SEARCHSECURITY.COM

technical guide on

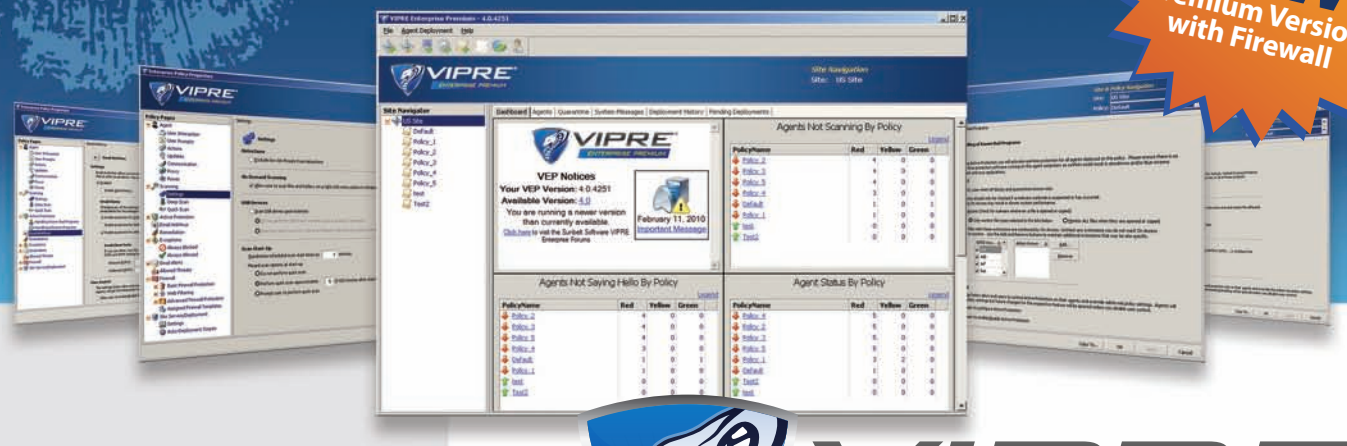
COMBATTING EMERGING Web Threats

contents

TechTarget

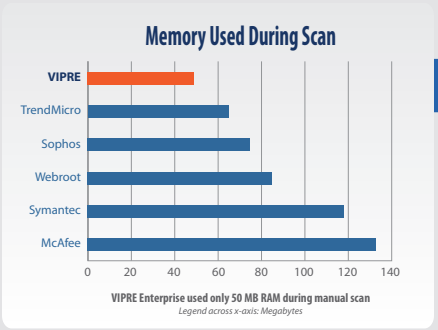
Kiss your antivirus bloatware goodbye

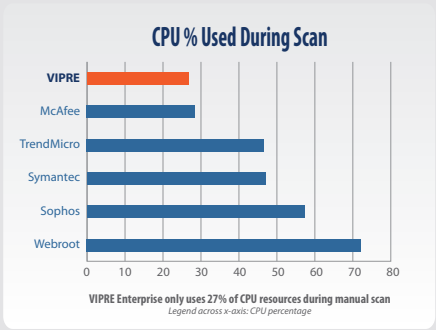
NEW Premium Version with Firewall



VIPRE®

TEST DRIVE ENTERPRISE PREMIUM





How does your current software compare? VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

Sunbelt Software

Special Competitive Upgrade: *50% Discount!*

Until now, antivirus engines have been Frankensteins, bolted together from bits and pieces of different products. They're slow, full of bugs, and hard to manage.

VIPRE Enterprise Premium is a revolutionary new approach. It combines high-performance antivirus, antispyware, and desktop firewall into a single agent so you get comprehensive endpoint malware protection with low system resource usage. It's fast, powerful and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Ask for a quote with our 50% competitive upgrade discount!

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

Curious? Download your FREE copy of VIPRE Enterprise Premium and give it a test drive.

When you compare VIPRE Enterprise Premium to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though.You can get VIPRE Enterprise Premium with a **50% competitive upgrade discount!**

Compatible with Windows 7

BEST IN TECH 2009 Business Administrator

Windows IT Pro 2009 Community Choice GOLD

vb 100 VIRUS virusbtn.com

Plus we will buy out your existing maintenance contract for 1 year!

