



Protecting Client Systems from the Crimeware Invasion

Protecting Client Systems from the Crimeware Invasion

Contents

The new threat landscape	4
Through the backdoor	6
Mobile workers	6
Remote workers	7
Peripheral devices	8
Personal email	8
Closing backdoors and stopping crimeware	9
Virus protection and remediation	9
Spyware protection and remediation	10
Vulnerability-based intrusion prevention	10
File-based intrusion prevention	11
Inbound and outbound traffic control	12
Integrated client protection	13
Conclusion	14

Protecting Client Systems from the Crimeware Invasion

The IT threat landscape has changed from one where individual glory-seeking hackers work to see how many network operations they can disrupt to one where organized crime makes a concerted and financially motivated effort to silently steal confidential information from specific organizations. Ignoring traditional IT perimeter defenses, this new breed of hackers enters networks through the backdoor, frequently hitching rides on laptops, tunneling into the network through VPN connections opened by remote users, sneaking in via smartphones, or hijacking instant messaging sessions. Once on the inside, they employ complex, stealthy crimeware methods to collect passwords, credit card information, bank account numbers, customer records, or any other type of information that they can profit from. The true goal of these new attacks is to gain unauthorized access to your systems and information on an ongoing basis.

For organizations, not only is the threat of information theft real, but there is also a real impact on the organization with every successful infection. When spyware or adware infects the endpoints, end users see their system speed and productivity grind to a slow pace. Help desks are inundated with support calls from unhappy users that can't access information or run business-critical applications. Worst of all, IT administrators don't have enough time and staff to continually track down, quarantine, and repair infected endpoints.

These new and sophisticated types of threats and attacks require new levels of protection on an organization's client systems. While antivirus technology can play an important role in the defense, it must be joined by a coordinated, multilayered defense that includes proactive vulnerability-based intrusion prevention, file-based intrusion prevention, and inbound and outbound traffic control.

The new threat landscape

Only a few years ago the majority of threats to the well-being of an organization's computing infrastructure came from glory-seeking hackers that simply wanted to impress their friends. Virus and worm authors unleashed their creations with a shotgun approach in an attempt to hit as many targets as possible. They typically didn't care who suffered from their attacks as long as the results were disruptive and readily noticeable to the world. In many ways, being hit by such an attack was like being tagged by graffiti—highly visible and a nuisance, albeit sometimes an expensive nuisance.

Protecting Client Systems from the Crimeware Invasion

But the threat landscape has changed. The shotgun paradigm has shifted to a sniper rifle paradigm. The majority of today's threats have specific targets, and the attacks are now silent, often going unnoticed until it's too late. The reason that the threat paradigm has changed is that the perpetrators of attacks and their objectives have changed. Glory-seeking individuals are not the ones behind these new-style attacks. The instigators come from the depths of organized crime, bent on reaping financial gains.

Often data theft becomes the goal of a targeted attack, including customer account information from credit card companies and banks, competitors' business plans, employee records, and corporate financial data prior to an IPO or announcement that could affect a company's stock price. Some attacks are stepping-stones to uncovering even more confidential data, such as when Trojans gather personal passwords and users' keystrokes, or track visited Web sites. An attack could also have the sole purpose of a tarnishing a company's corporate image or weakening the strength of their brand.

Stolen data might be used by the attacker, given to the client who hired the attacker, or sold to the highest bidder. The financial implications of data theft are nearly endless: stolen funds, lost profits, government fines, customer lawsuits, employee lawsuits, and more.

But stolen data isn't the only means for this new breed of attackers to reap financial gain. Some attackers have resorted to blackmail, threatening to unleash an army of 50,000 bots against an organization's online commerce network unless the organization agrees to pay them an exorbitant sum of money. Other attackers have used Trojans to encrypt valuable information on an individual's hard drive, virtually holding that data for ransom until the victim agrees to pay to have the data unencrypted.

Multipurpose bots, Trojans, and spyware programs form the crimeware arsenal of today's hackers and are regularly bought and traded on the black market. Unlike viruses of the past, the development of crimeware is not an after-hours hobby. It is professionally developed, with its creators working on it as their full time job. The price tag for a piece of crimeware typically ranges between \$100 and \$1,000, but it's reported that the WMF exploit sold for as high as \$4,000. Ultimately, the selling price for any crimeware is usually based on its ability to steal sensitive data and its potential to make the wielder of the crimeware richer.

