



# Mitigating Rootkit Threats

## How Secure Pocket Drive Can Help Prevent Information and Identity Theft

### Introduction

Information Technology environments face an ever-increasing threat from network sources, some of them direct and overt, others subtle and hidden. One of these threats is the “rootkit.”

A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. In a nutshell, an attacker finds a vulnerability in the targeted operating system (OS) or gains access to a system administrator account by discovering an existing user name and password. Once he has unfettered access to the system, the attacker installs the rootkit, which normally does its best to stay hidden from authorized users and whatever security mechanisms are implemented in the OS.

Although rootkits can serve a variety of ends, they have gained notoriety primarily as malware, hiding applications that hijack computing resources or steal passwords without the knowledge of administrators and users of affected systems. Rootkits can target firmware, a hypervisor, the OS kernel, or—most commonly—user applications.

Since the Sony BMG copy protection rootkit scandal in 2005, the threat from rootkits has received considerable attention. Rootkit attacks have also become more prevalent, and the rootkits themselves have become more sophisticated. Rootkits have become a real threat to computer processing environments, because they can be installed when

a computer is connected to the Internet and then users unwittingly bring them into a secure network environment to steal information.

Modern rootkits do not elevate access but rather are used to make another software payload undetectable by adding stealth capabilities. Most rootkits are classified as malware, because they are bundled with malicious payloads. For example, a payload might covertly steal user passwords, credit card information, or computing resources.

This paper shows how the SPYRUS Secure Pocket Drive can help mitigate the threat of rootkits in a network setting.

### Anatomy of a Rootkit

So what is a rootkit and why is it so dangerous? There are several reasons that computers are targeted by attackers: to gain information that resides on a specific computer, to use one computer to attack another specific computer or network, or to use a specific computer as part of a botnet that can send SPAM or perform other nefarious actions. We will concentrate on the first two, because they involve using a rootkit to steal information.

*The goal is to provide a mobile computing environment in which users have a high degree of assurance that they are working in a known and trusted environment.*



An attacker needs to find a way to inject the rootkit into the OS. If this is a remote attack, the attacker begins by gathering general intelligence on the targeted organization. This might include scans of the targeted organization's network, calls to the organization's employees or helpdesk, and looking at the Internet's domain name system (DNS) entries to get the IP addresses of external hosts.

After discovering the general layout of the organization's network, the attacker works to find vulnerable computers by using tools like Nmap to enumerate live hosts and determine which services are exposed to the outside world. From there, the attacker works to deduce which software is running on the computer, including the OS, web server, database, and applications.

Known vulnerabilities for specific pieces of software are available on the Internet, and as the Stuxnet worm demonstrated, many vulnerabilities are not publicly known until they are used by an attacker. Once the attacker knows the profile of the system that he is attacking, he then looks for any vulnerability to gain shell access.

Because shell access allows attackers to execute arbitrary commands in an attempt to escalate their rights, this is the prize they seek. For example, if the machine under attack is a web server, attackers might launch an SQL injection attack against a poorly written web application to compromise the security of the associated database server. They can then leverage their access to the database server to acquire administrative rights.

In general, the tools used to root a machine run the gamut from social engineering to brute force password cracking or causing the target machine to run a buffer overflow exploit. More sophisticated rootkits can exploit the pre-boot process and hide in places on a drive that are not within the standard file system.

Secure Pocket Drive is designed to identify and prevent the operation of rootkit infections regardless of the level they target.

### **Mitigating Risk with Secure Pocket Drive**

Secure Pocket Drive (SPD) from SPYRUS is the first licensed Windows® environment on an encrypting USB flash drive, designed for trusted mobile computing. SPD includes a hardware platform, a licensed version of Windows Embedded Standard or Linux that is cryptographically bound to the device, and a trusted ToughBoot boot loader that the host computer boots via the USB port.

Because all of the software, including the boot loader and the operating system, is integral to Secure Pocket Drive, no external drivers or middleware are required on the host PC. The goal is to provide a mobile computing environment in which users have a high degree of assurance that they are working in a known and trusted environment.

SPD provides three services that help prevent infection of the device and further mitigates the installation or concealment of rootkits should they gain entry into the device.

- ▲ **Data-at-Rest Protection**—When SPD is powered off or is inserted into a computer and powered on, its full disk encryption features provide strong data-at-rest protection to prevent infection of an inactive device. The OS partition is not decrypted until the user successfully authenticates to the device.
- ▲ **Resistance to Persistent Infection**—When active, the write filtering incorporated into the embedded Windows operating system blocks writes to the operating system and application files on SPD. This ensures that each time the SPD is booted, a known good operating environment is in place.
- ▲ **Integrity Verification**—A number of hardware-based and software-based integrity checks are performed during pre-boot, boot, and post-boot processing to ensure that the device has not been tampered with.