Download now: www.TestDriveVipre.com

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.SunbeltSoftware.com sales@sunbeltsoftware.com

Discount available on new licenses only for a limited time. Buy-out offer good on contracts up to 1 year. Subject to change without notice. Contact your Sales Representative for details.

insight

Combatting Emerging Web Threats

Attackers are almost exclusively targeting enterprises with hacks perpetrated over the Web. As most enterprises move operations and functionality online, Web-based applications become a tempting threat vector for sophisticated hackers.

SEARCHSECURITY.COM presents a comprehensive guide to combatting emerging Web threats. Our experts cover all the angles around the latest hacker techniques as they exploit Web vulnerabilities and target your most important data. Learn more about memory-based attacks, botnet prevention, man-in-the-middle SSL attacks, and the realities of cyberwarfare.

contents

Everything you want in an AV solution.

eset®

Internet Security

NEW
Remote Administrator 4 features:

- Intelligent group manager
- Firewall rules merge wizard
- Improved policy manager
- Simplified remote administration
- Cross-platform management

Protection, speed and flexibility.

ESET NOD32 Antivirus 4 + Remote Administrator

ESET NOD32® Antivirus 4 Business Edition is more than simply powerful Internet security. It's a comprehensive network-wide solution. And, when paired with ESET Remote Administrator, it takes the headaches out of IT management. Light on client resource consumption and easy to manage, ESET NOD32 + Remote Administrator (RA) saves money that might otherwise be wasted upgrading computers running sluggish AV. And because it's so easy to manage, your IT department gets back what it values most — hours in the day.

Proactive protection

We scan all incoming and outbound network traffic, email attachments and removable media — but that's not enough. We compare unknown code to millions of database signatures — but that's not enough either. We even have frequent ultra-small updates that incorporate signatures from threats encountered across ESET's 100-million user network — but you still need more.

Superior protection doesn't depend on updates at all. In comparative testing using outdated signatures, ESET consistently outperforms other AV solutions. "ESET offers the highest proactive threat detection," independent AV-Comparatives May 2009.

The difference? Advanced heuristics. Proactive protection that doesn't just passively look for existing features of malware — it actively predicts strains that haven't been written yet and sandboxes them in a controlled disk environment where they can do no harm. And when a block of code seems suspicious — it is immediately repaired or quarantined. Smoothly. Efficiently. Seamlessly.

Unmatched speed

On the user end, ESET runs just two processes — the scanning kernel and the user interface — and together sip just about 44 MB of RAM. Typically, that's less than an instance of Word, Communicator, Excel, Explorer or Firefox. And with minimal interruptions or pop-ups and no scanning slowdown at file open or startup, your users won't even notice its running. But they will notice they no longer need to phone IT for lagging startups or malware infections.

On the server side, mirrored downloads and small signature updates mean your network traffic will never lag because of your antivirus solution. Mail scanning happens in the blink of an eye and compatibility with a variety of protocols and systems, from Cisco NAC to Microsoft Exchange means that you'll never have to deal with multiple antivirus solutions for your mixed network.

Flexible management

For mixed networks, ESET NOD32 delivers comprehensive protection — working natively in Windows XP, Vista and 7; Linux / BSD / Solaris; Mail Server; Exchange; and soon Linux Desktop and Apple Mac OS X.

Vast multiplatform protection doesn't have to be a management nightmare. ESET Remote Administrator allows for simple push-installation of preconfigured NOD32 packages to client computers and now with RA4 – allows Active Directory management of dynamic networks.

The combination of ESET NOD32 + Remote Administrator means simple, powerful management of a network of 10 computers or 10,000 with protection for every system and every platform. Each computer is an attack surface — and you need the best available protection on all of them.

Solutions to fit all your business needs

- File server security
- Mail server security
- Gateway server security
- Mobile phone security

www.eset.com/business/products

Request your free trial at www.eset.com/business-trial

MEMORY ATTACKS

Defending Against RAM Scraper Malware in the Enterprise

A new type of memory-based malware attack, RAM scraping, may pose a serious threat to enterprise security. BY NICK LEWIS

A NEW TYPE of malware designed to capture data from volatile random access memory (RAM) within a system is on the rise. RAM scrapers, which were brought to light in a Verizon Data Breach report, represent a relatively new method of attack on credit card data.

