Malware Protection for Today's Threat Landscape

A SafenSec Technology White Paper

Two things are clear in today's corporate security world. One is that every company has installed protection for its computers, and the second is that the bad guys are still getting in. Something is not working.

But we really should not be surprised that anti-virus technology, which has fundamentally not changed since the 1980s, is not up to the task of combating 21st century cyberthreats. Imagine if cell phone technology had remained the same for the past 20 years? We'd still be carrying around bricks that could just about manage a couple of phone calls per battery charge instead of what amount to pocket computers.

This paper presents the rationale behind the development of the SafenSec line of security products and why the technology developed by SafenSoft represents a radical yet rational departure from the "norm" to deliver appropriate protection for networks in the 21st century.

Table of Contents

Common vectors for malware infection

Let's start by reviewing the most common methods by which malware enters a computer in today's world:

- *Removable media autostart*
  When removable media (flash drives, digital cameras, iPods, and other USB devices for the most part) are connected to a PC, the malware code is executed automatically.

- *Software vulnerabilities*
  Malware distributors exploit software vulnerabilities to access vulnerable or unpatched PC(s) across the network and register their malcode in the system as authorized for automatic execution. The actual code used for these exploits is usually very small; its task is to perform a few basic operations that will facilitate the integration of the full malware package into the operating system. In most cases, these exploits simply download an installer module or dropper which is subsequently executed.

- *Social engineering*
  Social engineering is all about tricking users into doing something they wouldn't normally do. Usually the aim of the trickery is to get the user to run an executable file – often in the guise of a codec or (ironically) a spyware removal tool. What actually happens is similar to an exploit – malcode is downloaded and installed on the targeted PC(s).

- *Compromised software*
  Less common than the above three methods, this situation involves malware entering the operating system when it is executed as part of an installer or application. The damage done by this type of vector, however, can be quite extensive, as well as case with the case with the mass propagation of the virus Win32.Virut.

Once malware has gained access to the targeted PC(s), it is loaded into the system RAM and executed and the payload is delivered.

Traditional security solutions and today's threat environment

Now let's take a look at how traditional security products address this new threat environment. Are they up to the challenge?

Anti-virus software

The purpose of traditional anti-virus software is to control the execution of malcode by comparing its signature with a database of signatures for known malcode. This approach is fine in a world where the only concerns are viruses that have been around for a long time and/or that spread very slowly. In today's world, however, when tens of thousands of virus samples appear in security companies' research labs every day, it's simply not feasible to equip customers with a signature for every virus that arrives in the lab. Traditional anti-virus has also proved less than effective with fast-mutating polymorphic viruses that modify their code with each infection, as

little or no identical code may appear in the different infections for signature-based solutions to identify.

Host intrusion prevention systems (HIPS)

Most HIPS solutions control the execution of malware and limit its interaction with the operating system through a proxy of the Windows API. This gives the malware full access to a vast range of Windows API functions. HIPS solutions that permit the execution of code within the operating system cannot control the full scope of operations that malware can potentially perform. From this perspective, it is quite logical that certain elements of the Windows API should serve as the "front door" for cybercriminal attacks, as these elements operate "below the radar" of the HIPS installation.

HIPS cannot be regarded as an effective approach to security, since such systems modify the OS kernel, making the effectiveness of the security system dependent on operating system updates, considerably undermining its stability. At the same time, bugs in the kernel modification code increase the chances of a system crash. Moreover, the security system itself provides the malware with additional privileges, making it more vulnerable to DOS attacks.

Existing HIPS solutions still have many shortcomings. The ubiquitous nature of parameter handling errors found among intercepted system functions in many existing commercial HIPS products confirms this.

HIPS solutions based on network traffic analysis equally fall short of providing effective protection. The purpose-built hardware and software platform that constitutes a network intrusion prevention system (NIPS) is designed to inspect traffic; depending on their configuration and/or security policy, they may easily miss malicious traffic traveling on trusted channels such as HTTP.

Time for a different approach

Clearly neither of the above two approaches, while still valid in the context of yesterday's security environment, are up to the task of protecting computers under attack from all corners in today's threat landscape.

