementing *Folder* and *File Extension Protection*, would enhance the D3E product. D3E administrators should be able to build an alphabetized list of files that receive either *Always On* or *Dynamic* protection. Such an implementation would avoid the *Folder/File Extension* conflict and confusion described above.

E.g.,

| - Sensitive personnel data.docx | Dynamic Protection |
|---------------------------------|----------------------|
| - Attack plans 2021.pdf | Always On Protection |

• Use of wild-card characters would help to ensure that outdated or other variants of sensitive files receive appropriate protection.

E.g., - Sensitive personnel*.* Dynamic Protection - Attack plans 20**.* Always On Protection

A.3.6.3 Win10 Evaluation

• File Extension protection worked well on the Win10 64-bit laptop equipped with Cigent Secure SSD Drives. The feature performed as advertised.

A.3.6.4 Win7 32-Bit Evaluation

• File Extension protection worked well and as advertised on the MITRE Win7 32-bit laptop.

A.3.6.5 Win7 64-Bit Evaluation

• File Extension protection worked well and as advertised on the MITRE Win7 64-bit laptop.

A.4 Removable Storage Protection

• To evaluate D3E's *Removable Storage Protection* feature, we connected a <u>WD Elements</u> hard drive via USB cable to the three evaluation laptops sequentially, tested the drive under *Trusted* and *Untrusted* conditions, and documented how D3E protected file access.

A.4.1 Removable Storage Protection – Evaluation Steps

• The removable drive had previously been connected to the evaluation laptops and trusted. Therefore, to test storage protection, it was necessary first to untrust the device before proceeding with the test. Refer to Figure A-128 and Figure A-129.



Figure A-128. Untrust Removable Storage – Non-SSD Laptop



Figure A-129. Post Untrust of Removable Storage - Non-SSD Laptop

• After untrusting the USB drive, our attempt to access a file on the drive failed. See Figure A-130. Similarly, an attempt to copy a file to the drive failed while the drive was untrusted.



Figure A-130. Cannot Access File on Untrusted Removable Drive

• As expected, untrusting the removable device did not trigger *ActiveLock* at the laptop, and it was possible to access files not on the USB. In summary, it was possible to access files on the storage device only when the device was trusted in D3E. This behavior is entirely appropriate.

• We noticed slightly different behavior when evaluating *Removable Storage Protection* on the SSD-equipped Cigent Win10 laptop. Compare Figure A-131 below with Figure A-129 above. Note that the SSD-equipped laptop provides the option to "forget" a removable storage device after it has been untrusted. The status of the "Forgotten" USB drive is shown in Figure A-132. The next time the storage device is connected to the laptop, the user must make an explicit choice to trust the device.



Figure A-131. "Forget" Removable Device on Cigent SSD Laptop



Figure A-132. Forgotten Storage Device – SSD-Equipped Laptop

A.4.1.1 Win10 Evaluation

• *Removable Storage Protection* performed as expected on the Cigent SSD-equipped Win10 64-bit laptop, preventing access to files on an untrusted removable-storage device without affecting access to files on the laptop itself.

A.4.1.2 Win7 32-Bit Evaluation

• *Removable Storage Protection* performed appropriately on the MITRE Win7 32-bit laptop.

A.4.1.3 Win 7 64-Bit Evaluation

• *Removable Storage Protection* performed appropriately on the MITRE Win7 64-bit laptop.

Appendix B Anomalies

As we noted elsewhere in this report, our impression of the data-protection features of Cigent's Dynamic Data Defense Engine (D3E) software is favorable. Cigent's dual firmware- and software-protection approaches combine to form a strong defense against tampering and theft of sensitive data.

The D3E suite of tools is simple to use, and D3E would be particularly effective and easy to manage in a networked deployment with a centralized management console.

As is to be expected in software still under development, however, we did encounter a few instances of anomalous D3E behavior. None of these instances constitutes a "show stopper," and some may be attributable to the underlying computing environment, rather than to D3E. The perceived idiosyncrasies are catalogued here to enable the vendor to consider, explain, or fix them.

B.1 Password Reuse is Allowed

As part of the procedure for de-configuring (Section A.1.1.2) and re-configuring (Section A.1.1.3) a Cigent Secure Solid-State Drive (SSD), we were required to enter a provisioning password. D3E let us reuse the old provisioning password when we re-configured the SSD. This was convenient for the purpose of our evaluation, but DoD and other government agencies recommend more stringent practices regarding passwords and identity management.

