



Identifying and Thwarting Malicious Intrusions

Table of Contents

Introduction	4
Malware Types and Threats	5
Advanced persistent threats	5
Blended, multi-vector threats	5
Polymorphism	5
Rootkits	5
Spyware/adware	6
Trojans	6
Viruses	6
Worms	7
The Future of Malware	7
Malware Distribution and Control	8
Bot Propagation and Sustainability	8
Command-and-control	8
Drive-by attacks	8
HTTP	8
Internet relay chat (IRC)	8
Peer-to-peer	9
Pull propagation	9
Push propagation	9
Zero-day exploit	9
Zero-day window of opportunity	9
The Dark Side of Social Networks and Web 2.0	9
Social networking	9
Web 2.0	10
Phishing	10

Types of Botnets	10
Conficker	10
Gozi	10
Mariposa	11
Queen Botnets	11
Detecting and Combating Malware	11
Protecting Assets	12
The McAfee Security SaaS Advantage	12
McAfee SaaS Email Protection	12
McAfee SaaS Web Protection	13
McAfee Global Threat Intelligence	13
Enterprise-class protection	14
Conclusion	14
About McAfee, Inc.	14

Introduction

As social networking websites such as Twitter and Facebook have grown, cybercriminals have quickly adopted these sites as attack channels in their searches for sensitive, profit-generating data. Facebook boasts more than 400 million members,¹ with the largest recent growth occurring in the 35 to 55 age group.² Twitter doubled in size every three months in the beginning and now has a community of more than 58 million users.³

Attacks start with enticing news snippets and compromised URLs or corrupted TwitPic photos, often riding the appeal of celebrity news.⁴ Although Twitter growth flattened out in late 2009, innovations like geo-location and retweets maintain its appeal to users and cyber-thieves and provide an example of the kaleidoscopic change possible with Web 2.0, compared to the static email and web of a few years ago.

Every day, cybercriminals launch sophisticated new attacks using stolen social network credentials or bogus accounts. They seek to lure unsuspecting users into revealing passwords, which they use to compromise other accounts for launching more attacks or to steal credit card numbers or bank accounts for identity theft and financial fraud.

Hundreds of thousands of new malware attacks appear yearly. The impact of a successful attack ranges from embarrassment and brand damage due to the posting of sensitive data on public Internet sites to costly notifications of affected parties, regulatory fines, lost consumer confidence, and potential legal liability. The worst case is a business dead in the water, unable to access information needed to manage operations.

Many businesses, focused on sustaining profitable operations, lack the deep skills needed to protect critical information and infrastructure from sophisticated attacks. Often a business cannot recognize when it is under attack, or it does not have the skills to identify and locate malware infections. Fewer still have the know-how to completely remedy infections and prevent their embarrassing spread to business partners or customers.

There is a way for businesses to mitigate the risk of cybercriminals. Vigilant defenses can detect attacks as they are launched and eliminate threats before any damage occurs. Layers of security help shield identities, remove infections before they spread their malignancy, or repair the damage from an attack that is underway.

A proper defense against malicious information attacks starts by educating businesses and users on the nature of malware threats. This white paper will help decision-makers effectively plan malware defenses by providing critical information on how cybercriminals operate:

- Cybercriminals have migrated from email to social media as the primary attack channel
- Constantly changing, often encrypted malware escapes detection and is controlled in botnets of “zombie” computers managed by far-flung command and control centers
- Cybercriminals blend multiple attack methods into more virulent, multi-stage attacks to increase their payoff and skirt detection

¹ As of March 29, 2010, <http://www.facebook.com/press/info.php?statistics>

² <http://www.krishnade.com/blog/2009/facebook-coo-sheryl-sandberg/>

³ <http://www.techchuck.com/2009/10/26/twitter-finds-growth-abroad-with-58-4-million-global-visitors-in-september/>

⁴ <http://hollywoodcrush.mtv.com/2009/06/29/britney-spears-ellen-degeneres-and-diddys-twitpic-accounts-get-hacked/>

Malware Types and Threats

McAfee Labs defines malware simply as malicious programs. Viruses, worms, Trojans, spyware, and rootkits are examples of malware. Potentially unwanted programs (PUPs), such as adware, are not necessarily malware, but are usually considered risky by security professionals.⁵

Countless variations of new and existing malware are being launched constantly across the Internet. Originally, malware was distributed via email messages from bogus or stolen email accounts. Now, it is more often hidden in websites or inserted into ad networks to be injected into the browser of an unsuspecting visitor. For instance, malware today lurks in social media pages or messages, ready to infect users lured by offers from compromised or bogus Facebook or Twitter accounts. Mobile devices, USB sticks, and other portable systems also carry malware into the network, where it propagates.

