Mitigating Endpoint Threats to Information Assets

How Secure Pocket Drive Can Help Prevent Data Theft

Introduction

Information belonging to government and private organizations faces ever-increasing threats from network endpoints. Some are direct, while others are subtle and hidden. This paper deals with these threats and shows how the SPYRUS Secure Pocket Drive can mitigate them in a network setting.

We can group these threats under the term *exfiltration*, which is, in many ways, a new name for an old problem. Exfiltration is a form of unauthorized disclosure or leakage of sensitive information assets that is difficult to detect by the victim. Sophisticated hackers use a creative combination of threat technologies to access and download confidential information when sufficiently motivated.

The consistent and growing need for secure remote access while teleworking creates many more endpoints that can be used to launch an attack against corporate or government data assets. These endpoints must be treated as hostile environments, and we seek to address the threat scenarios and mitigation of them in this paper.

The Threat of Exfiltration

The difficulty of detecting information exfiltration stems from the use of covert channels to transfer data from the target network system to a remote site without permission. The identification and subsequent termination of this class of attack is generally not achieved until irreparable exposure has been exploited by the threat agent.

The consistent and growing need for secure remote access while teleworking creates many more endpoints that can be used to launch an attack against corporate or government data assets.

Having stated the general problem, it is necessary to examine the motivation and anatomy of these attacks. Experts in the field of digital threat analysis agree that exfiltration attacks are not mere opportunistic hacks but are specifically targeted at desired information. They are far too well constructed and success-oriented to be the work of so-called "script kiddies."

Exfiltration attacks belong to an increasing class of sophisticated schemes that target commercially valuable information and other sensitive assets that are easy to trade for cash. Credit card, ATM debit card, and related financial information are prime targets for exfiltration, as are other types of information assets. Organized crime is a highly motivated source of threats to the network owners and their customers. Without strong protection of private data assets, a company cannot remain solvent and prosper in today's demanding business world.

Typical exfiltration success factors are stealth and target system vulnerability. The stealth aspect is achieved by breaking the attack into three distinct phases. Assuming that the target system is vulnerable, these phases are infiltration, data harvesting, and exfiltration. Each of these phases

must be accomplished without the knowledge of system administrators and legitimate users. If the attacker tips his hand in any of them, the attack may result in little or no impact.

Infiltration

Initial entry by the threat agent is the starting point of many breaches of security, whether the object is to steal information or to create a denial of service by disabling system functionality and availability. The attacker must first infiltrate the network as a seemingly credible player in order to harvest and remove the targeted data. This can be accomplished by remote access, third party connections, SQL injection, exposed services, remote file inclusion, email Trojans, or direct physical access, to name the most common methods. In many cases, the use of default account names and weak or well-known passwords are prime factors that account for the success of the attack.

Data Harvesting

Data harvesting is the next phase of the attack. The threat agent must assess and determine which assets are of maximum value to himself or his employer. Network mapping tools are a boon at this stage, providing the attacker with user and group lists, privileges, and storage locations that are essential to gaining knowledge of the lay of the land and the location of targeted data resources.

Gaining access to these assets may require additional privileges within the system, so this might be the initial objective of the attacker. Finding and obtaining data targets to harvest and the means to access them are aided by malware resources such as memory parsers, keystroke loggers, network sniffers, and similar tools. As in the initial entry phase, stealth is important in all these interactions.

According to Trustwave Spiderlabs researcher Nicholas Percoco in 2010, about 54% of data harvesting attacks were accomplished by malware applications of this type. The table below shows percentages of successful attack strategies among actual attacks (also sourced from Trustwave real world studies). The attacker must also maintain an aura of typicality to avoid alerting alert system administrators or installed safeguards and watchdog applications.

Exfiltration Threat Category	Attack Percentage
Microsoft Windows Network Shares	28
Native Remote Access Capability	27
Malware Capability: FTP	17
Native FTP Client	10
SQL Injection	6
Malware Capability: SMTP	4
Malware Capability: IRC	2
Exposed private web application interface	1.5
HTTP File upload site	1.5
Backdoor: Malicious PHP-based Web Shell	1
Anonymous FTP	< 1
Encrypted Backdoor	< 1
Physical Access	< 1

Exfiltration Phase

Exfiltration in the narrowest sense of the word is the actual export of sensitive information in such a way that the data movement is not detectable. This is the third and most important part of the attack. However, if the threat agent has acquired sufficient privileges, there may be no need for stealth during this phase. FTP, HTPP, HTTPS, and SMTP protocols have been effectively used to accomplish the exfiltration. Typically, the agent employs additional covert channels that prevent detection and ensures repeat attack potential over a long period of time. To make it easier for the hacker, there is an ample supply of academic and hacker studies on the types of covert channels that work well for removing information without detection.