Recommendation: We recommend that D3E consult NIST Special Publication 800-63-3 [10] and other entities, government and civilian, for guidance on constructing robust digital identities.⁴⁴ The following is a non-comprehensive list of recommended practices.

- Enforce a strict (high) *Password history* parameter value to discourage password reuse.
- Make users change passwords at frequent intervals, e.g., 90 days or less.
- Prevent passwords from being changed immediately; i.e., enforce a minimum wait time to change passwords (enforce *minimum password age*).
- At a minimum, prompt users/administrators to follows DoD guidance when creating passwords.
- Ideally, creation of login credentials should be under the oversight of a Central Administrator Console, and local users/administrators should not be able to weaken the assigned password policy.

Similar guidance should apply to creation of D3E authentication PINs, as well.

⁴⁴ Cigent response: "Cigent will add the ability for password policy enforcement for both the Secure SSD password and authentication PIN in the upcoming release. It is also worth noting that that file authentication via CAC/PIV will be supported in a near term release."

B.2 Honeypot Files Can Be Moved, Changed, and Deleted

D3E provides a system-generated *passwords.xls* honeypot (*Deception*) file to ensnare malefactors. If any user or attacker attempts to open the file in its assigned *Deception* location, D3E triggers an *ActiveLock* condition and locks all sensitive file types and folders. Under *ActiveLock*, Secure SSD drives also are locked and unmounted; i.e., they become "invisible." D3E allows the administrator to create additional *Deception* folders; when the contents of a *Deception* folder are opened, D3E triggers *ActiveLock* to protect sensitive data elsewhere on the machine. Refer to Section A.1.3 for details.

D3E satisfies its advertised *Deception* functionality, in that it detects an attacker (or any user) clicking on a honeypot file and appropriately takes action to keep designated drives, folders, and file types safe. We discovered some aspects of the feature, however, that likely are outside the scope of Cigent's intended *Deception*-file behavior.

B.2.1 Manipulation of User-Generated Honeypot Files

Although attempts to open user-created *Deception* files triggered the appropriate D3E responses, it was possible to delete those files from within Windows Explorer. The files also could be moved to another location and subsequently opened, edited, and copied back to the original *Deception* folder. Refer to Section A.3.3 for details.

B.2.2 Manipulation of passwords.xls File

While it was not possible to delete the system-generated *passwords.xls* file, that file could be moved, opened, examined, edited, and copied back to the original *Deception* location.

B.2.3 Impact of Unintended Deception Feature Behavior

While the *Deception* file is merely a honeypot, and the ability to delete, copy/move, open, or edit it with impunity perhaps may not immediately harm the host, such behavior provides an attacker with a means of analyzing and eventually circumventing D3E defenses.

Also, failure to prevent hackers from manipulating honeypot files could have embarrassing consequences, if original file contents were replaced by threatening, mocking, or otherwise inappropriate text or images.

B.2.4 Issue Resolution

At present, D3E appropriately triggers *ActiveLock* whenever someone "double-clicks" on a honeypot file in an attempt to open it. It should be fairly straightforward to tweak D3E software so that it reacts to attempts to "right-click" on the file/folder to manipulate (i.e., copy, move, modify, or delete) the data. Cigent has identified a fix for this issue.⁴⁵

⁴⁵ Cigent response: "Deception files should not be able to be opened, edited or overwritten. This behavior is a bug inadvertently introduced in the latest version of D3E and will be fixed in the next release."

B.3 Windows Service Host Process Tries to Access *passwords.xls*

During the Version 2.4.4. D3E evaluation at the Win7 64-bit laptop, something in the host process for Windows Service kept trying to access the *passwords.xls* file, triggering *ActiveLock*. This happened periodically while D3E was running. See Figure B-1.⁴⁶



Figure B-1. Host Process Triggers D3E Deception Event

Recovery from the problem is straightforward: simply use the prescribed authentication method to clear the threat. The condition's persistence, however, even after reboot, makes it a good candidate for further investigation. Our observation indicated that D3E consistently and repeatedly generated the *Data Deception Event* message shown in Figure B-1 seven minutes after the administrator cleared the threat.

MITRE is working with Cigent to determine which process is attempting to access the *Deception* file. If the application is deemed legitimate, it could be designated a "Safe App." This would put a stop to the unwanted *Data Deception Event* alarms. Note that the Safe App feature requires a special license from Cigent, available to premium customers upon request.