Conficker was a 2009 worm that used several of these paths simultaneously. It spread across the network through a Microsoft vulnerability, email, unique websites, and a peer-to-peer protocol. It also infected endpoint systems directly through USB drives.

Different types of malware behave in different ways, classified by their format, content, behavior, infection characteristics, and propagation techniques. Some newer, narrowly targeted malware types are heavily camouflaged, employing behavior disguised or hidden to avoid detection.

Advanced persistent threats

Advanced persistent threats (APT) are an increasingly common form of complex and directed attacks that use insidious techniques for gaining access to privileged systems and maintaining that access until all of the attackers' objectives have been met. A recent example, Operation Aurora, proved extremely successful in targeting, exploiting, accessing, and exfiltrating highly valuable intellectual property from its victims (see sidebar), succeeding at Google and at least 20 other companies.

Blended, multi-vector threats

New hybrid threats combine several forms of malware into one very malicious payload. A single blended virus infection may include keyloggers to steal sensitive financial information, email, and corporate secrets while turning users' systems into a spam zombie in a botnet. Blended threats that enable botnets are a significant threat escalation because they offer cybercriminals a variety of opportunities for making money.

For instance, a botnet sending spam can generate recurring revenue as part of a spam network, while simultaneously propagating viruses and stealing online banking, gaming, and social networking logins, as well as the account information required for perpetrating fraud. (See section that follows for more on botnets.)

Polymorphism

Cybercriminals design malware to update after each use, or at least to be updated frequently. By changing its online fingerprint, it will escape detection by commercial anti-virus defenses that use signatures to identify and block malware.

Rootkits

Invisible malware that hides within authorized software in a computer's operating system is called a rootkit. Malicious services in rootkits allow undetected operation while stealing information, monitoring user actions, modifying programs, or changing security settings to enable remote control. Some rootkits have very sophisticated capabilities, such as encrypted communications sent to a master controller that installs malware updates.

Master Boot Record (MBR) rootkits escape detection by hiding in a protected disk sector used to launch the operating system, allowing the MBR rootkit to relaunch and take control of the infected system with every boot sequence. These rootkits are especially insidious since they can survive a reimaging of the

Operation Aurora: How It Worked

Operation Aurora included numerous steps that all occurred invisibly, in an instant, without any apparent signs of malicious intent or actions. Operation Aurora completed its attack in six simple steps:

1. A targeted user received a link in email or an instant message from a "trusted" source.
2. The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
3. The user's browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.
4. The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
5. The payload set up a backdoor and connected to command and control servers in Taiwan.
6. As a result, attackers had complete access to internal systems. They targeted sources of intellectual property, including software configuration management (SCM) systems accessible by the compromised system. The compromised system could also be leveraged to further penetrate the network.

—Protecting Your Critical Assets: Lessons Learned from "Operation Aurora," By McAfee Labs and McAfee Foundstone Professional Services, available at http://www.mcafee.com/us/threat_center/operation_aurora.html

machine. The rootkit uses virtualization and replication to reinsert itself in the protected area of the host after the operating system is reinstalled.

Spyware/adware

Introduced in 2003 with a commercial purpose, adware, also called spyware, was designed to display pop-up ads and track user behavior. Cybercriminals leverage adware technology to capture information from users' systems without their knowledge and use it for malicious purposes.

Trojans

Trojans appear harmless but conceal the most frequently used malware and use many distribution methods. Often, social engineering tricks lure users into downloading Trojans from bogus websites or opening infected email attachments or website files. Trojans are usually distributed by infected programs, hence the warning to not open any attachments or files received from untrusted sources. Trojans also can be installed in drive-by downloads from malicious websites with no user action required.

With less programming skill than a drive-by download requires, Trojans can be presented as a software upgrade necessary in order to view an image or file, often Adobe Flash or Reader. Users have been trained over the years to automatically accept these upgrade requests. An intriguing variation is known as "rogue anti-virus," which offers a free scan of the system, announces that the system is infected, and sells an anti-virus program that merely turns off the alert. The system remains compromised, naturally.

