TAKE BACK

the Endpoint

CDW

KASPERSKY lab

TABLE OF CONTENT

Waging War at the Endpoint

During the course of three days in late 2009, cybercriminals acquired the banking credentials, username and password, for Hillary Machinery, Inc., located in Plano, Texas, and conducted more than 45 separate transactions to over 40 different payees. The result was a loss of $801,495. While Hillary Machinery was able to recover some of their lost money, $250,000, plus attorney fees and court costs, was outstanding, along with an ongoing lawsuit between the company and its bank. According to Troy Owen, owner of the company, "While the loss didn't cause us to go out of business, it certainly put off the business growth plans that we had."

Open a newspaper any given day and you'll read stories of companies being attacked by cybercriminals. Data breaches are rampant. Banker Trojans are stealing online-banking credentials, resulting in massive financial losses. In 2010, CSO Magazine conducted the Cyber Security Watch Survey. Senior Editor Bill Brenner states "Even those companies making sizable efforts to keep their data secure admit it's almost impossible to outpace the bad guys."

It's a war out there, a war against cybercriminals who have one goal in mind – making money. Today's cybercriminals are perpetually after data that can be easily converted into profit or credentials that will allow them to transfer money directly from the company coffers.

According to SANS.ORG in their report The Top Cyber Security Risks, "The number of attacks is now so large and the criminals sophistication is so great that many organizations are having trouble determining which new threats and vulnerabilities pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt with first." As IT Departments spend on security today, many are overlooking the primary attack target – the endpoint.

The Endpoint – a user's desktop, laptop, or mobile device – is the richest target for cybercriminals today. Endpoint systems have become more mobile, making the traditional "IT perimeter" ineffective in providing the right level of protection for corporate users and these assets. According to IDC, "Endpoint... solutions are now a primary line of defense."

In this article we'll discuss the growing malware threat, how cybercriminals are targeting the endpoint, and how you can protect your endpoints from these malicious activities.

The Growing Malware Threat

Through Kaspersky Lab's 25 years of experience protecting companies from Internet threats, we have seen an exponential increase in malware threats on the Internet today. The numbers are sobering. Over 30,000 new threats are discovered every day—over 3.4 million in all of 2009. More than 3,500 new anti-malware signatures are released every day to ensure protection from the latest attacks. On one particularly busy day, Kaspersky created 13,500 signatures to combat the high volume of threats released on that day. In addition to traditional protection of workstations and servers, more than 1,200 mobile malware signatures have been created to protect the smart mobile devices from these threats.

And the trend continues in 2010:

- During Q1 2010, over 327 million attempts were made to infect users' computers around the world, an increase of 26.8% over the previous quarter.
- Also during Q1 2010, more than 119 million malware hosting servers were detected, of which 27.57% were located in the U.S. and 22.59% in Russia, with just 12.84% in China.
- The total number of exploits targeting vulnerabilities in browsers and plug-ins, as well as PDF viewers, increased by 21.3%, nearly half of them targeting vulnerabilities in Adobe programs.

A recent whitepaper released by RSA on cybercrime reveals **that 88% of Fortune 500 companies have compromised PCs running Trojans in their environments**. According to RSA's Uri Rivner, "these Trojans are busy moving terabytes of corporate data to stealthy drop zones scattered around the 'Dark Cloud' of the Cybercrime infrastructure."

This is consistent with data reported by CNET News in October, 2009, stating that 63% of midsized organizations saw an increase in cyber threats in 2009. According to the article, **71% of US mid-sized companies think that a serious breach could put them out of business**. This startling revelation emphasizes the focus for cybercrime today—to make money. In fact, according to the FBI's Internet Crime Complaint Center, while reports of cybercrime increased 22.3% in 2009, the reported losses as a result of that cybercrime more than doubled from $265 million to over $560 million that same year. And those numbers represent only the attacks that were reported. Since the vast majority of attacks go unreported, the number of attacks and the financial losses are, in reality, significantly higher.