Trojan Programs

Trojan programs pretend to be harmless, normal files and software but are actually malicious software that could potentially steal passwords, destroy data, or otherwise allow a hacker to use the compromised computer without the user's knowledge. Increasingly, Trojans are the first stage of an attack, and their primary purpose is to stay hidden while downloading and installing more sophisticated threats such as a bot.

Bots

Bots often spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. After they infect a machine, they stay hidden until they are awoken by their controller to perform automated tasks such as sending spam or knocking Web sites off the Internet as part of a coordinated "denial-of-service" attack. Since a bot-infected computer does the bidding of its master, these victim machines are referred to as "zombies."

Through the backdoor

In the past, hackers attempted to access computers in an organization's network by breaking through the network's perimeter defenses. Over the past several years organizations have become more security-savvy, building up these perimeter defenses with stronger firewalls, gateways, intrusion detection systems, and other security protections that keep frontal attacks at bay. While many organizations might think they have created an impregnable fortress, hackers have discovered virtual backdoors that can be easily and silently breached, often leaving its victims unaware until the damage is done. The most popular of these backdoors, and often the easiest to exploit, is the mobile laptop computer.

Mobile workers

For salespeople, executives, and nearly any employee that is constantly on the move, the laptop has become critical to the way they work. For many organizations and their workers, productivity would come to a standstill without their laptops. Still, these same laptops that have become key to business success can also prove to be a business' downfall if not properly protected against the new organized threat of crimeware.

When mobile workers take their laptops and leave the office network, those laptops are no longer protected by the organization's perimeter defenses. While on the road, in hotels, airports, or Internet cafés, they hook up to different wireless networks that lack the protections offered by their office network. While a few mobile workers might use their laptop strictly for business, most will conduct some personal business while using the laptop. Online banking, checking their stocks, catching up on the latest celebrity news, getting new ring tones for their cell phone, shopping online, checking their personal email, playing online games, downloading the latest MP3s, file sharing, visiting chat rooms, and even perusing some of the Internet's more questionable sites have become common activities for many mobile workers.

Although some of these activities might seem harmless, the results can be devastating when carried out on a wireless or wired network that lacks the proper protections. The latest Trojans, bots, spyware, and worms lie in wait on these seemingly harmless sites, emails, and downloadable files. Not only do they silently infect the laptops, but when the laptops return to the offices and reconnect to the network, they have basically opened a backdoor into their once impregnable network fortresses. From their hiding places on the laptops, crimeware bots, Trojans, and worms stealthily spread themselves from within the network to other machines.

Protecting Client Systems from the Crimeware Invasion

A January 2005 study conducted by the Symantec Enterprise Security Group verified this scenario, finding that 43 percent of worm attacks originated from laptops carried into the network confines by employees. The source for 34 percent of worm attacks was reported as coming from laptops brought in by non-employees.¹

Even the most conscientious mobile workers that limit their computing activities to work-related tasks can put their laptops at risk. This is especially true when they utilize wireless networks outside their enterprise infrastructure. Many Internet cafés, hotels, and other locations that offer wireless Internet access put little effort into managing their networks. Often they implement little security or little control over wireless activities that take place on their networks. This makes it easy for malicious users on the wireless network to gain control of traffic flowing to and from other connected laptops, giving them the opportunity to intercept or modify a connected laptop's content. Tools for eavesdropping, sniffing passwords, or gathering data have become ubiquitous and can often be employed by even the most unsophisticated users, creating significant risk of exposure for both corporate and personal confidential information.

Remote workers

The Enterprise Security Report also found that the fourth most common originating source for worm attacks came from home systems connected to the network through the organization's VPN. In this scenario, employees without a laptop might occasionally use their personal desktop computers to work on a project at home after hours in order to meet a critical deadline. While this can definitely help organizations meet deadlines, if the desktop computer is not properly protected, it can open another virtual backdoor into the corporate enterprise.

Since home computers are primarily used for personal use, they are more likely to be exposed to Web sites, files, and emails harboring crimeware. Also, since home computers are typically shared computers, spouses or children that use the computer and are not as educated to computer security risks might employ even less caution in the sites they visit, the emails they open, and the files they download. Inevitably crimeware makes its way onto the desktop, and when the unaware home worker connects to the company network over the VPN, it opens a tunnel for the malicious code to pass through and spread to other machines from within the network.