### **Data-at-Rest Protection**

Before a user authenticates to SPD, the full disk encryption features of the device provide strong

data-at-rest protection to prevent infection of an inactive drive.

SPD implements XTS-AES encryption, which uses two AES-256 keys for extremely strong sector-based encryption of its storage medium. Encryption of both the OS and boot loader partitions of SPD prevents modification of the storage area by using an external memory card reader, and it also defeats watermarking and related attacks that AES-CBC encryption cannot protect against. The integrity of OS resources is therefore appropriately protected for the next power-up.

### Resistance to Persistent Infection

Rootkits are designed to load and enable a software payload to operate undetected on a computing platform. This, obviously, requires loading that payload onto the SPD. This type of malware can be downloaded and installed by exploiting a web browser, email client, or OS bug without user detection. Within a single SPD session, preventing threats of this type may depend on current updates of antivirus and antimalware countermeasures, which can be problematic. However, malware agents that are automatically downloaded by applications do not persist beyond one SPD boot session because of internal SPD security measures that block all writes to the device.

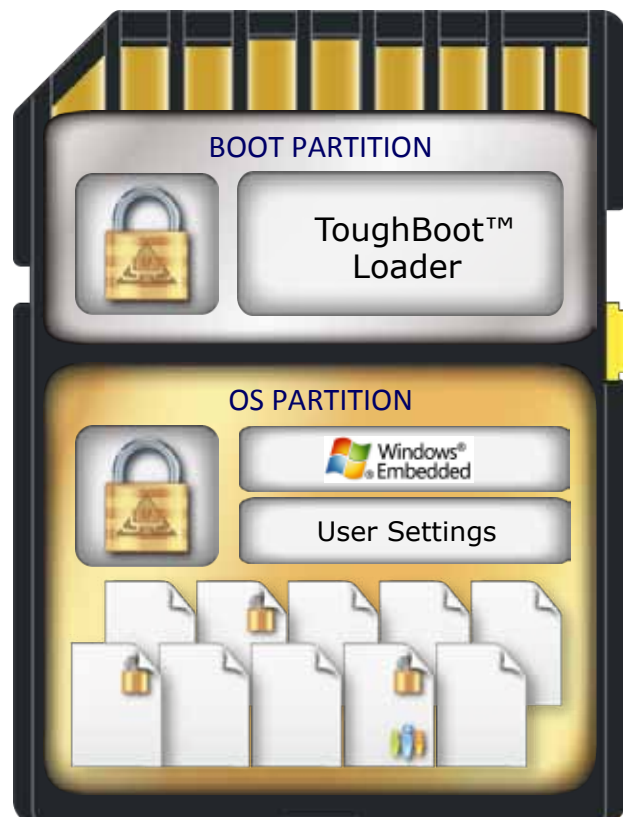
The write filtering incorporated in the Windows Embedded Standard operating system blocks writes to the SPD operating system and application files. The integrity of the OS and its resources is therefore appropriately protected for the next power-up. This means that even if the device is infected outside of the organization's network, a reboot clears the infection, preventing it from entering the organization's network if the SPD is booted on a computer internal to the network.



Contrast this with your regular laptop used at a coffee shop in the morning and then on the internal network later in the day. Even if your laptop is rebooted, the infection persists and can create an attack point inside of the secure network.

The SPD Productivity Edition uses file-based write filtering, which allows files to be saved within the Documents and Settings folder. However, this can present an attack point for malware files that persist across logon sessions of the device. To more thoroughly protect sensitive user information and to further reduce the risk of malware infection, you can couple SPD with a Hydra Privacy Card® (Hydra PC™) encrypting USB flash drive from SPYRUS. The optional Sentry A-V antivirus scanning engine built into Hydra PC will minimize the chance of you storing an infected file on the device and retrieving it either on SPD or on a different PC or network where it could cause damage.

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).

### Pre-Boot Integrity Verification

When SPD is inserted into the host computer, it goes through a power-up sequence before arriving at a fully operational state. This includes performing a variety of integrity and security checks, as well as initializing the various hardware components and software/firmware states. If any of these tests fail, the device will not mount.

If the self-tests complete successfully, the boot loader partition is decrypted, the boot loader is read into memory, and control is passed to it. After more self-checks, the device prompts for the device unlock password, which is sent to SPD over a secure channel for evaluation.

If the password is correct, the encrypted partition is decrypted. In the WES 2009 version, the boot loader “walks the file system” before loading it into memory, validating specific OS files against pre-stored signatures (hashes). Depending on the outcome, the boot loader either terminates the boot process or loads the OS into memory.

### Post-Boot Integrity Verification

After control is passed to the OS, additional SPYRUS software running within the OS environment validates the integrity of a larger set of files before allowing the user to authenticate (log in) to the OS.

