



The Stuxnet Virus

How Vir2us Immunity™ defeated the Stuxnet Virus before it was created.

Case Study: The Stuxnet Virus

How Vir2us defeated the Stuxnet Virus before it was created.

Vir2us (pronounced, Virtuous) is a Silicon Valley based technology firm that has created the first technology solution that makes enterprise computing systems inherently immune to hacking, viruses, spyware and related network security threats. The Vir2us suite of patented and proprietary technology solutions are designed to end the fundamental problem of computer security threats from hackers, cyber terrorism, viruses, and myriad related threats, while remaining transparent to users of desktop computer software applications. Vir2us inherently protects against new and previously unknown threats.

What is “Stuxnet?”

Stuxnet is a computer worm discovered in July 2010. It targets Siemens industrial software and equipment running on Microsoft Windows. While it is not the first time that crackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller rootkit.

The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens Supervisory Control And Data Acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Stuxnet infects PLCs by subverting the Step-7 software application that is used to reprogram these devices.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface. While it is not completely unproductive to take a look at each of the different components of Stuxnet to understand how the threat works in detail, we need to keep in mind that the uniqueness of the Vir2us Immunity technology is that we need not know how the threat works or even be aware of its existence in order to defeat it.

Different variants of Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran; Symantec noted in August 2010 that 60% of the infected computers worldwide were in Iran. Siemens stated on November 29 that the worm has not caused any damage to its

customers, but the Iran nuclear program, which uses embargoed Siemens equipment procured clandestinely, has been damaged by Stuxnet.

Stuxnet is quite sophisticated, but really nothing entirely new. It pieces together a legacy fabric of virus, Trojan and worm techniques to increase infection rates and protect itself. This is all a piece of malware needs to do:

- spread and infect
- avoid detection/removal
- deliver its payload

Stuxnet is considered advanced because it uses sophisticated means to accomplish these steps. Examples include:

Multiple infection vectors

- attacks a known vulnerability in the Server Service on Windows
- attacks local networks and spreads through shared network files
- copies itself on to attached USB flash drives and infects subsequent hosts via the Auto-Run feature of Windows.

Self-preservation

- disables security software and updates
- deletes system restore points
- blocks websites that provide patches
- blocks anti-virus and security websites

Self-updating

- authenticates its own updates
- generates tens of thousands of domain names that its master can register and use to deliver updates
- peer-to-peer push and pull mechanisms for updating associated corrupted computers

Once an “army” of computers is in place, (i.e. computers that can be harnessed to run any program the remote “master” wants), its potential is limited only by the imagination of its master:

- delete all files on the computer (or threaten to) unless a ransom is paid
- flood a targeted website to create a “Distributed Denial of Service”
- spread more malware with new purposes
- harvest financial records and personal information

- extortion
- flood the Internet with fraudulent sales and money-scheme emails (SPAM)

According to SRI International, the reason *“why Stuxnet has been able to proliferate so widely may be an interesting testament to the stubbornness of some PC users to avoid staying current with the latest Microsoft security patches. Some reports, such as the case of the Stuxnet outbreak within Sheffield Hospital's operating ward, suggest that even security-conscious environments may elect to forgo automated software patching, choosing to trade off vulnerability exposure for some perceived notion of platform stability.”*¹

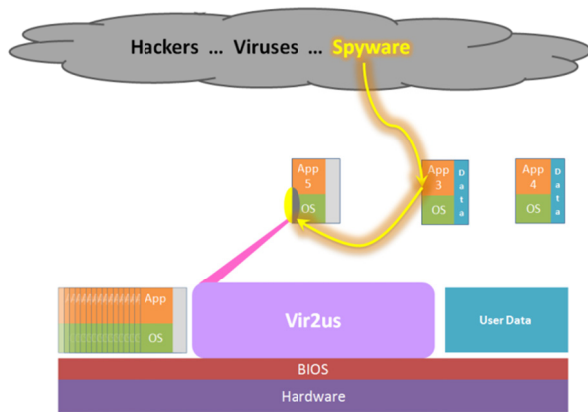
Indeed, *“The decision to disable automatic security updates was taken during Christmas week after PCs in an operating theatre rebooted mid-surgery”* according to *The Register*.² *“But for anyone who has been following botnets, Stuxnet isn't so much something that seems surprising as much as something that seems inevitable that will mostly likely be soon surpassed by another even smarter form of botnet campaign... it's actually already yesterday's news.... Is the story here that the mainstream is finally getting a fix on botnets? Well, that's good, but only about five years too late,”* Matthew Hines – *eWeek*.³