¹ Enterprise Security Group, January 2005 ESG Research Report, Network Security And Intrusion Prevention

Protecting Client Systems from the Crimeware Invasion

Examples of such worms in the past have been the W32.Spybot.Worm and the W32.Mumu.B.Worm. In the case of the W32.Spybot.worm, it spread by using network-level vulnerabilities in hosts, which would only become visible once a VPN connection was established. In the case of W32.Mumu.B.Worm, it would attempt to force common user names and passwords onto other enterprise computers, which again would only become visible once a VPN connection to the enterprise had been established. Once it had successfully compromised a host, it would then spread.

Peripheral devices

A less common backdoor for crimeware, but just as dangerous, is peripheral devices connected to a computer within the network. Employees insert infected CDs or DVDs into their work computer, which in turn can infect other computers on the network. Cell phones, handheld computers, and MP3 players have become malware carriers that have the potential to open a backdoor into the network when they connect to a desktop. Thumb drives have become a double threat. They can unknowingly contain bots, Trojans, or worms that can contaminate the machine and the network when they are plugged into a computer's USB port. They can also become a vehicle for data theft by dishonest employees or by non-employees visiting the company.

Also, hackers can program peripherals, such as a USB storage device, to exploit known vulnerabilities in peripheral drivers. When plugged into a machine, the programmed peripheral can give the hackers administrator or system-level access to the client and its connected network. Darren Barrall and David Dewey demonstrated this attack vector in 2005 at the BlackHat briefings in a presentation titled "'Plug and Root'—the USB Key to the Kingdom" (www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf).

Personal email

Personal email often serves as a carrier for introducing crimeware into an enterprise. When users check their personal email on an account other than the organization's email system, the downloaded email can sometimes bypass an enterprise's email protections and firewall, infecting the client machine with crimeware. Once on the inside, the crimeware can spread to other clients connected to the enterprise network.

For example, the Microsoft® Windows® WMF exploit was heavily used as a generic infection vector for malicious code in a variety of manners, including introducing malicious crimeware into the enterprise via external email. Users would read their own Web-based email from within the corporate network and click on what appeared to be an innocuous link in the email, only to open the door for this exploit to compromise their host.

Closing backdoors and stopping crimeware

A knee-jerk reaction to the threat of crimeware coming into the network through a virtual backdoor might be to ban laptops, remote connections, and peripheral devices. But such rash actions are not feasible in most organizations. Of course, it would be wise to closely govern the usage of laptops, remote systems, and peripherals, as well as educate their users to the inherent security risks. But the most prudent course of action is for organizations to employ multilayered security solutions on all of their clients—laptops, desktops, and remote machines. These solutions can close backdoor breaches and effectively protect against the new wave of crimeware threats.

The primary elements of such a client security solution must be integrated to work together and include:

- Virus protection and remediation
- Spyware protection and remediation
- Vulnerability-based intrusion prevention
- File-based intrusion prevention
- Inbound, outbound traffic control

Virus protection and remediation

Antivirus technology plays a key role in any client security solution. Solutions must be able to recognize, remove, and repair the effects of crimeware on the client system. To reduce the number of calls to the help desk and eliminate the need for IT professionals to be full-time spyware cleaners, the solution must be continually updated with new definitions and repair information and helps. To avoid missing potential crimeware threats, the solution also needs to search within files and archives, and not just check for known files and registry keys.

The solution must be able to automatically protect against and block known crimeware vulnerability exploits. Its antivirus engine must also include protection against unknown threats, with the ability to recognize and stop attacks that attempt to disable the antivirus software.

The antivirus solution must be able to detect and remove polymorphic viruses. Polymorphic viruses seek to evade detection by changing their characteristics (i.e., byte patterns or encryption techniques) every time they infect a new computer. Polymorphism has become quite common in many worm attacks.

In addition to being able to automatically scan and remove any detected viruses, the solution needs to be able, in real time, to prevent and block viruses from ever being downloaded or installed onto a client.

Spyware protection and remediation

Strong client security requires strong antispymware and adware protection. This includes the ability to detect and remediate sophisticated kernel and application-level stealth techniques, such as rootkit, that hackers use to hide the existence of crimeware and crimeware actions against a client.