Six Classic Trojan Malware Payloads

- Remote access—Allows hacker logins to infected systems through a backdoor
- Data destruction—Early Trojan virus attacks that destroyed data on infected systems
- Downloader—Turns infected systems into a downloading and storage zombie, frequently for information stolen elsewhere
- Server Trojan—Installs a server for file transfer, email, or other purposes to perpetuate fraud or spread zombie infections
- Security software disabler—Disables defenses and security updates on infected systems
- Denial-of-service (DoS) attack—Thousands of infected zombies in a botnet act in a concerted attack, sending packets to disable target systems

Some Trojans are malware cocktails combining several types.

Computers hijacked by Trojans with communications capabilities become remote access Trojans (RATs) and resemble rootkits in their ability to send credit card numbers and/or passwords to a remote botnet controller.

Viruses

Viruses are the original form of malware and contain software that infects other programs rather than targeting a software vulnerability or security hole. Viruses require a user action to propagate, such as opening a link or executing a program. Viruses originally spread from infected data on magnetic disks or tapes to computers. Networks have accelerated a virus's ability to spread and have magnified their impact. They frequently are directed by remote botnet controllers to spread spam, harvest sensitive user information, or propagate more malware.

Recent Malware Milestones

- Operation Aurora—On January 14, 2010, McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point to exploit Google and at least 20 other companies. This advanced persistent threat (APT) was initiated surreptitiously when targeted users accessed a malicious web page and ultimately connected those computer systems to a remote server. That connection was used to steal intellectual property and gain access to user accounts.
- Mariposa—This botnet discovered in December 2009, with arrests in March 2010, included 12.7 million compromised PCs representing half of the Fortune 1000 and more than 40 banks. It spread using a Microsoft Internet explorer vulnerability, Microsoft Instant Messenger, and USB sticks.
- Conficker—Discovered in November 2008 and still doing damage as of January 2010, Conficker quickly grew into the largest Internet worm ever. Advanced software and encryption make it difficult to detect and defend. At least five varieties have infected more than 20 million Windows systems, forming a large potential “command-and-control” botnet.
- Short URLs—Tweets, Facebook messages, or traditional spam include short URLs from abbreviated URL services (such as tinyurl.com) in order to link to and shield malicious websites hiding cross-site scripting or injection attacks
- Search engine optimization—These attacks use the most popular topics from search engines, often tied to celebrities and current events, to lure web users to malicious websites hiding cross-site scripting or injection attacks
- Hactivism—This form of attack burst onto the Internet in 2007 with denial of service attacks launched against government websites in Estonia, Lithuania, Georgia, and South Korea. These political attacks likely had state sponsors.
- Click fraud—A fast-growing cybercriminal activity, click fraud has doubled in the past two years. Botnets hijack legitimate search queries or masquerade as valid search advertising, and then use automated clicking to steal from advertisers and search engines.

Worms

Worms, first detected in 1988 with the growth of computer networks and the infamous Morris Worm, target computers rather than executable software programs. Worms self-propagate and typically lack the sophisticated logic found in viruses. They can do major damage by clogging communications bandwidth (denial of service) and overloading computers or networks.

The Future of Malware

The growth of malware is accelerating, with much of the volume due to polymorphism. In 2009, McAfee Labs™ saw more than twice as much unique malware than was recorded for all of 2008, more than 3 million pieces. The pace is increasing because:

- Web 2.0 applications and services have matured. The large-footprint Web 2.0 client systems have fewer defenses than servers and are an easier malware target for exposing new communication protocols, file types, and software applications.
- Rapid growth in social networks increases the “attack surface,” the available targets including users, devices, and applications
- More robust software functionality is available on client systems and browsers, and patching processes are less regimented than those in place for servers.

Recent successes such as the Waledac and Mariposa botnet takedowns and arrests testify to the improvement in global cybercrime enforcement.⁶ However, law enforcement and criminal justice systems are still responding to events, not preventing them. Where the perpetrators are in jurisdictions on other continents, local authorities still have little incentive or means to investigate and prosecute these “virtual” crimes.

The tremendous profit potential of cybercrime attracts highly skilled developers. This criminal service industry, devoted to stealing information and profiting from it, produces malware exploits that rival commercial software in sophistication and quality and are increasingly difficult to detect.