The use of concealment mechanisms to hide the exfiltration process can lead to impressive benefits in two important ways. Nicholas Percoco of Trustware has calculated in a recent study that the average attack of this type goes undetected for an average of 156 days. This gives the attacker the luxury to choose a low-bandwidth covert channel or to maximize yield over multiple data resources in a given target network.

A final stage of the basic attack is for the attacker to cover his tracks to ensure that subsequent exfiltrations can be carried out at a later date and that the technology of the attack does not become known to the defenders of the network. The use of hypervisor attacks and rootkits to remove all traces of the attack is a convenient hacker strategy.

Mitigating Risk with the SPYRUS Secure Pocket Drive

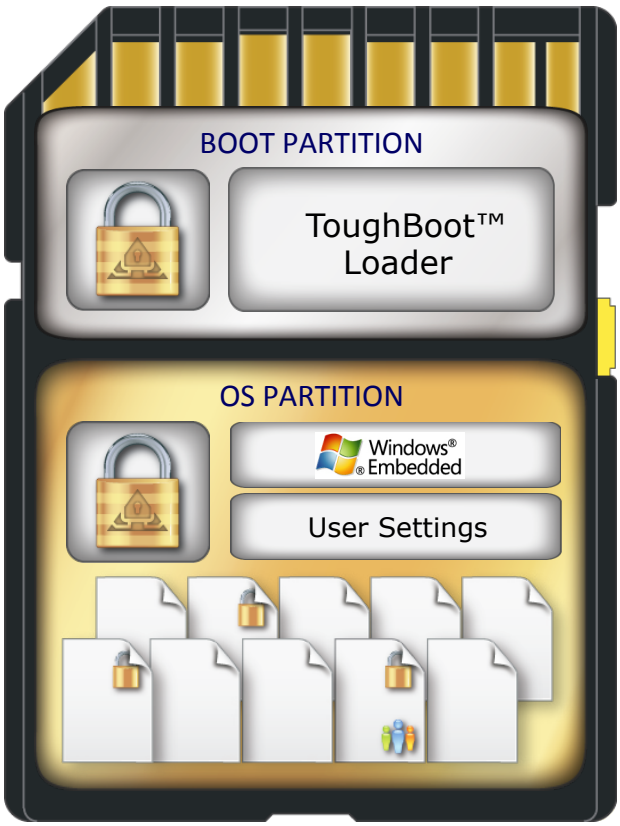
The SPYRUS Secure Pocket Drive (SPD) is the first native, licensed Microsoft® Windows® environment locked to an encrypted USB flash drive.

SPD implements XTS-AES full disk encryption and secures the Windows operating system, applications, profiles, and data on the user's drive.

To more thoroughly protect sensitive information, SPD can be coupled with a SPYRUS Hydra Privacy Card® (Hydra PC™) encrypting USB flash drive. Both SPD and Hydra PC implement full Suite B hardware-based cryptography that is designed, engineered, and manufactured in the USA. Suite B algorithms include EC-DH key agreement and ECDSA digital signatures with high-strength P-384 keys, AES-256, and SHA-384. This solution will be discussed in the sections that follow.

This combination provides strong cryptographic protection in five important ways.

- The Master Boot Record (MBR) and the related SPYRUS ToughBoot™ loader process components are encrypted with XTS-AES to protect from tampering and are validated at boot time. Any attempt to modify the ToughBoot loader is detected, and the user logon then fails.



- The integrity of the host operating system is validated by SPD prior to transferring control to it. In effect, SPD acts like a high-assurance TPM chip, but one that uses the higher-strength Suite B cryptographic algorithms.
- Any attempt to modify the operating system once it is loaded and operational is intercepted and written to a RAM cache, and is lost on power-off. Any impact is therefore a one-time event.
- User software applications are encrypted, write protected, and access controlled.
- User data files can be individually AES-256 encrypted and digitally signed in hardware, using a supplementary SPYRUS hardware device such as the Hydra PC Digital Attaché.

This protection relates directly to the prevention of exfiltration attacks and effectively mitigates their risk.

Information must be protected whether it is at rest, in transit, or in use. SPYRUS believes that the operating system and applications should be protected using a data-at-rest scheme, while user data needs to be protected with a data-in-use scheme. Data-in-transit protection is a function of the network and is not addressed in this paper.