SafenSec goes beyond signature databases and proactively, automatically, defends networks against external threats like hacker attacks and malware activity as well as malicious or accidental data loss from inside threats. The software also enables organizations to control and monitor how users interact with confidential information.

This proactive protection is driven by SafeSec's patent-pending VIPO® (Valid Inside Permitted Operations) technology. Based on system function call interception at the OS kernel (Ring 0) level and loaded ahead of all other applications, VIPO identifies, analyzes and blocks as required:

- Access to file system and registry objects
- Application execution
- Network activities that have the potential to impact security

A versatile rules engine explicitly identifies which actions are to be blocked under what circumstances. Each decision to block or allow a specific system activity is based on a set of multi-level behavioral rules, which allow on-the-fly analysis of complex malcode activity.

Meta rules define the analysis algorithm itself and the system response to various application actions during certain periods of time. The rule base has two parts:

- **System rules** are designed to protect the OS and common applications from known and unknown threats, may not be modified. These rules are created and maintained by SafenSoft engineers.
- **Custom rules** are defined by the system administrator and leverage corporate security policies to protect other applications and privileged information.

All of these elements are controlled through an intuitive graphical user interface that is designed to operate with concepts of trusted applications and confidential information. VIPO-based products provide a solid level of protection out of the box and can be tuned over time to deliver optimal security for every organization.

Inside VIPO

The VIPO technology is at the heart of all SafenSec products, and addresses the challenge of today's network threats head on.

VIPO is designed to prevent malware from installing itself in the operating system and prevent the execution of any software that has not been authorized to run on any individual machine or group of machines. By operating from the core of the computer outwards, VIPO creates a wall around the heart of the machine to prevent the execution of harmful code. It represents a completely different approach to security – one that is extremely well-matched with the needs of today's computing environment.

VIPO makes it possible to prevent the execution of any unidentified code that attempts to infiltrate the operating system. It does this by setting up an isolated environment – or sandbox – in which to safely execute the code without impacting any other part of the computer, using seldom-used functions available within Windows and originally created back in the days of Windows NT.

The original developers of Windows NT were required to comply with federal security requirements that conformed to the specifications published by the Department of Defense's National Computer Security Center (NCSC), specifically the Trusted Computer System Evaluation Criteria. As implemented in Microsoft's operating systems, this becomes C2 Controlled Access Protection, under which no interactivity is possible between malware and the operating system. In practical terms, this means that malware cannot access the operating system, permitted applications, or the clipboard to install eavesdroppers, keyloggers, or other potentially harmful code. It also means that the code and data associated with other processes cannot be altered, nor can executable files be modified without authorization.