However, RAM scraping isn't entirely new. A different form of RAM scraping was used in the cold-boot attacks of 2008. For those who don't remember, researchers demonstrated how to subvert disk encryption by abruptly cutting a computer's power, which causes its RAM to preserve a near-perfect copy of its most recent memory image. Simply by cooling and removing its RAM chip, dropping it into another computer and examining the RAM chip, an attacker can obtain the original computer's disk encryption key in a matter of moments. The attack could even be effective without taking the memory out if the computer was power cycled and immediately loaded with a specialized operating system designed to dump the contents of memory.

Today's RAM scrapers are able to bypass most security protections and access credit card data by either injecting themselves into running processes to hide, or directly executing on machines.

The cold-boot vulnerability clearly pointed out that data stored in RAM was there for the taking. This same method could be used to access credit card data stored in RAM, but the RAM scrapers in the report didn't require physical access.

Today's RAM scrapers are able to bypass most security protections and access sensitive credit card data by either injecting themselves into running processes to hide, or directly executing on machines. Once in a system, the RAM scraper can read passwords, encryption keys, credit cards, Social Security numbers, or any other type of data that is easy to monetize. The RAM scraper then can either save this sensitive data to a local system or send it directly to the criminals via a number of different methods. Even if the stolen credit card data is encrypted, damage can still be done if

the attacker is able to also grab the private key used for encryption in a method similar to that described earlier.

RAM Scrapers in the Enterprise

So then it's no surprise that RAM scrapers can compromise enterprise information security in many different ways. This form of malware can gather data by reading directly from memory, or even from a swap file (virtual memory on a hard disk) if it's being read offline. Regardless of how it obtains the data, in order to be successful, a RAM scraping attack must either exploit a configuration weakness to be able to read all of the memory, or have the executable run with enough privileges to read the memory. Reading from all the memory is slow, inefficient and easier to detect, but it is still a potentially effective attack.

Attacking software is another possible target for RAM scrapers. More specifically, such malware attacks the memory management aspect of software and sensitive data. This would be more efficient than reading all the memory, because it would have to monitor where the program wrote to memory, rather than read gigabytes of memory. In addition, this RAM-scraper method is more difficult to detect, but there are also drawbacks for the attacker.

Crafting RAM-scraping malware requires a higher level of sophistication than most commonly seen malware because it must be tailored for the specific software or environment.

These types of attacks represent a realistic threat to enterprises, but only for high-value targets. Crafting RAM-scraping malware requires a higher level of sophistication than most commonly seen malware because it must be tailored for the specific software or environment.

To defend against RAM scraping, it's a good idea for enterprise IT security managers to make sure preventive and detection measures are in place for the organization's high-value targets, typically devices where sensitive data resides or that may represent a way to easily obtain access to it. Obviously those targets need to first be identified, and then evaluated to determine if existing defensive measures are adequate, or if new technology or processes are needed.

Putting a process in place to follow up on potential RAM-scraping attacks (or any attacks, for that matter) is as important. If network-monitoring systems identify when a high-value target, such as a stationary point-of-sale terminal, starts communicating with new systems on an internal network in the enterprise or on the Internet, this alert should not only draw the attention of the security staff, but also be investigated quickly. Investigating potentially illegitimate communications quickly could help to identify serious incidents early on and limit or prevent damage or data loss.

Also to protect against RAM-scraping attacks, systems should not be run at an administrative level, or with generally high levels of system access. The easiest way for an attacker to get access to the sensitive data from RAM is by exploiting software already running with administrator-level privileges. Secondly, the location of sensitive data should be kept up to date in a detailed systems inventory. IT infrastructures

grow and change over time, so it's important to make sure security measures are in the right place.

RAM scrapers aren't new, but recent developments represent an evolution in prior attacks that will continue to advance in the future. Enterprises must continually improve their defenses by implementing some of the aforementioned best practices to make sure sensitive data is protected effectively as possible.›

Nick Lewis (CISSP, GCWN) is an information security analyst for a large public Midwest university responsible for the risk management program and also supports its technical PCI compliance program.

A Vision of Next-Gen WAF

Imperva is the global leader in data security. Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk.

Hacking has become "industrialized" with a well organized infrastructure, defined roles and responsibilities, and sophisticated attack vector automation that generate large-scale attacks of unprecedented size, speed, and devastation.

The industrialization of hacking coincides with a critical shift in focus. Sensitive data is the new target. Data drives businesses more today than ever. In order to protect the business, organizations need to protect the web applications and the data. This level of defense requires the next generation web application firewall.

