2022 Hendry Street, Ft Myers, FL 33901
CPRTools.com | 239-464-3282

SECURITY IN REVIEW

Datashield Pro USB by

Fantom Drives

Document Number: 20210415-03

2022 Hendry Street, Ft Myers, FL 33901
CPRTools.com | 239-464-3282

BACKGROUND

SELF ENCRYPTING DRIVES (SEDs) are becoming more and more prevalent in the market place. CPR Tools, Inc. is uniquely qualified, through years of media storage research, data recovery and data eradication experts, to understand multiple methods of securing data and discovering and/or creating methods, techniques or hardware to exploit and defeat many such methods.

Having worked extensively with and having a deeply intimate understanding of the low level workings of TCG OPAL Locking Ranges, we recently encountered the DataShield Pro encrypted drive enclosures from Fantom Drives.

EVALUATION

Preliminary research into the DataSheild Pro USB encrypted drive enclosures from Fantom Drives revealed a surprisingly poor implementation of security from the perspective of preventing unauthorized/unauthenticated access to data stored on the 'secure' drive.

Our evaluation of these drives revealed that, unlike other drives in this category which typically employ both physical and virtual obfuscation techniques, such as epoxy on chips and masking software/firmware authentication methods, the subject drives in this case appear to store all metadata required to decrypt the user data on the drive itself.

The drive employs a section of LBAs towards the end of the available LBAs as a partition to store the metadata. While the drive is in the enclosure, this partition is blocked from reads and/or writes, but upon removing the drive from the enclosure, this partition is visible as are the data sectors therein.

Further, it does not appear that the metadata used for password and encryption key storage is unique to a drive or enclosure, as we were able to copy the metadata and encrypted user data to another drive and decrypt it using the same password on a second enclosure. The hardware does not employ any means of obfuscation, which provides a clear view of the components.

Given all of these shortcomings, it would be possible for a determined attacker to read the contents of the SPI flash which would most likely contain the firmware of the USB/SATA bridge chip, and make modifications to potentially store the encryption keys used. Communications between the microcontroller that verifies the password input and the USB/SATA bridge chip could easily be monitored as all pins are accessible and able to be probed.

Given that we did not dedicated much time at all to this research and had not yet determined the method to check and validate PINs, we believe it would take a dedicated attacker very little time to monitor the change in the metadata as new passwords are generated; this would certainly lead to being able to determine or inject a known password into the metadata and decrypt the drive. The fact that this can be done on a separate drive in a separate enclosure would provide more than enough time for a determined actor to access this data.