Malware Distribution and Control

Malware is increasingly distributed via bots or botnets. A bot is a computer program that performs automated tasks, and botnet (an amalgam of the word “robot” and “network”) is a private network or army of compromised computers used to carry out automated tasks such as spamming.

Almost all computers infected with malware belong to at least one botnet, some more than one. Individual bots, or zombies, are infected without the owner’s knowledge and are controlled by one or more outside sources. Botnet remote controllers direct millions of zombies to send spam, spread more malware, or capture and report sensitive information to the bot controller.

An infected zombie may appear to be operating normally to the user as it spreads spam, viruses, and malware with rootkits, or captures and reports sensitive information.

Bot Propagation and Sustainability

Bots, or zombies, employ a variety of techniques to spread their infection, manage and update the zombie army, and escape detection.

Command-and-control

Command-and-control botnets are managed by a single central controller, often a purpose-built botnet control console such as Zunker, WebAttacker, MPack, or IcePack. Anti-malware defenders developed decapitation countermeasures to silence controllers and neutralize botnets. Cybercriminals responded with redundant controllers, allowing any zombie in the botnet to assume control. Peer-to-peer technologies are helping them increase resiliency while remaining under the radar of reputation systems that track malicious sender and destination addresses.

Drive-by attacks

Cybercriminals use a couple of different drive-by attack mechanisms. In one, a bogus website scans a site visitor’s system for specific vulnerabilities. If a vulnerability is found, Code such as JavaScript or an ActiveX executable is injected, turning the visitor’s system into a zombie. The second drive-by attack is drive-by pharming, or DNS rebinding. A visitor to an innocuous website is re-directed to a hidden bogus or spoofed website that injects malware into the visitor’s system.

HTTP

The ubiquitous hypertext transfer protocol is a foundation of the Internet—and enterprising cybercriminals have turned it into a communications channel, hiding their command-and-control messages to zombie armies inside innocent web communications protocols.

Internet relay chat (IRC)

This mature communications protocol from early network bulletin boards lets anyone hold live keyboard conversations with other computers. IRC also is used by botnet zombies to listen for IRC commands from a botnet controller.

Peer-to-peer

A botnet fault-tolerant strategy, peer-to-peer botnets ignore the loss of any controller and continue operating standalone until a new manager emerges. Peer-to-peer bots often contain encryption keys for authentication and opening secure communications. A decapitated botnet operates standalone until a zombie assumes a management role, authenticates itself, and sends botnet updates over an encrypted channel.

Pull propagation

A widely used means of botnet propagation, the “pull” technique also uses a lure such as an email or instant message from a spamming bot with a special offer guiding the victim to a download at a criminal website. Upon clicking on the link, the recipient’s system may first be scanned to determine if it is vulnerable for the planned malware injection. Often, there are multiple injections available, increasing the chance of matching a vulnerability in the browser, player, or operating system on the host. The malware is downloaded, or “pulled,” into vulnerable systems. If target systems do not have the desired vulnerability, users are enticed to download the malware and infect their own systems. As we discussed in the Trojan section earlier, these downloads are readily accepted when they appear to be a logical upgrade to a commercial product. “Pull” virus propagation is an effective use of polymorphism because it’s difficult for anti-virus vendors to analyze and publish signatures in time with constantly changing malware downloaded from websites.

Push propagation

A classic bot attack “pushes” spam with a special offer or lure containing a malicious payload. An unsuspecting recipient opening the special offer attached to the email installs the virus and becomes a botnet zombie.

Zero-day exploit

A zero-day exploit refers to the release of code whose purpose it is to exploit a just-published or unpublished vulnerability within an operating system or application program.

Zero-day window of opportunity

This agile botnet strategy targets the time window between when a virus is released by cyber criminals, to the subsequent distribution of a defense. Zero-day window can also be used to refer to the time between announcement of a vulnerability and the release and installation of its associated patch. Cybercriminals extend zero-day windows with polymorphism and encryption to delay the introduction of signature defenses and extend the lifespan of their malware.