⁴⁶ Cigent response: "Most Windows processes and all registered AV programs are allowed to access the deception file. When connected to the Cigent Management console, additional details regarding the offending application (including PATH) are collected and reported. Should the application be determined to be authorized (backup, EDR, etc.) administrators can add the application as a Safe App to a D3E policy."

B.4 APPCRASH Condition at Win7 64-Bit Laptop

On a few occasions during testing at the Win7 64-bit laptop, the D3E Dashboard stopped working due to an "APPCRASH" condition. Like the *Deception* issue cited in Section B.3, this problem deserves further investigation.⁴⁷



Figure B-2. D3E Dashboard APPCRASH

⁴⁷ Cigent response: "Cigent would be very interested in further investigating the cause of this crash condition as we have been unable to reproduce in-house."

Appendix C D3E Central Management Console

MITRE did not evaluate D3E central-management capabilities. We did, however, receive a Cigent briefing [12] on the subject on 26 May 2021 to familiarize ourselves with the capability and to buttress our belief that centralized D3E management would be a safer, more efficient means of deploying D3E than per-device configuration and management.

The following paragraphs contain a very high-level summary of D3E Central Management capabilities.

C.1 Overview

D3E can be deployed with a central management console capable of monitoring and managing data security throughout a network and responding (activating *ActiveLock*) either manually or automatically.⁴⁸ Cigent's centralized D3E-management feature can run either in the cloud or locally on-prem.

With centralized management, D3E software running on each end-user machine can be controlled remotely. Management policies can be created and applied for user groups and/or for individual devices. The Central Management Console administrator can make D3E software-protection changes at any of the managed machines, but a user/administrator at the local computer also can change settings, as long as those changes do not lower the assigned security profile. Both the central and local administrators may respond to *ActiveLock* security alerts.



Figure C-1 shows the Central Management Console Dashboard.

Figure C-1. Central Management Console Dashboard

- The central manager creates default or specialized security policy for computers or for groups of computers.
 - Users/administrators at the end devices may increase the security level of their devices, but they may not lower security below the assigned default level.

⁴⁸ Presently D3E Central Management & Configuration applies only to D3E software; however, the ability to extend this centralized management capability to secure Solid State Drives is on the Cigent roadmap.

- D3E at each end device responds autonomously to security events, protecting data (engaging *ActiveLock*) in accordance with the security profile for the device or the group of which the device is a member.
- End devices reach out automatically at configurable intervals to provide security-status updates to the central manager and to download changes.
 - An overview of the security status of specific devices can be displayed at the Central Management Console, as shown in Figure C-2.



Figure C-2. Device Security Status

• The Central Console administrator also can view the threat history for each of the managed devices. See Figure C-3.

| Consels X | + | | | | | | | | |
|-----------------------|------------------------|-----------------|-----------------------------|-----------------------------|--|--------------------------|-------------------------|-----------------------|---------------------------|
| | D 🔒 ettps/loentra | licigentucom | Anistory | | | A search | | | IVA 60 |
| -L. Stack | Confluence @ Interiece | is for Fersonal | • IRA @ Homopage CISA @ | CPk loots CDC Dudy 🕲 ANDI 🕥 | The Office of Access b 🦉 Switch Windows 10 ft. | rg* 1003/1030 User Guide | Smart Card Magic All T. | 1 STESSAZ SmartCard : | |
| | D Threat H | listory | | | | | | | David Wolf |
| | | | | | | | | | slavid102e.colligmail.com |
| | Exter a partial End | paint Name, | Threat Type, or Description | THE REAL PROPERTY AND | | | CALCO NET | Thra Filter 2 week | |
| | Endpoints | | 3 Threats | | | | | | |
| | Threat Types | | | | | | | | |
| | Active Lock | | Timestano 4 | Conductional Name | Thread types | Active Lock | Source | Description | |
| | Source | | May 26, 2023, 9.05:12 AM | DESKTOP-86K3531 | Antivirus disabled | Clear | Dar | | |
| | Comme | | Mey 26, 2021, 9:05:03 AM | DESKTOP-BEK3531 | Antivirus disabled | Сланое | DIF | | |
| | Gioths | - | May 28, 2021, 3:59:30 PM | DESKTOP-ABLOBUM | System connected to a new/unite work | usted net- Clear | USE | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | 1111 | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | 1 | | | | | | | | |
| | | | | | | | | | |
| | x | | | | | | | | |
| States and a state of | | | | | | | | | |

Figure C-3. Threat History for Managed Devices

• Presently D3E Central Management applies only to D3E software. Cigent plans to extend the feature to firmware protection and Secure Solid-State Drives (SSDs).