Learn more and download the following two whitepapers:

www.imperva.com/go/NG-WAF

White Paper: The Industrialization of Hacking

This whitepaper identifies the "Industrialization of Hacking"

White Paper: Next Generation Web Application Firewalls (NG-WAF)

This whitepaper explores Imperva's vision of next generation WAFs, or NG-WAF in three interrelated sections covering: industrialized attack mitigation, interoperability and service delivery models, and risk management. It also highlights some of the capabilities currently delivered through Imperva's SecureSphere solution.

iMPERVA®
Protecting the Data That Drives Business

3400 Bridge Parkway
Redwood Shores, CA 94065
Tel: +1 (650) 345-9000

info@imperva.com | www.imperva.com | Blog | Twitter | YouTube | iTunes | LinkedIn | Facebook

WINDOWS SECURITY

Server Message Block Version 2 Security in Question: Disable or Patch?

Learn about the Microsoft Server Message Block flaw and why you may have to disable SMBv2 as a workaround, or wait for a patch update. BY NICK LEWIS

LAST SEPTEMBER, Microsoft advised users of a remote code execution vulnerability found in its Server Message Block Version 2 (SMBv2) protocol. SMB is a file sharing and printing protocol used in Windows to pass messages between networked devices.

Researchers developed working exploit code that could be used to exploit the flaw and cause a denial of service (DoS) or unauthenticated remote code execution. This exploit code has been publically released as well.

Early on, Microsoft released a fix that disabled SMBv2. SMBv2, an update to the protocol, is supported only on Windows Server 2008, Windows Vista and Windows 7, and can be used only if the client and server support it. Windows Vista SP2 and prior and Windows 2008 SP2 and prior are vulnerable. Windows 7 Release Candidate is also vulnerable, but was patched prior to Windows 7's official release. Windows XP, Windows 2003 and Windows 2008 R2 are not vulnerable.

In October, Microsoft issued a security patch as part of its normal Patch Tuesday cycle. Enterprises were advised to apply this patch during their normal patching cycle, and if they could not deploy it, they should have done so prior to the next Microsoft patch release. In this article, let's explore why enterprises should consider expediting SMB patch deployment or using one of the workarounds.

Remote code execution or denial-of-service attacks are serious threats to an environment. The Server Message Block Version 2 security vulnerability could be incorporated into bots, worms or other malicious code to attack an organization, access its data and gain a further foothold into its network. Many bots, worms, or other types of malicious code are developed in a modular fashion to easily incorporate new attack methods and vulnerabilities.

For example, the notorious Conficker worm (or Conficker/Downadup) used several different Windows vulnerabilities to spread and infect systems. Similarly, the SMB vulnerability has the capability to be included in a worm and spread quickly. While the exploit code hasn't yet been included in other malware, it could be incorporated into worms or bots and used in targeted attacks. It also has been included in the Metasploit open source penetration testing framework.

However, the likelihood of being exploited on client computers is negligible, unless several best practices are not followed, namely disabling the default host-based firewall and not firewalling Windows networking, including SMB functionality, at the perimeter(s). The exploits depend on malicious code reaching a vulnerable host over Windows network using SMBv2. The likelihood of being exploited on Windows Server 2008 is higher because a file or print server would not be able to firewall off Windows networking from clients' systems.

Enterprises unable to deploy the patch immediately should use one of the workarounds, which will disable SMBv2 to ensure adequate projection of your systems until the patch is deployed; we'll get to those in a minute. But one question an enterprise must answer before deploying a workaround is whether doing so will be less effort than deploying the patch. The deployment mechanisms are potentially different between the patch and the workarounds.

The patch can be deployed with standard patching tools, but executing a workaround may require additional test and deployment efforts.

The patch can be deployed with standard patching tools, but executing a workaround may require additional test and deployment efforts. There are two ways to disable SMBv2 using workarounds: Microsoft released a FixIt package that will disable version 2 of the Server Message Block. SMBv2 can also be undone via a registry key that requires restarting the server service. Both will require re-enabling SMBv2 after the patch is deployed to make the functionality available again.

Disabling the server service has been suggested as a workaround, but this may have a significant effect on systems because the server service is core to the operations of some management systems and providing Windows file and print services. An additional workaround is to re-enable the Windows firewall to the default state. Both of these options would need significant testing prior to deployment; dependent software or services need to be identified by re-enabling the Windows firewall.