The Dark Side of Social Networks and Web 2.0

Cybercriminals have rapidly co-opted social networks and Web 2.0 technologies, replacing email as the preferred distribution channel. Today’s propagation model for malware relies on the following:

- A target-rich and trusted distribution channel like Twitter or Facebook for launching attacks
- An abundance of bait gleaned from search engines and other sources to lure even more unsuspecting users
- A trap in the form of malicious content embedded in messages or websites waiting to infect a recipient or visitor’s system

Social networking

The explosive growth in social networking has created a new attack vector, a new field where malware and attack techniques can be put to use. The implied trust of social networking users coupled with fewer content controls and insufficient security offer cybercriminals an increased probability of success compared with mature spam and malware channels such as email and IM. The result is an all-out assault by cybercriminals on social networks and their users.

Hackers target the trust relationships of social networks with malicious tweet messages from bogus Twitter users, and fake Facebook pages spewing messages laden with malware to propagate infections. Social networking users and their assumed trusted relationships are vulnerable to hacker exploits stealing “buddy lists,” or personal networks of friends and associates. Armed with distribution lists stolen from social network members, hackers leverage the trusted relationships to repeat proven attacks with messages containing malware, or they lure trusting users to malicious social networking pages where they inject malware.

Web 2.0

Web 2.0 places more functionality on the user’s client systems for a range of robust applications, from messaging and multimedia to gaming and geo-location, such as traffic and other GPS-based information services. The combination of a less mature Web 2.0 security environment, coupled with the larger software attack footprint, has created a toxic stew. Skilled hackers have developed specialized exploits using open source Web 2.0 application programming interfaces (APIs) to compromise social networks and search engines and hide malware behind popular sites.

Phishing

Web 2.0 technologies in social networks like LinkedIn, MySpace, Facebook, and Twitter have given cybercriminals new phishing attack channels. The trusted relationships in social networking sites increase the probability of a hacker infecting a recipient’s system. Using addresses stolen from compromised social networking accounts, hackers lure unsuspecting recipients to malicious websites with offers of popular content, videos, or music, as vetted by search engines. Malware is then downloaded to the systems of unsuspecting visitors system when they click to download the file.

Types of Botnets

Conficker

The game-changing worm, Conficker, was the first digitally signed botnet to push authenticated (digitally signed) updates. Digital signing served a dual purpose. It increased the difficulty for anti-malware researchers who were attempting to penetrate Conficker to learn its inner workings and design countermeasures. And, it also prevented compromise and botnet hijacking by only accepting updates from an authorized source.

Conficker’s origins and malicious intent are unknown, although it remains a large potential command and control network awaiting activation to spread future infections or launch denial of service attacks. It is a threat for unpatched Microsoft systems, with Microsoft Windows XP/IE6 combinations being most infected, followed by systems with unauthorized or pirated Windows or no security updates. Conficker also spreads via virus scareware, urging recipients to download a security update containing a Conficker executable.

Gozi

Gozi was the first malware to pack executable files to help escape signature-based anti-virus defenses. Packing programs generate several versions of the same malware, making each version appear unique. Anti-virus experts first had to unpack and decipher malware payloads and then identify changed polymorphic exploits before designing Gozi countermeasures.

This Russian virus, distributed as a Trojan, targets financial data by exploiting an Internet Explorer browser vulnerability. One variant targets a PDF vulnerability. Gozi grew the commercial malware business model with a mix of attacks and new levels of sophistication. Gozi has the ability to steal data from encrypted secure sockets layer (SSL) tunnels by intercepting keystrokes with a keylogger before the session is encrypted.

Mariposa

The Mariposa botnet that made headlines in March 2010 included 12.7 million compromised PCs representing half of the Fortune 1000 and more than 40 banks. It spread using a Microsoft Internet explorer vulnerability, Microsoft's Instant Messenger, and USB sticks.

In addition to its scale, the botnet showcased the evolution from teenage hackers to big business. The Mariposa ringleaders were "not like these people from the Russian mafia or Eastern European mafia who like to have sports cars and good watches and good suits—the most frightening thing is they are normal people who are earning a lot of money with cybercrime," commented Cesar Lorenza, a captain with Spain's Guardia Civil, discussing the Mariposa botnet with reporters.⁷

Queen Bots

A "queen bot," a botnet controller embedded in a website, distributes polymorphic viruses to infect or update the machines of site visitors. Polymorphic viruses change every use, so when they infect compromised web servers, they escape detection by existing signature-based defenses. Queen bot addresses are added to block lists and reputation filters as they are discovered. However, agile criminals circumvent IP reputation defenses against malevolent websites with "fast flux" and "double flux" techniques to quickly rotate IP addresses and authoritative DNS servers. This constant movement has increased the difficulty of ISPs to shut down compromised hosts and has complicated forensics.