C.2 Notifications

The Central Management Console administrator chooses how notifications will be sent from managed devices. Note that both email and in-app notifications may be made, and the option is configurable for each of many possible security events. Refer to Figure C-4 below.

| PROFILE PASSWORD 2FA NOTIFICATIONS PA | YMENT METHODS |
|---|----------------------|
| Freat fortunation (incomes) Incomes Income Security on Event Security | |
| Never - | margandais dissolute |
| | SEV4 |
| Enable advanced features | |
| | |
| Type | E-mail In-App |
| | Cherry Contractory |
| Removable storage device inserted | |
| Data deception his accessed | 2 |
| Network deception service accessed | |
| System connected to a new/untrusted network | |
| Antivirus detected threat | |
| Annivirus disabled | |
| Automated typing detected | |
| CyberArk EPM agent detected threat | |
| CyberArk EPM agent detected threat | |
| Blocked bad program | |
| Detected virus | |
| D3E autó lock | 0 0 |
| Dell Trusted Device | |
| Manual Lock Event (Console) | |
| Carbon Black Event | |
| Carbon Black Unreachable | |

Figure C-4. Security-Event Notifications

C.3 Security Policies

The Central Console administrator sets D3E policies for various computer work groups. As the note in Figure C-5 states, if a device falls outside a group ("device-set") policy, the default policy will be assigned to the device.

| nterrore 🕒 Interfaces for Personal. 🔷 JRA 🔇 | Hómapaga CISA () CPR Taxas CDC D. | aly O ANDI O The Office of | Accessib. Switch i | Windows 10 fr 9" H3 |
|---|--|----------------------------|--------------------|---------------------|
| Policies Policies are applied using groups. Aft | er completing a policy, visit the grou | ups page to activate it | | |
| Policy | | | | |
| Remote Worker Policy | < N Adobe Files | Custom File Types | D Folders | Safe Apps |
| HR Policy | Allow 'Always On' file type | protection ① Off |) (6 | |
| Engineering Policy | Sync interval () | 1 5 | • 60 JE | seconds |
| Central Folicy (Centrality) | Sync interval metered @ | | 2 60 E | minutes |
| | License Interval ① | 1 2 100 | * 60 1 | minutes |
| | Import policy ① | Selected | Device | Import |
| Roorder Policies | | | | |
| Note: Policies are applied uting device sets. If a device is a member of more that one device set, the first matching policy is the list will be applied devices outside and works not me applied to the | | | | |

Figure C-5. Central Manager Policy Screen

C.3.1 Set the Synchronization Interval

The Central Management Console administrator sets the sync interval – the frequency at which managed devices reach out to provide security-status updates to the central terminal – at the

Policy screen. Refer to Figure C-5 above. Note that a unique sync interval may be established for each policy. The interval should be fairly tight, to ensure that important status information is sent to the central administrator on a near-real-time basis.

C.3.2 Safe Applications

Occasionally applications at a device will need access to sensitive files for legitimate and safe reasons, and it will be impracticable to cope with large numbers of *ActiveLock* alerts generated for accesses that are harmless. For example, backup software requires access to all files on a device, including sensitive files. Cigent allows selected programs to access protected files without end-user authorization. Such programs can be designated as "Safe Apps" at the policy screen shown in Figure C-6 below.

For security, PKI⁴⁹ certificates should be used for Safe Apps, and the path or filename for the application should be identified.

