



WHITEPAPER

RETURNIL VIRTUAL SYSTEM: Maximizing Security, Minimizing Costs

It is becoming increasingly difficult to combat malware and manage the systems required for protection. This white paper explains why anti-virus and anti-malware solutions are failing and how organizations can boost their security and reduce their management costs.

Contents

Overview.....	3
The Malware Landscape.....	3
The Rise of Crimeware.....	3
Increasingly Complex Attacks Make Defending Systems More Problematic.....	4
Email Viruses On The Rise.....	5
Fighting a Losing Battle.....	5
The Cost to Business.....	6
Returnil Virtual System: Real Security.....	6
How Returnil Virtual System Works.....	6
Benefits of Returnil Virtual System.....	7
Conclusion.....	7
About Returnil.....	8
References.....	8

Overview

It is becoming increasingly difficult to combat malware and manage the systems required for protection. This is true for organizations of all sizes, from small to medium-sized businesses to the largest multinational enterprises. Driven by the potential of enormous profits, malware creators are deploying increasingly sophisticated techniques in order to evade security solutions – and they are also becoming increasingly successful.

This white paper explains why anti-virus and anti-malware solutions are failing and how organizations can boost their security and reduce their management costs.

The Malware Landscape

In 2008, a study found that 23% of home computers and 72% of corporate networks with more than 100 workstations were infected by malware¹. What makes this study both alarming and somewhat surprising is that it was conducted by Panda Security: a vendor of anti-virus and anti-malware solutions. It was, in effect, an admission that traditional security solutions cannot be relied on to provide protection from viruses and other forms of malware.

To understand why traditional, anti-malware solutions are failing, it's necessary to understand how the malware landscape and the motivations of those who create malware have changed.

In the past, most viruses were created by teenagers such as Sven Jaschan, the 18 year old German student responsible for the infamous Sasser and Netsky worms. These self-taught script kiddies designed viruses in order to earn recognition in underground communities and their wares, although destructive, were usually easy to detect and easy to block – and very often did not work as planned. However, times have changed.

The Rise of Crimeware

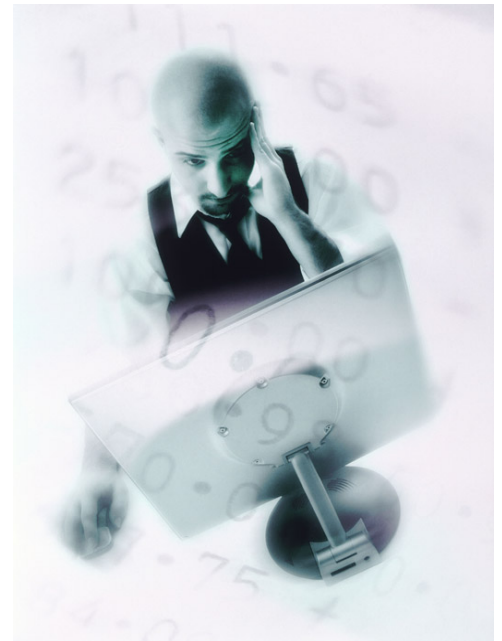
Malware is no longer the domain of mischievous script kiddies; instead, the majority of malware is created by skilled coders employed by organized, criminal gangs. It is designed with a single, specific objective: to enable those gangs to steal money.

The business models and processes used by the criminals have become increasingly sophisticated and complex. Computers infected with malware become co-opted into a network of similarly infected computers, (a botnet). The owner of the botnet will then rent it out to criminals who use it to relay spam and for other

illegal activities. (The Srizbi botnet was able to send out an estimated 60 billion spam emails per day). The spam emails serve a variety of purposes: for example, they may contain links that will lure users to phishing websites, contain bogus stock tips intended to artificially increase or decrease share prices, (pump-and-dump scams), or simply contain links which lead to infective websites in an attempt to co-opt other computers into the botnet.