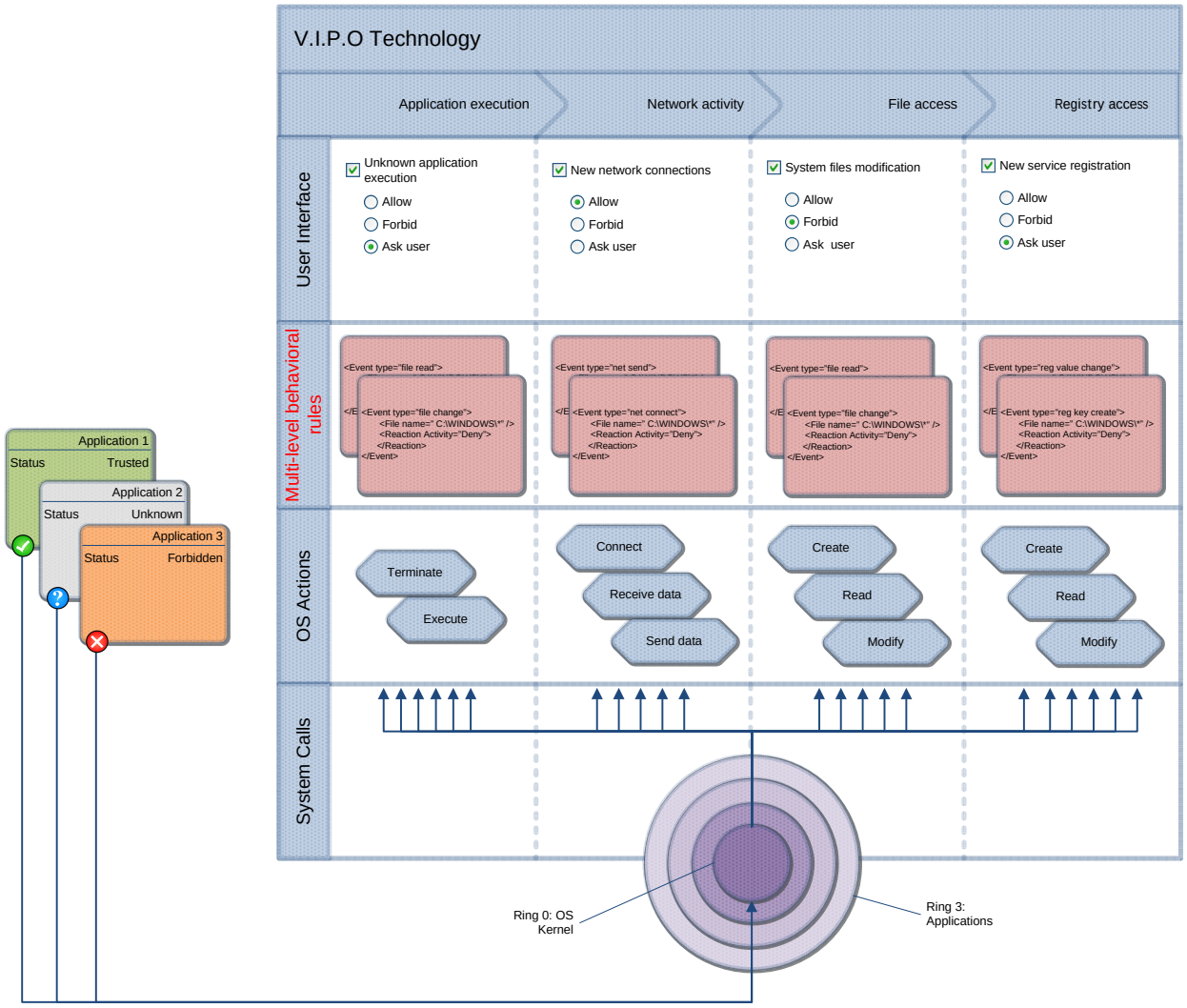

Figure 1: Multi-level behavioral rules are at the heart of VIPO protection

Unlike any other HIPS solution, SafenSec's VIPO controls the full range of potential malware activities without compromising the integrity of the operating system kernel via access token modification or the use of Discretionary Access Control Lists (DACLs). Additionally, VIPO protects users from software input simulation techniques – the imitation of keystrokes or mouse movements – through a "safe user alert" display.

By taking this approach, SafenSec software ensures that potentially vulnerable applications such as browsers, peer-to-peer networks, and e-mail clients are allowed to run only with certain limitations imposed by the security system. Such applications are identified at runtime by the security system and executed in a special environment, under a restricted-access user name, which prevents the application from making any unauthorized file or registry modifications. This is particularly important for the prevention of exploit installation, as well as to support the system profiling technology described above. Applications can be added to this list by the system administrator at any time.

Evaluating VIPO

When evaluating any SafenSec product containing VIPO, bear the following in mind:

1. VIPO's main objectives are: to deny OS access to any software, including modules and components, and to prevent the execution of any application that has installed itself or is trying to install itself onto a target PC without the permission of the user ot the system administrator.

2. Whenever a user runs a suspicious application, the security system creates a secure sandbox environment by default. This is done to prevent any of the following:

    a. Operating system integration (autostart privileges), the alteration of modules within other applications or the operating system itself.
    b. Access to sensitive data – ie any privileged information stored in a user's profile or documents folder, as well as other folders specified by the user or system administrator.
    c. Modification of the code or the data pertaining to other processes or thread contexts; the launch of independent processes or the termination of other users' or processes' threads.
    d. Keyboard input monitoring by proxy by global eavesdroppers or Ring) modules/drivers (keylogger defense).
    e. Read or write access to data stored in the Windows clipboard.
    f. Stripping away an application's access rights or administrator privileges

The above limitations notwithstanding, the most commonly used programs, such as audio and video players, image viewers, etc, retain full functionality in this mode. Remember that such applications are frequently used as bait in social engineering attacks.