| Centiuence \ominus interfaces for Personal 🔶 JRA 🔘 H Remote Worker Policy | omepage C C osoft Ol | ISA 🖨 CPR Tools' CDC Delly 🖨 Frice Files 🗖 Adobe Files | ANDI 🐡 The Office of Acces | olb. 9 Switch Windows 10 fr., 4* H90/H350 User Guid ypes D Folders Ø Safe App | e. 📴 Smart Cord Mogie N s 😨 🖓 |
|--|---------------------------|--|---|--|----------------------------------|
| HR Policy | Sole a | ipplications are allowed to access prote | cted files without authorization | by the end user. | |
| Engineering Policy | Add a Exem | n item to Sate Apps if the application re- ples: backup programs, cloud and file sy | quires access to protected files no applications | for proper operation | |
| Default Policy (default) | Sate a | applications are centified by matching is Safe Application | ey certificate fields and can be f | ruther narrowed using path or file name. | |
| | > | OneDrive Dropbox | | | |
| | | Extracted Certificate Information | | | Upload Ce |
| Reorder Policies | | Common Name (CN) | | | |
| Note: Policies are applied using device sets. If a device is a member of more than one device set, the test matching policy in the list will be applied. Devices outside any device set are assigned to the detaut policy. | | Organization (0) | | | |
| | | Locality (L) | | | |
| | | State or Province (ST) | har day | \$≥* | |
| | | Country Code (C) | | | |
| | | Path or Ellanama | | | |

Figure C-6. Policy – Safe Applications

C.4 Third-Party Security Integration

D3E can work with 3rd-party Antivirus (AV) and Identity and Access Management (IDAM) products to provide enhanced endpoint protection and authentication. Figure C-7 shows the vendors with which Cigent has partnered thus far.

At this time, the Cisco and CyberArk products can provide security notifications to the D3E administrator, but they are not yet fully integrated with D3E. Sophos and Carbon Black are

⁴⁹ PKI = Public Key Infrastructure

sufficiently tightly integrated with D3E that suspicious behavior detected in their software can trigger security alerts in D3E.



Figure C-7. Third-Party Integration for User Authentication

Appendix D Abbreviations and Acronyms

| AF | Air Force |
|-------|---|
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| AV | Antivirus |
| CAC | Common Access Card |
| CROWS | Cyber Resiliency Office for Weapons Systems |
| CSV | Comma Separated Values |
| CTI | Cigent Technology, Inc. |
| CUI | Controlled Unclassified Information |
| D3E | Dynamic Data Defense Engine |
| DCO | Defensive Cyber Operations |
| DoD | Department of Defense |
| EDR | Endpoint Detection and Response |
| FIPS | Federal Information Processing Standard(s) |
| FOUO | For Official Use Only |
| FTP | File Transfer Protocol |
| GB | Gigabyte |
| HDD | Hard Disk Drive |
| IDAM | Identity and Access Management |
| I/O | Input/Output |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| MFA | Multi-Factor Authentication |
| ML | Machine Learning |
| NERVE | Networked Experimentation, Research, & Virtualization Environment |
| NIST | National Institute of Standards and Technology |
| NTFS | New Technology File System |
| NVMe | Non-Volatile Memory Express |
| | |

| OPAL | Storage specification for self-encrypting drives (not an acronym) |
|--------|---|
| OS | Operating System |
| PC | Personal Computer |
| PCIe | Peripheral Component Interconnect Express |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure |
| PW | Password |
| RCAT | Reconfigurable Cockpit Avionics Testbed |
| RDP | Remote Desktop Protocol |
| RPC | Remote Procedure Call |
| SATA | Serial Advanced Technology Attachment |
| SED | Self-Encrypting Drive |
| SIEM | Security Information and Event Management system |
| SMB | Server Message Block |
| S/N | Serial Number |
| SOC | Security Operations Center |
| SP | Special Publication |
| SSD | Solid-State Drive |
| ТВ | Terabyte |
| ТСР | Transmission Control Protocol |
| TCG | Trusted Computing Group |
| Telnet | Terminal Network |
| UBA | User Behavior Analytics |
| USAF | United States Air Force |
| USB | Universal Serial Bus |
| Win7 | Windows 7 Operation System |

Distribution

Government

NAWROCKI, JOHN P NH-04 USAF AFMC AFLCMC/CROWS john.nawrocki@us.af.mil; HOPKINS, LYLE L GS-13 USAF AFMC AFLCMC/CROWS lyle.hopkins.2@us.af.mil; MARTIN, LLOYD H NH-04 USAF AFMC AFLCMC/CROWS lloyd.martin@us.af.mil; BEARD, ROGER A NH-04 USAF AFMC AFLCMC/CROWS roger.beard.1@us.af.mil; LEHMANN, ZACHARY M Lt Col USAF AFMC AFLCMC/CROWS zachary.lehmann@us.af.mil

MITRE

Christian Fiore Jeffrey Higginson John Mulrey Donna Rondeau (Project File) Sven Skoog Justin Yeager