In addition to more malicious attack methods that result in more money stolen per intrusion, cybercriminals no longer target only large companies. Small businesses, state and local government and educational institutions are specifically being targeted by cybercriminals because they are often behind in security spending and protection. Mid-sized companies in the US lost over $100 million in 2009 to fraudulent bank transfers. Even the Pentagon, an organization with heavy investments in security, was the victim of cybercriminals in 2009, resulting in the loss of terabytes of sensitive data, including data on the new F35 Lighting II Joint Strike Fighter. While the most sensitive Department of Defense data is stored on computers not connected to the Internet, hackers gained access to this ultra-sensitive data via endpoint computers belonging to third-party contractors hired to design and build the fighter jets.

Why is the Endpoint a Target?

The increasing malware threat is focused on one target today—The Endpoint. But why? Why have cybercriminals become so interested in the endpoint? Several factors make the endpoint interesting to cybercriminals:

- **Decentralized Data.** Data no longer resides on the mainframe. Sensitive and confidential corporate data is constantly being created, used and stored on the desktop, the laptop and the smart mobile device. Access to these devices means access to data with a potentially high monetary value.
- **Keys to the Kingdom.** Placing the right Trojan on an endpoint system gives a cybercriminal access to data as well as credentials to other corporate systems - including online banking and financial systems. Millions of dollars are lost every day due to fraudulent transfers from corporate bank accounts through the use of login information captured by banker Trojans.
- **Complete Control.** Deep access at the root level on the endpoint also gives cybercriminals access to any system or data the end-user can access. The cybercriminal also has the ability to make the endpoint a "zombie" machine as part of a larger botnet, using the system to spread malware to other systems. And ultimately, this kind of endpoint access can give hackers the ability to watch email content, IM chats, web traffic, individual keystrokes and more, making the endpoint a wealth of opportunity.

Today's computer hackers are not yesterday's script-kiddies looking for fame and glory. Today's cybercriminals seek access to the endpoint while remaining hidden so that they can steal data and money without the user's knowledge.

A number of factors make the endpoint an easy target:

- **Easy Access.** As the network perimeter has become more porous, allowing end users access to all that the Internet has to offer, the endpoint has become the new perimeter and, in turn, the new target for cybercrime.
- **Mobile Data.** Corporate road warriors travel the globe on a daily basis, connecting to unsecured networks in airports, hotels, at home and on airplanes. These systems are outside the confines of the corporate perimeter, creating a constant threat to corporate data and making the perimeter even more porous and accessible to cybercrime.
- **Multiple Attack Vectors.** End-users today use the corporate Internet for both business and personal purposes, providing the cybercriminal multiple attack vectors into the endpoint. Valid business websites become distributors of malware, and social media sites are a playground for cybercriminals. Cybercriminals prey upon individuals and companies alike as they engage in online social networking to keep track of friends, family, customers, prospects and partners. Personal web surfing, dating sites, music sites, video sites, etc., are also vectors for cybercriminals to spread malware to the endpoint. And let's not forget the ever-present threat posed by email.

The ultimate goal is to get malware onto the endpoint. Again, according to RSA:

" Once infected, malware, typically Trojans, will start recording all Internet-related traffic, perform keylogging, grab emails, browser-stored passwords, and a long list of additional items. The Trojan doesn't stop at online banking credentials and credit card data: it steals your social network posts, your medical content, your private chats, your constituent letters, and all of your work-related content: credentials for internal systems, emails you sent or received, corporate financial results, sensitive customer-related web forms you completed in CRM systems."