Such scams can make their perpetrators a considerable amount of money. For example, in June 2009, a man admitted various charges relating to a spam and pump-and-dump scam which netted him and his co-conspirators an estimated \$3 million². And according to Gartner, 3.6 million people in the U.S. lost a total of \$3.2 billion to phishing attacks during the 12 months up to August 2007³. That's \$3.2 billion in the hands of spammers and cybercriminals. To put it simply, malware creation has become a multi-billion dollar industry.

To succeed in their scams, malware creators and the gangs that finance them need to get their malware onto people's computers . Because the profit margins are so great, they are motivated to find and use increasingly sophisticated techniques to ensure that their malicious programs are able to evade detection.



Increasingly Complex Attacks Make Defending Systems More Problematic

Viruses used to be spread almost exclusively by email, however, as email systems became increasingly hardened and less vulnerable, attackers started to look for other propagation mechanisms and found the Web to be the ideal candidate. The sheer number of operating system, browser and browser plug-ins, such as Flash and QuickTime make the Web a perfect vector for distributing malware. Links in spam emails and social media sites are used to lead people to infective websites. Thousands of these websites appear each and every day and a frequently live for only a very short period of time, (often less than 24 hours), which enables them to evade detection by web filters and other URL blacklisting mechanisms. Similarly, web application vulnerabilities enable legitimate websites to be compromised and used to deliver malware to unsuspecting visitors. This is a common occurrence. The websites of embassies, government departments, retailers and social networking sites have all been hijacked and used in this manner.

While such attacks are becoming increasingly commonplace, they are also becoming increasingly sophisticated, often cycling through multiple browser and browser plug-in vulnerabilities until an exploitable weakness is discovered. Additionally, attackers make use of packaged modules and other obfuscating techniques in order to conceal from anti-virus solutions the malicious payloads these websites host. Similarly, modular Trojans – installed via a drive-by-download from a compromised site – seek to disable installed security solutions prior to downloading additional malicious software. Highlighting the severity of the threat, the SANS Institute listed “Increasingly Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web Sites” in number one position on its *Top Ten Cyber Security Menaces for 2008 list*⁴.

In short, each time one of your organization’s computers is used to visit a website - even a trusted website - it is at risk of being infected by malware.

Email Viruses On The Rise

While the Web may have become the attack vector of choice, email viruses nonetheless continue to be a risk and are, once again, on the rise. According to Web and messaging security company CommTouch, successive and massive increases in the number of new malware variants enabled millions of virus-laden emails to bypass many major anti-virus engines during the second quarter of 2009⁵. The CommTouch report also noted that spammers are becoming increasingly inventive and again finding ways to enable image-based spam to slip by spam filters, creating additional problems and challenges for businesses.

Fighting a Losing Battle

The vendors of traditional anti-virus and anti-malware solutions are fighting a losing battle. Between 2006 and 2007, the number of new strains of malware identified more than doubled. In 2008, Google announced that



the company’s researchers had discovered more than 3 million malware-serving URLs⁶ – and, due to the ephemeral nature of such URLs, that was probably no more than the tip of the iceberg. PandaLabs claim to have identified more than 15 million strains of malware in 2008⁷. In short, anti-virus vendors simply cannot keep up with the exponentially increasing volume of ever more complex malware – and that is resulting in more and more computers and networks being compromised.

The Cost to Business

Businesses spend enormous sums attempting to secure their infrastructures against malware. Simply managing the installed security solutions eats up as considerable amount of IT's time – and time, of course, is money. In 2008, the worldwide revenue from the software security market totalled \$11.3 billion, up 18.6% from 2007. Despite this increased spending, businesses continue to be landed with substantial remediation bills: according to the Cyber Security Institute, costs of the Conficker worm alone could run to as much as \$9.1 billion⁸. Similarly, according to one study, 13% of IT pros felt that the vulnerability of their organization to breaches and malicious code was worse in 2008 than in 2007⁹.

Clearly, increased spending does not equate to increased security. There has to be a better a solution.

Returnil Virtual System: Real Security

While mainstream vendors continue to fight a losing battle against a barrage of increasingly sophisticated malware, Returnil have taken a completely different approach to security – an approach which uses a blend of technologies to provide unprecedented protection from viruses and other forms of malware while simultaneously easing the management overhead.

