

Introduction

What are the objectives of the modern malware security systems and how are they implemented? Let us try and observe how malware intrudes the targeted PC and what happens next.

The most common sources of malware are as follows:

- **Removable media autostart.** When removable media (flash drives for the most part) are attached to one's PC, the malware code is executed automatically.
- **Software vulnerabilities.** The perpetrators use security exploits in order to load malware modules into the targeted PC and register them in the system as subject to automatic execution. The actual code of a security exploit is usually minimal volume-wise due to certain coding limitations; its task is to perform a few basic operations aimed at the integration of the harmful code into the OS. In most cases, such exploits download installer modules, also known as droppers, which are subsequently executed.
- **Social engineering.** The essence of this method is as follows: the user is tricked into running an executable presumably used for opening files of an unknown format, self-extracting archives or some such – in reality, the application in question installs malware on the targeted machine.
- **Compromised software.** In this case the malware enters the OS when it gets executed as part of some application, installer etc. This method is less common than the above three; however, the damage from virus epidemics spread by infected software can be quite formidable, as was the case with the mass propagation of Virus.Win32.Virut.

The intrusion of malware into the targeted PC is followed by the next stage – the malware code is loaded into the system RAM and executed.

Antivirus software

The purpose of classical antivirus software is to control the execution of harmful code, whose signature is compared to those contained in the database. This approach may yield certain results in the treatment of an existing infection; however, it cannot protect one from unidentified threats. No classical antivirus product can protect the user from the entire range of existing harmful software

HIPS

The overwhelming majority of HIPS systems control the execution of malware and limit its interaction with the OS by proxy of the Windows API interface. This provides the harmful code with full access to a vast range of Windows API's functions. HIPS systems that permit the execution of code within the OS cannot control the whole scope of operations that malware is potentially capable of performing. It is only logical that certain features of the Windows API interface, which are in no way controlled by the security system, should serve as the "front door" for cybercriminals' attacks. The above can hardly be regarded as an effective approach to security, since such systems modify the OS kernel and thus make the efficacy of the security system dependent on OS updates, considerably undermining its stability, while the bugs in kernel modification module code increase the chances of a system crash. Moreover, the security system itself provides malware with extra privileges and makes the machine more vulnerable to DOS attacks. Unfortunately, the existing HIPS systems still have many shortcomings. The ubiquitous nature of parameter handling errors found among the intercepted system functions in a variety of products such as Kaspersky, Outpost, DefenceWall etc confirms it.

Safe'n'Sec 2009

The philosophy of Safe'n'Sec® V.I.P.O.® is **to prevent the installation of malware in an operating system (performed as a result of social engineering, for instance) and forfend the execution of unauthorized intruder software.** This translates as complete protection of the system from the execution of harmful code. What we offer is a whole new approach to security.

The system profiling technology makes it possible to prevent the execution of any unidentified code module that may enter the operating system. The V.I.P.O.(R) technology creates an isolated environment used for the execution of unidentified applications, taking full advantage of the features offered by the NT family of the Microsoft Windows OS. The developers of the NT OS family were under obligation to comply with federal and industrial security requirements. Security labels conform to the specifications published by the National Computer Security Center, or NCSC, of the USA Department of Defense. The specifications taken into account in the development of the security architecture of this operating system family are the Trusted Computer System Evaluation Criteria, which rate it C2 - Controlled Access Protection. No "dialog" is possible between the malware and the operating system. It is impossible to access sensitive information or the clipboard, install eavesdroppers, keyloggers or any other harmful software under these conditions. It is also impossible to alter the code and the data associated with other processes or perform unauthorized modification of executable files.

Unlike any other HIPS system, the Safe'n'Sec V.I.P.O.® controls the whole scope of possible malware activities without compromising the primordial integrity of the OS kernel via access token modification and the use of discretionary access control lists, or DACLs. Additionally, the Safe'n'Sec V.I.P.O.® technology protects the user from software input simulation (imitation of keystrokes or mouse movements) via the safe user alert display.