Detecting and Combating Malware

Most malware infections are detected by users observing unexpected computer behavior. Classic symptoms of an infected system are slow performance, excessive disk activity on an idle machine, frequent unexpected pop-up windows, and the inability to run or update anti-virus software. Much of today's malware installs updates to help escape detection. Infected systems are prone to re-infections, usually from risky web surfing, so active defenses are called for. At all times, users should run anti-spam and desktop anti-virus software to screen malicious code and repeatedly scan for and remove infections. Here are some other measures companies and users can take to block malware from their systems:

- Implement layered security company wide. Using anti-spam, anti-virus, and anti-spyware solutions on the network and at the gateway, in addition to endpoint anti-virus, increases security beyond desktop solutions alone. Cloud-based services can deflect spam and malware before it ever touches your network.
- Deploy a firewall at the network perimeter and on the desktop to prevent infections by blocking inbound malicious traffic. Network firewalls also can block unwanted outbound traffic, such as Internet Relay Chat (IRC), peer-to-peer (P2P), instant messaging, FTP, or other protocols used for malicious purposes, such as botnet communications. Host Intrusion Prevention Systems (IPS) provide more sophisticated defenses to block attacks and compromise on the desktop, laptop, and server.
- Use "strong" passwords. It's critical to select passwords that are difficult for attackers to guess, so they should have a combination of letters, numbers, and special characters that do not spell dictionary terms or common catch phrases.
- Use different passwords for each application, an especially critical rule for online banking and other sites and applications that access personal information. Many keyloggers capture passwords from one account to reuse on another, since using the same password for multiple accounts is common. Never write down or share passwords between users. Ideally, you should change passwords every three months.
- Do not allow the computer to remember passwords.

- Keep software up-to-date. Installing software patches increases the difficulty of exploiting known vulnerabilities. Enable automatic updates to operating systems and anti-malware applications to make installation easier.
- Never download from unknown or untrusted sites or individuals. It's critical to insure the validity of websites that are visited by typing URLs directly into a browser instead of clicking links. Use online reputation services, such as McAfee SiteAdvisor and McAfee SECURE, to assess the safety of links when you search or before you click.
- Ensure that anti-malware software is from a reliable vendor (not free or rogue anti-virus), actively scanning, and up to date with virus and malware definition files (DATs). Activate dynamic updates, such as McAfee Artemis technology, to assess threats between DAT updates.
- Don't assume systems are secure because they have anti-virus software installed. In many cases anti-virus software cannot accurately detect polymorphic or zero-day viruses and Trojans. Additionally, some desktop scanning software can't detect malware until the system is already infected—after it's installed in the operating system of the PC. Some malware will turn off anti-virus or make it appear that the scans are running, while hiding undetected.
- Think before you click. Just as with email spam, the short URL or subject in a tweet or IM may be misleading. If a file or link comes unexpectedly from a "friend," it makes sense to validate its legitimacy through a separate communication before opening. Remember, an infected machine will attempt to infect other "friends."
- Control and check portable storage devices. Anti-malware should scan USB devices and other handheld devices before they attach to laptops or other hosts. Consider using technology to limit the range of devices that can be used or the actions they can perform (such as transferring to or from the device).

Protecting Assets

A layered approach to security is the best defense. Desktop and server software, network appliances, and managed services all provide different levels of protection against different threat types. As threats become more sophisticated, having multiple checks increases the probability that one layer will detect a threat en route to its destination, or detect a threat that is originating within the network from a device that is already infected. Multiple anti-malware layers provide better protection than any single solution, regardless of the strength of a vendor's product. Also, multiple defensive applications running on a single platform can consume so much processing, memory and storage that it decreases performance. A layered approach adds multiple security checks with no performance penalty, allowing stronger security for more systems.

The McAfee Security SaaS Advantage

One of the simplest and most effective ways of adding a protective layer is to include a managed service in the security mix. Cloud-based security services, or Security-as-a-Service, sit outside of the corporate infrastructure, providing another security buffer in the network cloud.