Vir2us Technology –

By inventing a secure methodology and architecture for isolating all processing events, any attempt at malicious activity will be frustrated by an inability to access or affect the computer. In fact, malicious code will be unable to persist within the computer after an infected program has been shut down. The core technology principles are applicable to nearly every computing device. Vir2us plans to leverage its fundamental development activities across multiple products and multiple marketplaces.

Vir2us patented technologies are based on four fundamental concepts:

- A multiplicity of thoroughly isolated and pristine computing environments to independently support individual file processing without exposing system resources or data to unauthorized manipulation.
- A trusted computing base existing outside of the computers operating system and securely isolated from all processing events.
- A logically structured set of rules for isolated program execution and controlled data access, rigidly enforced from the impenetrable computing base.
- A reservoir of application templates with uncorrupted, factory-fresh program code that are used to launch every computing environment with both an operating system and an installed application.



Incremental programs not launched by Application Templates are also run within dedicated, Isolated Computing Environments (ICEs). If they contain Spyware or Virus code, they can only infect or spy on themselves, or commit malicious suicide.

How does Vir2us defeat Stuxnet? –

The innovative architecture of the Vir2us core technology actually defeated the Stuxnet worm before the worm was ever conceived.

The core mechanism that achieves this includes four fundamental steps:

- 1.) Create multiple, Isolated Computing Environments
- 2.) Redirect and isolate files, programs and activities in the computer, without user knowledge or awareness
- 3.) Spawn pristine, Isolated Computing Environments *before* processing is attempted
- 4.) Discard each computing environment after a single processing activity

The following describes the primary vectors that Stuxnet uses to infect computers, and discusses how Vir2us handles them:

USB storage device attacks via Auto-Run –

When any USB storage device is plugged into a Vir2us computer, Vir2us spawns a new, pristine and Isolated Computing Environment, and redirects the USB Auto-Run to launch there instead of in a common (primary) computing environment. The user is unaware that this has happened, and simply sees a normal file explorer window for the USB key, as with a typical Windows computer.

When the USB key is removed, the Computing Environment in which it was opened is discarded. In this way, if the USB key is infected, it only infects the Isolated Computing Environment in which it ran. The next time the USB key is inserted, the process repeats itself, starting with a pristine, Isolated Computing Environment.

Exploits hole in Server Service on Windows –

Vir2us runs individual programs and services in Isolated Computing Environments, each one containing its own isolated copy of Windows. Thus, if a Windows hole is exploited, the worm can only infect the Isolated Computing Environment that is running that particular instance of the service that contains the hole and the infection will only persist as long as that Isolated Computing Environment is operating. This is because each computing environment is isolated from the rest of the system.

This stealthy exploitation of holes in the Windows operating system is similar to Stuxnet's other vector of attack:

Attacks local networks and spreads through shared network files –

Again, the same Vir2us architecture principals apply. Any processing of shared network files is isolated from the rest of the system, such that any potential infection is contained within its own Isolated Computing Environment. Upon completion of the files processing and storage function the used Computing Environment is discarded. Further, Tom Cross, X-Force researcher in the IBM ISS division, puts it this way:

*"If it [Stuxnet] copies itself to a file share, and if the user clicks on a file, the user's computer will get infected... even if the computer is patched, you can still get infected if you access one of the infected USB drives or file shares." Cross advises that Auto-Run be disabled.*⁴

As discussed, files, programs and activities are isolated, such that Auto-Run can be allowed to run normally and the system will remain protected from both known and unknown threats.

In summary, the **Vir2us** suite of solutions takes a unique and different approach to secure computing by fundamentally changing legacy protocols for the utilization of computer hardware and software. The **Vir2us** solution makes secure computing proactive, rather than reactive, and operates below the OS to deliver higher performance and a transparent user experience with peak performance. The Vir2us architecture inherently protects the user by changing the way in which a computer accesses its data and programs by using default isolation mechanisms. This is accomplished transparently, without changing the user experience or requiring any change in user behavior.