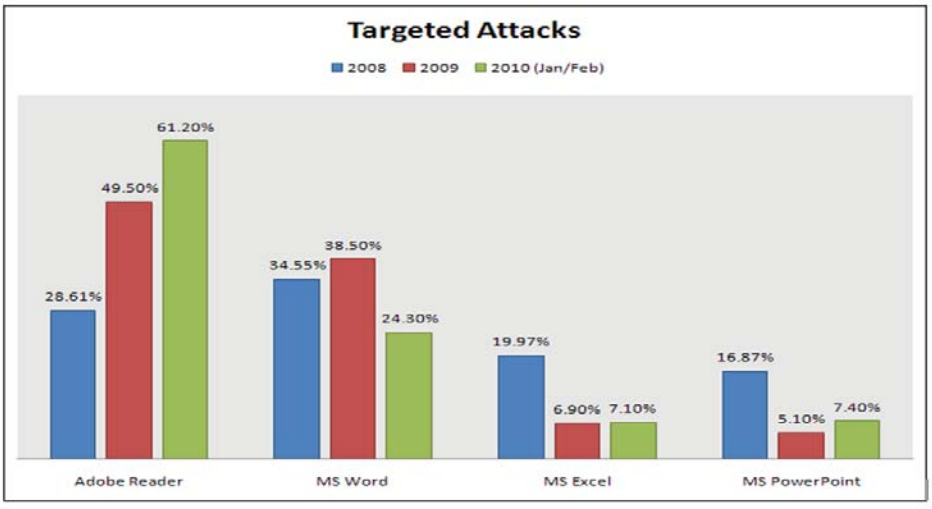
Once a Trojan is installed on an endpoint, it can become prolific and insidious – and incredibly profitable in so many ways.

It is no wonder, and not by mistake, that cybercriminals target the endpoint. Without the right protection, organizations' endpoints offer a target-rich environment of entry points.

How Are Cyber-Criminals Targeting The Endpoint?

Think you are secure? Think again. Perimeter security is proving ineffective in protecting the newest target of cybercrime. According to RSA's Uri Rivner, ". . . the battlefield is changing. Employees, rather than networks, are now on the frontline." Let's look at how cybercriminals are targeting the endpoint today.

In years past the operating system—primarily Microsoft Windows—was the hacker's paradise. As the OS has become progressively more secure, third-party client-side applications on the endpoints have become a preferred attack vector for cybercriminals. The user downloads applications such as WinZip, Realplayer, Quicktime, Adobe PDF and browser plug-ins (ActiveX controls, video codecs, etc.), with little concern for maintaining these apps. These undocumented and unmanaged programs, full of vulnerabilities, are seldom patched or updated. IT departments rarely know what versions of these applications are running in their environments let alone what patch levels these applications have installed.



According to Secunia PSI statics, **only 2% of Windows computers are fully patched**.

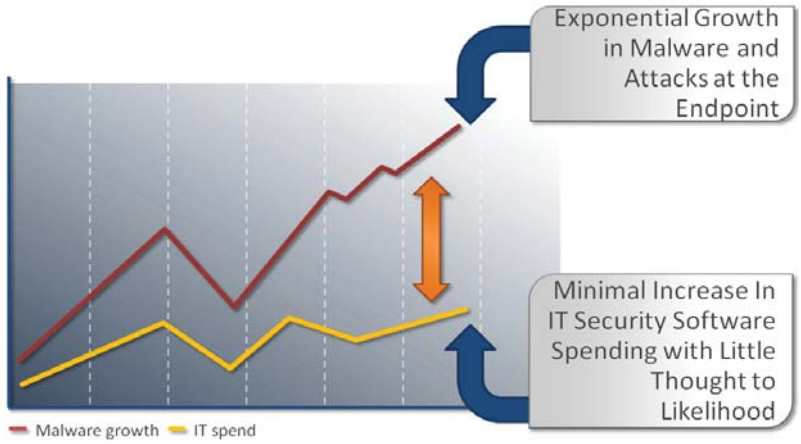
It is through these vulnerabilities that cybercriminals gain access to the company endpoints and use malware to carry out their nefarious schemes.