As stated above, when the OS is running, write filtering incorporated in the Windows Embedded Standard operating system blocks writes to SPD. This ensures that each time SPD is booted by the user, a known good operating environment is in place.

### Conclusions

Secure Pocket Drive is the ideal high-security solution for the travelling “road warrior,” the teleworker, or for pandemic and other disaster

preparedness. Other areas, such as health care and the financial sector, are sure to follow.

Secure Pocket Drive allows user to carry a complete, encrypted, high-assurance operating system in their pocket that can be booted in any available computer, completely bypassing the computer’s hard drive and any resident malware.

Secure Pocket Drive is not intended to replace a conventional desktop or laptop computer. It serves as a trustworthy companion to a computer when security is particularly important.

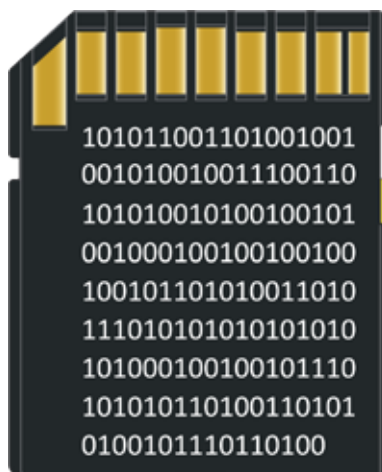
Secure Pocket Drive assures a pristine operating system environment when used with a computer that may be used by others who engage in risky behavior from a computer security standpoint.

Hardware-level protection ensures that the ToughBoot loader has not been modified, and when it is loaded, critical operating system files are hashed and verified against a digital signature to detect any modification.

In use, operating system files are protected against permanent modification. Any attempt to modify them, for example, by a virus, modifies only a cached copy of those files in RAM memory, and any such modifications are lost when SPD is powered off.

Secure Pocket Drive is flexible enough to meet your needs, whatever they may be. Here are some ideas to get you started:

- ▲ Remote Access—Employees can securely access the Internet, including web email, without fear of user modification or infection by malware. SPD can be configured with a VPN and/or remote access “thin” client, such as Citrix XenApp or Citrix Receiver clients. Neither users nor malware can save tool-bars, plug-ins, Active-X controls, or files on the device. An external USB flash drive can be used for document storage (of course, a SPYRUS encrypting flash drive is recommended).



- ▲ Mobile Workspace—With your organization’s productivity applications at their fingertips, employees can be productive even when they cannot connect to the Internet. Personal files such as documents and settings can be saved to SPD, while all other modifications are blocked.
- ▲ Read only Mobile Workspace—Users can run applications locally but cannot save settings. An external USB flash drive can be used for document storage (of course, a SPYRUS encrypting flash drive is recommended).



Proudly designed, engineered,



and manufactured in the USA

## ADDITIONAL INFORMATION

- Designed, developed, and manufactured in USA
- FIPS 140-2 Level 3 compliant
- Secure pre-boot authentication
- No residue left on host PC—you were never there.
- Malware protection
- Sophisticated self-destruct mechanisms
- Works with government-issued CAC cards
- Computer BIOS must support booting from a USB drive
- Minimum 1GB RAM required, more is better
- Fixed or removable memory (8GB, 16GB)

## CERTIFICATIONS

- FIPS 140-2 Level 3 certificate 1394 for the sector-based encryption module
- FIPS 140-2 Level 3 certificate 1302 for the SPYCOS® hardware security module
- Common Criteria EAL 5+ certificate BSI-DSZ-CC-0315-2005 for the Infineon SLE66CX642P cryptographic processor

For more information about SPYRUS products, visit [www.spyrus.com](http://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](mailto: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](http://www.spyrus.com.au)  
[info@spyrus.com.au](mailto:info@spyrus.com.au)



© 2011 SPYRUS, Inc. All rights reserved. Secure Pocket Drive is protected by U.S. Patents 7,757,100, 7,380,140, 6,088,802, and 6,981,149, with other patents pending. Individual Hydra PC products may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 6,088,802; 6,003,135; 7,757,100; 7,380,140; 6,981,149; 5,761,305; 5,889,865; 5,896,455; 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483; U.S. Pat. Appl. Ser. Nos. 12/018,094; 61/300,772; 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9; PCT/US08/51729; Israeli Pat. App. No. 199983; India Pat. Appl. No. 1422/MUMNP/2009. SPYRUS, the SPYRUS logo, Secured by SPYRUS, Hydra Privacy Card, Hydra PC, PocketVault, Digital Attaché, Rosetta, Rosetta Micro, Secure Pocket Drive, SPYCOS, and Security to the Edge are either registered trademarks or trademarks of SPYRUS, Inc., in the U.S. and/or other jurisdictions. All other company, organization, and product names are trademarks of their respective organizations.