Data at rest can be protected with full disk encryption based on XTS-AES 256, while data in use must be protected by encrypting every file under a unique key with AES-CBC 256. This provides maximum appropriate protection to all resources at all times and minimizes exposure to exfiltration threats.

Mitigation of Infiltration

From the standpoint of exploitation strategy, the infiltration phase is largely under the control of the attacker. Exploitation of weak passwords and access controls is a major source of entry into the network. Procedural security can be effective in closing these entry points to external hackers.

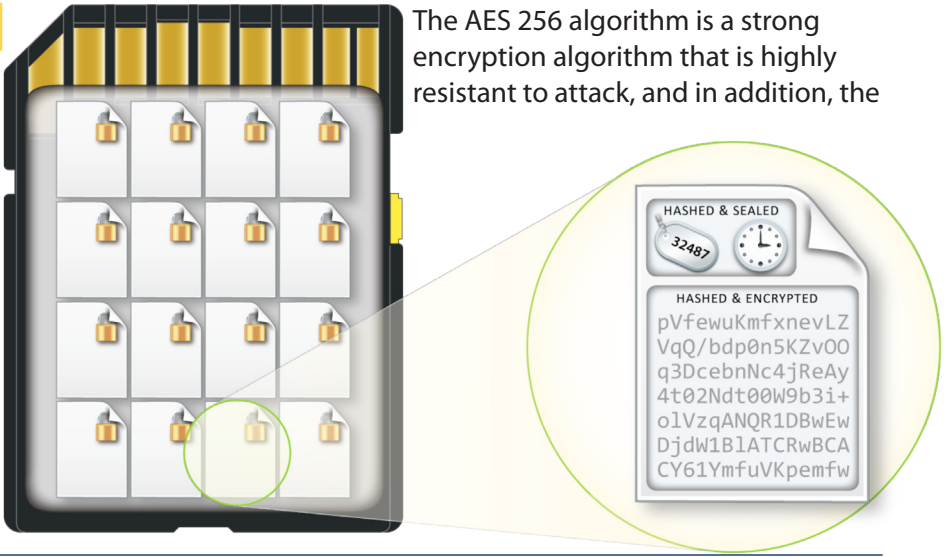
Drive-by attacks, in which malware is downloaded and installed by exploiting a web browser, email client, botnet, or OS bug without user detection, are more problematic. Threats of this type to SPD are only short-term entry points. Modification of OS or application files will not survive a reboot of the device because of internal SPD security measures and the use of a RAM-based disk cache.

The use of XTS-AES 256-bit encryption on both the OS and boot loader partitions of SPD prevents modification of the media using an external memory card reader, and it also defeats watermarking and related attacks that AES-CBC encryption can allow. The integrity of OS resources is therefore appropriately protected for the next power-up.

The data-at-rest solution provided by SPD component therefore continues to protect against malware using XTS-AES 256 sector-based encryption. As described previously, exposure during a login session does exist, and prevention depends on the use and update of antiviral and anti-malware countermeasures. However, a reboot will clear any malware.

Mitigation of Data Harvesting with SPD+

Secure Pocket Drive in conjunction with a strong cryptographically protected storage solution such as Hydra PC Personal Encryption Device or Digital Attaché encrypting flash drives provides an extremely effective prevention to exfiltration. The 256-bit encryption of individual files using the CBC mode of AES creates a high resistance to unauthorized access.



The AES 256 algorithm is a strong encryption algorithm that is highly resistant to attack, and in addition, the

CBC mode of AES provides appropriate resistance to offline decryption attacks when applied to individual files. Downloaded AES-CBC encrypted files retain their protection forever provided no key material is exported with them. The Hydra PC Personal Encryption Device and Digital Attaché protect the file encryption keys under a separately encrypted key hierarchy to prevent downstream exposure in an exfiltration attack. These keys are cryptographically unwrapped in hardware, are never exposed to a malware attack, and are zeroized immediately after the encryption or decryption operation completes. This ensures the core protection of data in use against unauthorized disclosure. We call this combined solution the SPD+.

The data-at-rest solution provided by the SPD component continues to protect against malware intrusions using XTS-AES 256 sector-based encryption. As described previously, exposure during a running session does exist. If malware is detected, however, powering down the system restores the secure OS configuration and eliminates a reboot into a hostile environment.