How Returnil Virtual System Works

Returnil Virtual System (RVS) uses a combination of virtualization, anti-virus and cloud technologies to overcome the shortcomings of conventional security solutions.

Upon installation, RVS automatically scans the system for viruses and other malicious software. The scan is performed using both local malware signatures and, in order to ensure up-to-the-second accuracy, a cloud database of signatures. Should any infections be found, RVS can remove them in much the same manner as any other anti-virus solution. But that is where the similarity between RVS and other security solutions ends. Once the system has been confirmed to be free from malware, RVS clones – or copies - the system partition and runs the cloned copy in a virtual machine. Users are automatically booted into the virtual machine and perform their day-to-day work within the virtual environment, rather than using the underlying operating system. While users are working within the virtual environment, the operating system is held in a secure, encrypted state and is, therefore, completely immune to malware that may infect the virtual system. The virtual system persists only for the duration of the session, with a new virtual system being created each time the system is restarted. Consequently, a simple reboot will eradicate any malicious software that may have been installed on the virtual system.

RVS is almost completely transparent to end-users and has zero impact on productivity. While working in the virtual environment, users have the option of saving documents and files using RVS' File Manager Feature so that their data will not be lost when the system is rebooted.

Benefits of Returnil Virtual System

RVS offers a broad range of benefits including:

- **Unprecedented protection from malware:** when RVS is installed, only the virtual system is exposed. The operating system and applications remain in a secure, encrypted state. Should malware become installed on the virtual system, it will automatically be eliminated when the computer is rebooted.
- **Protection from unwanted system changes:** RVS provides administrators with an easy way to enforce policy on workstations. While users may be able to alter system settings within the virtual environment, those changes will be lost when the computer is rebooted.
- **Reduced management overhead:** RVS drastically reduces IT's workload, enabling technical staff to concentrate on core business functions instead of having to clean up viruses and deal with problems caused by users altering default system settings.
- **Downtime eliminated:** with RVS installed, expensive unscheduled downtime is eliminated, ensuring that mission-critical business applications are available 24/7/365.
- **Optimized performance:** RVS has minimal impact on performance and, as it solves the problems associated with malware and unauthorized software installations, helps ensure that computers are performing optimally. Users are, in effect, starting with a freshly installed version of Windows every time that they boot their PC.

Conclusion

Malware is becoming an increasingly serious problem as its creators are becoming ever more adept at circumventing conventional security solutions. Despite spending billions of dollars annually on security solutions, business are as vulnerable today as they were in the past.

Returnil Virtual System represents a solution to the problem and provides businesses with an easily managed and unobtrusive way to protect their data against the vast array of threats which are too often undetected by mainstream security solutions.

About Returnil

Returnil is a privately held company with offices in Helsinki, Finland; St. Petersburg, Russia and Nanjing, China. Founded in 2007, Returnil is led by a strong executive team with many years of experience in managing and developing security companies and solutions and is backed by a range of private investors including VTB - Venture Fund.

Returnil uses advanced technology to provide innovative security solutions for enterprises of all sizes and for home users. Returnil's mission is to provide both businesses and home users with a more effective way of securing their computers and networks. To learn more about Returnil, please visit www.returnil.com.

References

¹ Panda Security

<http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9077&sitepanda=particulares>

² CRN

<http://www.crn.com/security/218100991;jsessionid=2EJ31NOELXD44QSNL0SKHSCJUNN2JVN>

³ Gartner

<http://www.gartner.com/it/page.jsp?id=565125>

⁴ SANS Institute

<http://www.sans.org/2008menaces/>

⁵ CommTouch

<http://www.commtouch.com/press-releases/new-trojan-variants-evade-major-anti-virus-engines-says-commtouch-report>

⁶ Google

<http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html>

⁷ PandaLabs

http://pandalabs.pandasecurity.com/archive/Can-we-cope-with-the-increasing-malware_3F00_.aspx

⁸ Cyber Security Institute

<http://cybersecureinstitute.org/blog/?p=15>

⁹ InformationWeek

<http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=208800942&pgno=1&queryText=&isPrev=>