Cybercriminals are targeting the endpoint with malware through numerous vectors:

- **The Need to Communicate.** Eight out of 10 emails today contain malicious or unwanted content. According to Gartner, the email threat increased six fold in 2009. These threats include infected attachments, phishing links and re-directs to third-party servers that download malware.
- **Good Web Sites Gone Bad.** Over 1.73 billion users, 25% of the world's population, visit more than 234 million web sites today. In 2009 alone, 47 million new web sites entered the Internet. Cybercriminals are using the exponential rise in Internet web surfing to spread malware to unsuspecting users. Two techniques, SQL Injections and Cross-Site Scripting, account for 80% of all exploited web vulnerabilities. Cybercriminals take advantage of web vulnerabilities and use these attack methods to hack into valid business web sites, planting obfuscated JavaScript that downloads malware as users hit the site. Known as a "drive-by download", users are infected with malware by simply visiting legitimate sites that have been compromised by a third-party server. Malware is no longer being spread solely through gambling and pornography web sites; **77% of web sites that contain malicious content are completely legitimate web sites that have been compromised by cybercriminals.**
- **Staying Connected.** Social media is on the rise for individuals and corporations alike. The need to stay connected to partners, customers, prospects, family and friends has led companies to open their perimeter security to a very insecure form of mass communication. Facebook, LinkedIn, Twitter and MySpace are the main social media sites that companies allow their employees to access every day, both for personal and business purposes. Cybercriminals are targeting the rapidly-expanding use of social media to make money and to proliferate malware to the desktop and into corporate networks. Social media exploits two common human traits: trust and curiosity. The trust factor is called into play since you only invite those you know and trust, therefore content they send is "okay." Curiosity drives our desire to click. The average user will click on practically anything. The problem with that is that we rarely know where that click will take us or what damage can be done by opening that file, that web page, that app. These two factors combine to make social media inordinately dangerous.
- **Fear, Uncertainty and Doubt.** Scareware and ransomware are an increasingly common mode of scamming money from unsuspecting and untrained users. While visiting a web site, a popup message tells the user that they have malware and are at risk. The message offers them protection by downloading fake security software that costs anywhere from $30 to $60. The enticement is protection. The reality is that you have lost money and that the software you downloaded was actually malware, not a program to protect you from malware. Scareware scammers earn weekly salaries that are more than triple the weekly salary of your company's CEO.

Protecting the Endpoint from Cybercrime

Although the malware threat has grown exponentially, the budget allocated to IT security has not increased proportionately. More importantly, the spending on endpoint protection has not grown in proportion to the real threat.



Traditionally, IT departments have focused their security spend at the perimeter – firewalls, IDS, IPS, spam engines and URL filtering. While these are absolutely necessary, and a key piece to a layered protection strategy, they do little to protect the endpoint from the onslaught of malware from multiple attack vectors. URL filters, while keeping employees from going to what are considered "bad sites," do nothing to protect users from malware being distributed by drive-by-downloads on valid business web sites. Firewalls have been configured to allow users unrestricted access to the Internet. Ironically, in the process they have allowed cybercriminals direct access to the desktop.

Protection at the endpoint has long been considered a commodity, with price being the ultimate deciding factor. Some companies even use free anti-malware software. Unfortunately, the malware that comes with it is also free. With IT departments focused on protection at the perimeter, IT managers give little thought to AV protection. Some IT managers see little difference among the various AV products. Others believe that all anti-virus software stinks, and they pick the one that stinks the least.

While these views are understandable, given the disastrous experiences that some customers have had, they are far from accurate. In fact, there is a huge difference in how AV software detects and removes malware from the endpoint, as illustrated by numerous independent testing laboratories. The time has come to change this mindset and focus on both detection and response at the endpoint.