In addition to being able to automatically scan and remove any detected spyware or adware, the solution must be able, in real time, to prevent and block them from ever being downloaded or installed onto a client.

Vulnerability-based intrusion prevention

While antivirus technology has become the foundation for building strong client security, it is still not enough. Today more than 90 percent of organizations employ some level of antivirus protection. But even with that degree of protection, systems are still being compromised with increasing intensity. The main reason for the still-growing number of successful assaults is that antivirus solutions are reactive. They can only protect against known crimeware threats for which a remediation solution has been created. Today, professional crimeware developers focus their attacks on system and application vulnerabilities for which no specific remediation solution yet exists.

Studies indicate that the average time for a vulnerability exploit to surface is six to seven days from the time that the vulnerability is announced. A few hours after the first attack, virus definitions and signatures become available to organizations to protect themselves against these attacks. This means that organizations are typically vulnerable to new exploits for about seven days, giving full-time crimeware developers plenty of time to develop worms, bots, Trojans, or other crimeware to exploit newly announced vulnerabilities.

The only way to combat against these vulnerability exploits is to employ vulnerability-based protection as part of an organization's client security solution. Instead of having to wait for a fix to a specific vulnerability, vulnerability-based protection utilizes vulnerability definitions to proactively watch and protect against behavior that attempts to exploit vulnerabilities. Unlike system and application patches, a vulnerability definition can usually be created in a day or two by the security solution vendor, typically well ahead of any exploit against that vulnerability.

The power of vulnerability-based intrusion prevention comes from the fact that a single vulnerability definition is not only protecting against one type of threat, but perhaps hundreds or thousands. Since it looks for exploit characteristics and behavior, it can protect against a wide range of threats, even threats that are not yet known or developed.

Rootkit

Rootkit refers to a set of applications or scripts used by hackers to gain admin-level access to a system. Rootkits conceal the existence of crimeware processes running on the system, as well as associated files and data. Rootkits are often used in conjunction with a keylogger to collect confidential information such as user IDs, account numbers, and passwords.

Protecting Client Systems from the Crimeware Invasion

The ability to protect against unknown exploits has become particularly critical in today's threat landscape due to the way crimeware developers operate. It used to be that when a new virus or worm was released, it would strike, a patch would be created, and the threat would go away. But now, when a vulnerability is announced and an exploit surfaces, if the exploit doesn't work as well as the hacker hoped, the exploit is modified to improve its attack success. If it still isn't doing the job as desired, another modification is made. Sometime modifications are made simply to help the exploit evade detection. This process of exploit modification continues until dozens or hundreds of different versions exist of that exploit, all attempting to attack the vulnerability in a different manner.

Number of Variants Attacking the Vulnerability	Exploit Example
65	W32.HLLW.GOP@mm
55	Welchia
51	W32.Zotob.A
43	Trojan.NT.A

Table 1: Exploit Variants

For example, Zotob has 51 different reported variants. A vulnerability-based intrusion prevention solution only needs a single definition for the vulnerability that Zotob exploits. Since it's a generic vulnerability definition, it also has the potential to protect against exploits that aren't necessarily variants of a known exploit, but are new, unknown exploits that behave in a similar fashion. The result is that vulnerability-based solutions are able to proactively protect clients against vulnerability exploits until a patch for that vulnerability can be developed and deployed.

File-based intrusion prevention

In addition to vulnerability-based intrusion prevention, an effective client security solution must be able to block common exploit flaws that use malicious files. An example of this is JPEG images that have been created to actually open a hole for spyware to be installed. File-based intrusion prevention would be able to detect and stop these types of known exploits.

Protecting Client Systems from the Crimeware Invasion

File-based intrusion prevention solutions scan computers, the network, and the Internet looking for known threats for which an organization has matching threat signatures. By identifying a threat ahead of time, file-based intrusion stops the threat before it can even be placed on a client.

To enhance their ability to stop file-based threats from spreading, file-based intrusion solutions also need to be able to interact with inbound/outbound traffic control firewalls on a client. For example, if a CD or USB device infected with a file-based threat is inserted into a client, file-based intrusion can detect it and prevent the infection of the client; but it needs to be able to interact with the client's firewall to keep it from leaking out to the network. In other words, the solution can tell the firewall to block a specific port that the threat is trying to use to spread itself onto the network.