In addition to encrypting individual files, the Hydra PC Personal Encryption Device and the Hydra PC Digital Attaché also "seal" the file at the time it is encrypted. The plaintext version of the file is hashed in software prior to the encryption stage, and then during the hardware encryption phase the ciphertext is hashed on a running basis before the data is written out. At the end of the encryption process, both the plaintext and ciphertext hashes are digitally signed and stored in a file trailer record. This protects those files against even so much as a single bit error or modification, whether accidental or deliberate. This provides a substantial degree of protection against infiltration, which might occur if one user were to encrypt a file, and somehow the encrypted file could be modified in such as way as to inject a virus that would then infect the recipient's system.

Of course, the file-encrypted files need to be decrypted to be accessed, and so long as the decrypted plaintext file exists, there is a potential vulnerability to data harvesting. However, this vulnerability can be minimized, if not eliminated. Through a policy setting, if the user decrypts a file, it is opened in a temporary folder that is watched. When the file is closed, it is automatically re-encrypted with the changes that have been made to it, and the plaintext version is overwritten.

While this solution is technically secure, it requires a strong procedural base on the part of the user and administrator. Users must keep plaintext versions of their sensitive data under tight control and use encrypted storage whenever possible. Of course, the defense against data harvesting attacks is only problematic when the system is powered on; not when the storage medium and SPD are powered down.

Mitigation of Exfiltration

The final stage of the exfiltration attack class is thwarted by both SPD and SPD+. Because the SPD operating system image and settings are protected by XTS-AES 256 encryption, an attacker is unable to permanently modify the OS with Trojan copies of OS functions or acquire access through unauthorized modification of the Windows OS configuration. MBR and other boot-level component modification attacks are likewise prevented by an integrity check on these components by the hardware. The Master Boot Record and the ToughBoot loader modification attacks are likewise prevented by an integrity check on those components by the hardware at pre-boot time.

The injection of malware into the SPD Windows operating system image or installation of malware, spyware, keyloggers, viruses, or Trojan horse applications on the running image can only be performed in a persistent manner by an authorized administrator. If the administrator is malicious, there is no limit to the hostile disclosure of user assets that could result and the issue of external exfiltration agents becomes moot. Damage from hacker, virus, or user insertion of malware is ephemeral, as any modification to the OS or applications will not survive a reboot.

The data harvesting and extraction phases of this attack class are severely hampered by the SPD+ encryption capabilities and functional design. The

only way an exfiltration attack could succeed is if the user saves plaintext versions of files on an accessible network drive. While other secure USB flash storage devices may offer bulk encryption protection of the user data, they lack the integrity enforcement on the operating system executables and configuration, the integrity protection of the MBR and related components, and the individual file encryption and sealing functions. These are significant advantages of the SPD+ solution over basic encrypted storage when considering the sophistication of an exfiltration attack by a capable agent.

Conclusion

In this paper we have examined the class of exfiltration attacks that are increasingly launched against corporate and government data with alarming success in both network and teleworking scenarios. According to recent studies, most networks have a moderate-to-high exposure to this attack because it has so many variants and takes time and effort to detect and eliminate. The risk of this attack may seem less pronounced in transient teleworking scenarios that typify the traveling worker due to the tendency for exfiltrations to be long-term violations. But once malware is covertly installed, both traveling and home-based teleworking situations are equally at risk. Moreover, the use of covert channels can render this attack even more difficult to discover. Only networks and platforms that contain nothing of intrinsic value to the attackers can hope to avoid this risk entirely.

One sure way to nullify the value of data in use to attackers is to encrypt individual files with a strong cryptographic algorithm such as AES-CBC 256 that has no reasonable hope of being broken. The SPD+ solution does this, acting as an effective defense against the data-harvesting capabilities of an exfiltration attack. In parallel with this, hardware-based full disk XTS-AES 256 encryption of operating system and software, and control of those elements, provides significant further data-at-rest integrity protection and mitigation, because they further reduce the likelihood of covert malware-based export of sensitive information.

As the perennial observation goes, no system is 100% risk free. While it is clear that additional procedural and automated elements are needed to successfully detect, disable, and deter exfiltration threats, Secure Pocket Drive coupled with a Hydra PC Personal Encryption Device or Digital Attaché encrypting flash drive can uniquely enhance these additional elements. This solution offers a broad spectrum of strong protective countermeasures that not only defend and contain user data but also preserve the integrity of core system processes and assets that could otherwise be subverted for use in data harvesting and exfiltration.

Proudly designed, engineered,

and manufactured in the USA

For more information about SPYRUS products, visit *www.spyrus.com* or contact us by email or phone.

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@spyrus.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 329-6211 fax

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phc
+61 7 3220-2233 fax
www.spyrus.com.au
info@spyrus.com.au

SECURED BY SPYRUS®

Document number: 412-390003-03

Microsoft GOLD CERTIFIED Partner