The philosophy of Safe'n'Sec® implies that potentially vulnerable software (such as browsers, BitTorrent and e-mail clients etc) should be run with certain limitations imposed by the security system. This software is identified by the security system at runtime and executed in a special environment under a restricted access user name, which prevents it from unauthorized file or registry modification. This is particularly important for the prevention of security exploit malware installation, as well as the system profiling technology. Safe'n'Sec is currently capable of identifying the following programs and restricting their privileges:

- Microsoft® HTML Help
- BitTorrent
- uTorrent
- Opera Internet Browser
- Mozilla Firefox
- Internet Explorer
- Download Master
- Winamp
- AIMP2
- Windows Media Player
- The KMPlayer
- Light Alloy
- Microsoft Office Outlook
- Microsoft Office Word
- Microsoft Office Excel
- The Bat! E-Mail Client
- Miranda IM
- Quiet Internet Pager
- Skype
- Adobe Reader
- DjVuViewer

The user can add any application to this list at any time and use the Safe'n'Sec interface to prevent any cybercriminal from taking advantage of the application's vulnerabilities.

Methodology

The following is to be taken into account when the Safe'n'Sec® V.I.P.O® is tested :

1. Safe'n'Sec® V.I.P.O® considers its main objectives to be as follows: **to deny OS access to any software, including modules and components, and to prevent the execution of any application that has installed or is trying to install itself onto the target PC without the participation of either the user or the administrator.**
2. Whenever a user runs a suspicious application, the security system creates the following environment by default. This is done to prevent any of the following:
 - OS integration (autostart privileges) or the alteration of program modules of other software or the operating system itself;
 - access to sensitive data (any private information stored in a given user's profile or Documents folder as well as other folders specified by the user).
 - 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' and processes' threads;
 - keyboard input monitoring by proxy of global eavesdroppers or Ring-0 modules/drivers (keylogger defense);
 - read or write access to the data stored in the Windows clipboard;
 - stripping away the access rights or system administrator privileges of an application.

The above limitations notwithstanding, the most commonly used programs such as audio/video players, picture viewers etc retain full functionality in this mode; one must remember that such applications are very often used as bait in social engineering. One must emphasize the unique approach of Safe'n'Sec® V.I.P.O® to setup files. The package includes an intellectual analyzer capable of finding installation packages and running them in isolated installation mode. If the software package of the PC owner possesses the digital signature of a trustworthy publisher, the entire setup process is perfectly transparent to the user; after the installation, the software functions within the OS without the need to pester the user with countless questions regarding illegal activity – a trait common for all the older HIPS systems. Should the installation package lack the digital signature of a reliable publisher or turn out to be corrupt, the user will be offered the default options of running it in an isolated environment or denying it any access to the operating system. One can also use a classical signature scanner as an auxiliary security measure and perform a scan as soon as one sees an executable alert, but a scan cannot guarantee anything remotely resembling perfect safety. If such software is run in default mode, the user can also study the behaviour of the application with every potential security threat minimized. The interface offers the option of logging the activity of such applications, which makes it feasible to estimate the application's trustworthiness at first run and either install the software or ban it from future execution.

In order to perform a live check of Safe'n'Sec® V.I.P.O® and its functions, one must:

1. Install the OS to be tested, the necessary software and the Safe'n'Sec® V.I.P.O® security system. Since no intrusion prevention system is oriented at the restoration of already compromised systems, a malware-free OS is implied. Seeing as how it is possible that users will install our product on compromised systems, we do actually use a classical signature scanner during the system profiling stage. However, it is very important to realize that we cannot guarantee that the user will end up with malware-free system – after all, the treatment of existing infection is the task of regular antivirus software as opposed to intrusion detection systems.
2. Check whether there are any opportunities for the successful implementation of an unauthorized installation, or

the integration of malware into the tested system by means of exploiting software vulnerabilities or the alleged shortcomings of Safe'n'Sec(R) V.I.P.O.(R). 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 etc.

3. Try out the V.I.P.O.(R) in action by running an unidentified application in an isolated environment. You may execute a known malware module on the tested system (introduced after the installation of Safe'n'Sec® V.I.P.O®) and allow its execution as the default option (by pressing the Allow button in the alert window). One must check whether or not there opportunities for:

- system installation (autostart registration as well as the modification of the software modules associated with other applications or the operating system);
- theft of important data from the user profile as well as the files and folders specified by the user;
- corruption of code or data associated with other processes, thread context alteration, running new threads or terminating the threads of other processes;
- keylogging by means of global eavesdroppers or internal ring-0 modules;
- Windows clipboard data access or modification;
- unauthorized access to system administrator access privileges.