McAfee Security SaaS suites combine the power and protection of industry-leading email security, web security, and email archiving security-as-a-service - all backed by live, 24/7 support, innovative technology, and our experienced team of threat experts. These McAfee services provide powerful, accurate protection that gives customers the confidence to focus on their core businesses and leave the threats to us. Between our dedicated security experts and the enormous visibility we have into global threats, McAfee can consistently provide the fastest response to new outbreaks. Our services are easy to set up and administer, available with one integrated console, and backed by 24/7 live customer support.

McAfee SaaS Email Protection

As a cloud-based service, McAfee SaaS Email Protection filters spam and viruses from email messages before they hit the corporate network. Up to 90 percent of all email messages is spam, so stopping those messages in the network cloud saves 90 percent in email processing and network bandwidth.



Reduced message traffic cuts the workload of email servers, reducing network latency, lowering email storage costs, and cutting archival needs. Cloud-based email filtering services also buffer corporate networks from spammers trying to find valid email addresses with directory harvest attacks. This classic spam technique is a guessing game, attempting to find valid email addresses using combinations of names and initials. SaaS Email Protection detects and stops directory harvest attacks in the network cloud with no impact on the corporate network or email system.

Proprietary WormTraq™ protection adds mass mailing worm detection to multiple layers of anti-malware engines. In addition to protecting from email-borne threats, SaaS Email Protection adds defenses for denial of service and other network threats that could disable networks and prevent access.

This multilayered, cost-effective solution offers rapid activation and is easy to configure and manage, helping to reduce IT-related costs and corporate liability while increasing employee productivity. Positioned between the Internet and the business network, SaaS Email Protection leverages the most effective technologies and techniques within more than 20 layers of filters to identify, quarantine, block, and strip email threats.

McAfee SaaS Web Protection

Like email protection, a security-as-a-service model strengthens web protections. McAfee SaaS Web Protection guards against threats to web browsers while providing content control.

Web security-as-a-service from McAfee prevents users from accessing phishing or spyware sources through a comprehensive set of reputation layers. Additionally, files from trusted websites are scanned for Trojans and viruses before reaching the corporate network. As another benefit, spyware is blocked from sending information back to controllers. The system blocks spyware requests and reports infected machines for corrective action.

Content controls are included. Companies can enforce acceptable use policies restricting objectionable content, and administrators can block access to entire categories of web content, such as porn, gambling, social networking, or sports-related sites. More restrictive policies can prevent access to news, music, or shopping.

SaaS Web Protection minimizes the risk of costly web-based malware and objectionable content to systems, users, and the business. With the advent of Web 2.0 and evolving web and email blended threats, organizations are more at risk than ever before from new threat vectors.

McAfee Global Threat Intelligence

All of these award-winning services benefit from McAfee Global Threat Intelligence, which powers the groundbreaking McAfee threat technologies, including McAfee Artemis™ technology and McAfee TrustedSource™ service. Continually tuned threat protection is distributed throughout the McAfee portfolio of endpoint and network security products.

Global Threat Intelligence is a comprehensive solution that tracks the entire threat lifecycle, enabling predictive security to guard against the latest vulnerabilities, ensure regulatory and internal compliance, and lower the cost of remediation.

Global Threat Intelligence was created and refined by McAfee Labs to power the next generation of security. Spanning the entire Internet, Global Threat Intelligence uses millions of sensors to gather real-time intelligence from host IP addresses, Internet domains, specific URLs, files, images, and email messages. It seeks new and emerging threats, including malware outbreaks, zero-day exploits, and malicious zombie senders generating spam and web attacks. The McAfee Labs team of more than 400 researchers in 30 countries is dedicated to providing the most relevant security information by tracking and analyzing the latest threats.

Enterprise-class protection

Many organizations cannot justify expensive high-end security safeguards. A managed service delivers the benefits of sophisticated technology with redundant systems, 24-hour monitoring, and expert threat knowledge that normally only well-funded large enterprises can enjoy. McAfee provides all the advantages with no hardware or software to install, administer, or maintain.

Conclusion

Email, the Internet, and other online tools are critical for success in today's businesses, but bring the risk of malicious attacks. Understanding and recognizing the threats is the first step in managing the e-business risk. Effectively removing the risks is best with layers of security to find and stop Internet threats before they infect a system, expose sensitive information, or damage a network. Security-as-a-service from McAfee provides a highly effective security buffer, providing new levels of assurance for corporate networks. Learn more at www.mcafee.com/saas.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>.