Attention should also be paid to VIPO's unique approach to setup files. VIPO includes an intelligent analyzer that can identify and run installation packages in isolated sandboxes. If the installation package includes the digital signature of a trusted publisher, the entire process is transparent to the user. After installation, the software functions normally and does not – as older HIPS solutions often do – continuously pester the user with questions about the legitimacy of the application.

If, on the other hand, the installation package does not include a trusted digital signature or appears to be corrupt, the user is given the option of running the application in an isolated environment and/or denying that application access to the operating system. You can also use a traditional virus scanner to supplement this process and perform an on-demand scan as soon as an executable alert occurs but, as we know, a scanner cannot make any guarantees.

By allowing the software to run in a secure sandbox, it is possible for the user to study the application's behavior in isolation and without risk to the rest of the system. SafenSec's user interface offers the option to log the activity of such applications, which enables the application to be properly assessed for trustworthiness and either allow its installation or ban it from future execution.

Real-world testing

To perform a real-world test of SafenSec VIPO technology, follow these instructions in your testing lab:

1. Install the OS to be tested, the necessary software and the SafenSec product. A traditional signature-based malware scan is run as part of the system profiling stage to ensure no malware is present on the base system. However, it must be realized that SafenSoft cannot guarantee that the system is malware-free at setup; SafenSec itself is not intended to function as a traditional anti-virus system but to complement such systems.

2. Check whether there are any opportunities for the successful installation of an unauthorized application or the integration of malware into the tested system by means of exploiting software vulnerabilities. This can be done by imitating regular PC usage – clicking links and opening web pages, downloading files and engaging in other online activities, as well as attaching infected removable media to the tested system. Also ensure that all available security patches and updates have been applied.

3. Test SafenSec VIPO's capabilities by running an unidentified application in an isolated environment. You can try executing known malcode (introduced onto the system after installing SafenSec) and allow its execution as the default option by pressing the Allow button in the alert window. It's also important to check whether there are opportunities for:

    a. system installation (autostart registration or modification of software modules associated with other applications or with the operating system
    b. theft of important data from the user profile or other files and folders specified by the user
    c. corruption of code or data associated with other processes, thread context alternation, running new threads, or terminating the threads of other processes.
    d. keylogging by means of global eavesdroppers or internal Ring 0 modules
    e. Windows clipboard data access or modification
    f. unauthorized access to system administrator access privileges.

If you have any questions during SafenSec testing that are not covered in the software documentation or in the tutorials on our website at http://www.safensoft.com/security.phtml?c=611, please contact support@safensoft.com with full details of your testing environment (operating system and application version and patch numbers).

Summary

SafenSec's VIPO technology has been specifically designed to fill the gaps in network security left by traditional anti-malware and HIPS products. It also brings the considerable benefit of freeing corporations from the tyranny of constant signature updates. Because SafenSoft is not in the traditional anti-virus business, the company has no vested interest in keeping its customers on a continuous renewal wheel; when an organization adopts SafenSec as a supplement to, or replacement for, a traditional anti-malware product, there is a one-time licensing fee and a small annual fee for support and integration services. It's totally transparent, and can be reliably budgeted for year after year.

About SafenSoft

SafenSoft was founded in Moscow in 2006 around the concept of hardcore DRM technology. Today, with offices in Silicon Valley, Southern California and Moscow, SafenSoft is a leading international developer of innovative corporate and personal information security products. SafenSoft's solutions are built around a unique technology core that combines adaptive profiling, sandboxing, and a behavior-based rules engine to deliver dynamic, proactive application integrity. The company's management team draws on experience at Kaspersky Labs, McAfee, Trend Micro, Symantec, Entercept, CA, and other major security vendors. SafenSoft works with channel partners in 20 countries and is backed by Troika Dialog venture fund.