Inbound and outbound traffic control

Another critical element of a client security solution is the ability to proactively control inbound and outbound traffic on the client system's firewall. It needs to be able to block inbound attacks on exposed ports. It also needs to be able to block data leakage in outbound communications from spyware or bots that attempt to contact their controllers. In other words, if users have undetected bots on their systems that have been collecting passwords and bank account numbers by logging keystrokes, when the bot tries to send the confidential information to its master, the firewall will block the communication so the information never leaves the client.

The firewall also needs to be able to protect the client against other network users in what are known as peer-to-peer attacks. This can be a case of someone else on a corporate or wireless network being infected and not having adequate protection on their own client. That infected client silently, and unbeknownst to its user, tries to attack peer clients on the network. Traffic control firewalls must be able to stop these types of attacks.

For the inbound and outbound traffic control to be effective, it needs to be able to distinguish between good and bad traffic. This can be determined through rules and policies inherent to the firewall or configured by the system administrator, but that's not enough. The firewall must be able to interact with vulnerability-based intrusion prevention to block traffic associated with vulnerability exploits. So, if the intrusion prevention solution detects exploit-related activity on a certain communication port, it needs to be able to tell the firewall to block that port for a specific amount of time or until the threat has passed.

Integrated client protection

As just described, integration is a critical aspect of any client security solution. The antivirus and spyware protection, the vulnerability-based protection, file-based intrusion prevention, and firewall traffic control aspects of the solution all need to be able to communicate with each other and work together to protect the client system. Lack of integration between solutions often requires manual intervention, weakening the solutions' ability to adequately combat threats. Only through a coordinated, multilayered defense can an organization effectively protect itself against the rising barrage of crimeware.

In addition to providing a coordinated defense, an integrated client security solution can be more easily managed than individual point products. Integration allows for centralized management from a single console rather than multiple consoles. IT administrators only have to learn and use one console instead of four. Additionally, instead of having piecemeal reports that leave gaps in the client security picture, they can run a single report to get either a comprehensive or snapshot view of the entire state of their client security, letting them easily see their weaknesses and strengths. This overall ease of management that an integrated client security solution provides greatly simplifies administration efforts and frees up IT personnel to pursue activities that drive business success and improve the organization's bottom line.

Buying antivirus, spyware, firewalls, and intrusion prevention from four different vendors results in four different licensing terms, four different service contracts, four different support centers to deal with, and four different update subscription terms. An integrated solution not only makes life easier for IT, but it can provide significant savings to an organization in terms of licensing costs.

Conclusion

In order to protect themselves against the organized and targeted wave of crimeware attacks, organizations need client security solutions designed to protect against this new threat landscape. Perimeter defenses aren't enough; neither is basic antivirus technology. Organizations need multilayered client security that integrates antivirus, spyware, vulnerability-based intrusion prevention, file-based intrusion prevention, and outbound/inbound traffic control.

As their number one priority, organizations must first implement this multilayered integrated solution on all of their laptop computers—the favored target of crimeware developers. They need to then follow up by adding this protection to all of their network clients, including clients inside the network infrastructure and at any remote sites that connect to the enterprise network, and clients that connect from users' homes.

Symantec, the world leader in providing solutions that help assure the security, availability, and integrity of information, offers Symantec™ Client Security to help keep enterprise client systems safe by providing comprehensive and proactive protection against the aggressive threat of crimeware. The solution automatically detects and repairs the effects of spyware, adware, viruses, and other malicious intrusions in real time. Its vulnerability-based detection works in concert with its antivirus and traffic control tools to detect and block known, unknown, and emerging vulnerability exploits to help keep systems safe and protect an organization's valuable and confidential information.

For organizations that want to add an additional layer of protection, Symantec Sygate™ Enterprise Protection can shield their enterprise from misbehaving clients and untrustworthy networks. It secures networks against non-compliant endpoints, enforcing compliance on contact through its seamless integration with Symantec Network Access Control.

Backed by Symantec Security Response, the world's leading Internet security research and support organization, the multilayered integrated approach provided by these Symantec solutions gives organizations the coordinated defense they need to protect themselves against organized crime's rising wave of spyware, worms, bots, Trojans, and complex attacks against their laptops, remote machines, and other clients.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Sygate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners.
06/06 10729032