Numerous factors must be considered when evaluating at endpoint protection solutions:

- **Overall Detection Rates:** How effective is the vendor at detecting both known and unknown malware, the former relying on signature-based analysis, and the detection of the latter driven by heuristic or rules-based analysis. The vendor should be able to detect the widest variety of malware types: Trojans, viruses, rootkits, and more. High scores in one type of detection while scoring low in another type of detection results in ineffective protection.
- **Holistic Protection:** Malware can be introduced to an endpoint in numerous ways and any anti-malware vendor worth its salt should be able to effectively block all threat vectors to the endpoint. The vendor should also be able to protect the system regardless of its physical location and easily adapt to changing locations so that more security can be provided when operating outside the corporate network perimeter. Personal firewalls, IDs, anti-spam, anti-virus, anti-phishing, web malware protection and more should all be considered vital to the overall protection strategy for the endpoint.
- **Performance:** Protection is of little use if it impedes the end user's ability to perform daily tasks. "Bloatware," as AV software is often called, uses system resources to the point that the employee no longer can use the system until the software is finished scanning. It is especially important to deploy protection that has virtually no impact on employee productivity. Is it possible to have both protection and performance together? Absolutely!
- **Manageability:** The management console for anti-malware software is an extremely important piece of the puzzle—and the buying decision. A cumbersome, non-intuitive, resource-intensive management console will make it difficult to manage your security posture, and your overall security solution will suffer. Management should be simple, easy to use, yet granular and powerful enough to mitigate risk anywhere in your endpoint environment. And it should be especially helpful in quickly deploying and maintaining the many instances of endpoint security.
- **Support:** No one has time to sit on hold for 45 minutes or more waiting to get help when there is a problem—and you shouldn't have to. Before buying AV protection, test the support center to make sure they are responsive and effective. How quickly do they answer the phone? How effective is the engineer are resolving your issues? Support shouldn't be a hassle; it should be an asset.
- **Price:** This category is last for a reason. All AV vendors today are highly competitive in price. They are not, however, highly competitive in functionality. Price is important, but only if you have found the security software that will provide the right protection, performance and manageability.

Endpoint protection should not be a commodity purchase. Due diligence will ensure you are providing the highest level of detection and response at your endpoints.

Case In Point - Are You Really Secure?

Stephan, an Administrator at Jackson Public School in Mississippi, though he had the right protection in place to keep malware out of his network. With over 9,200 seats under management, Stephan had made a solid investment to make sure they were all secure. When performance issues drove them to switch to Kaspersky, they found out how unsecured they really were.

Upon installation of Kaspersky, the IT team found out that there were extensive infestations in their network:

- 14,459 virus installations were found across their endpoint systems
- 43 different Trojans
- 56 different viruses
- 15,701 infected objects network-wide

Malware was running rampant! The current anti-malware vendor was not detecting and removing malware. The only way they found out was by installing a premium malware package—Kaspersky Lab.

This level of infection was completely inexcusable considering the investment the organization had made to protect itself from this risk. The pain and cost of removing all of the malware in their environment continued for several weeks until all infestations were cleaned.

You may think you are secure, but do you know for sure? Who is accessing your data without your knowledge? Who has access to your endpoints through the perimeter security you've put in place? Is your current anti-malware vendor really blocking malware and protecting your endpoint? These are real questions that in today's hostile digital environment require real answers.

It's time to wage war against cybercrime – and the front line is the Endpoint!

In Part 2 of this article we will examine ten ways that today's IT department is permitting cybercriminals to steal data and credentials by gaining access to the endpoint. A fundamental shift in mindset is required within IT to make sure that cybercrime is thwarted and the endpoint—as well as the user—is protected.

To download Part 2 of Combating Cybercrime go to www.kaspersky.com.

It's time to wage war against cybercrime –
and the front line is the Endpoint!

500 Unicorn Park
Woburn, MA 01801
866.563.3099
smbsales@kaspersky.com

www.kaspersky.com
www.threatpost.com

KASPERSKY lab