For future similar Windows networking or SMB vulnerabilities, enterprises should follow the same advice and compare the effort to deploy the patch, workaround, and availability of exploit code to determine the most appropriate strategy for their environments. Compare the risk for a new vulnerability and exploit to your environment to the amount of effort to adequately protect your environment from a new vulnerability. Deploying perimeter firewalls and utilizing client firewalls will help reduce the risk from computers being exploited over the network by the SMBv2 vulnerability.

Nick Lewis (CISSP, GCWN) is an information security analyst for a large Public Midwest University responsible for the risk management program and also supports its technical PCI compliance program.

Even **Zero-hour** Defense Leaves Open a **Window of Vulnerability**

You may think zero-day (or even zero-hour) defense provides adequate protection but, by the time you wake up in the morning, cybercriminals may have already slipped malware into the network. This window of vulnerability — even just one hour — compromises IT resources.

It's time to think faster.

M86 Security closes the Window of Vulnerability. Our patented, Real-time Code Analysis stops new Web threats missed by zero-hour technologies, and the M86 Dynamic Web Repair Engine removes malicious scripts from Web pages, delivering safe content to end users and enabling IT to stay focused on mission-critical applications.

Learn more about stopping new, Web-based Malware — in real time — with the **M86 Secure Web Gateway**. For additional information on zero-day vulnerabilities, visit: **www.m86security.com/zero-day.**

M86™ SECURITY

Real Time Security for the Borderless Network

Call 888.786.7999

BOTNET PREVENTION

Best Practices for (Small) Botnets

You may have a strategy to deal with a large botnet , but how would you deal with a micro-botnet that knows how to bypass antivirus and firewalls? BY MARCOS CHRISTODONTE II

LARGE-SCALE botnet events, such as those used to disrupt Twitter and Facebook, have been highly publicized in the news. While these high-profile security events have been hard to miss, it's the smaller, stealthier botnet attacks that may prove to be a greater threat to enterprises.

To take on evolving enterprise defense mechanisms, attackers look for weak spots, and have begun using smaller, less noticeable botnets to evade enterprise safeguards. In this article, we'll discuss why these so-called micro-botnets are proving successful, and how to identify and prevent them from doing damage.

Why Smaller Botnets are Better

Large botnets are frequently used to launch denial-of-service (DoS) attacks. To bring down an e-commerce website or to prevent an organization from accessing the Web, these attacks require resources—namely a botnet army. Much like sending thousands of soldiers to overwhelm an enemy in battle, attackers use the pooled resources of many computers to overwhelm a victim server or network. When an attacker wants to launch a DoS attack against an organization, he'll send commands to his dispersed botnet army to focus on his victim. Because this creates multiple connections within the target environment, it draws nearly all the attention (and resources) of host and perimeter protection systems, often rendering the victim helpless or even knocking its systems offline entirely.

Unlike large botnets flooding a network to deny service, micro-botnets are less likely to be detected. Because they utilize fewer slave computers, and in turn send fewer data packets, they are superior at evading traditional botnet-detection capabilities in firewalls and intrusion detection systems. To further avoid detection, a botnet controller can configure his or her micro-botnet to disable antivirus software (while the software still appears to be working properly), lie dormant for long periods, or call home for new commands at irregular intervals. Without a signature in place to detect them and no pattern of abnormal behavior, micro-botnets can make it difficult for even a state-of-the-art behavior-based intrusion prevention system to notice them.

Why Micro-Botnets are Successful

To get inside the enterprise, past firewalls and IPSes, attackers often target users.

Using social engineering attacks to target users is one of the easiest ways to infiltrate an enterprise. It's relatively easy to find information on an organization and its employees, and then incorporate that info into a crafty phishing email with a malware-laden attachment. Probing and footprinting a network for weaknesses, also popular tactics for micro-botnet herders, takes much longer than sending a simple email. Once a machine is compromised, the attacker can either send their malware additional commands to compromise other hosts and further expand the botnet, extract target data from the victim network, or simply sell the botnet to someone else and move on to the next victim.

Worse yet, once they compromise a network, micro-botnets can lie dormant for a period of time, waiting on further commands or a specific "trigger" event. Unlike large botnets that require better command and control and may result in bots not responding properly or being discovered, a smaller botnet is more precise and best suited for targeted attacks, especially in an effort to pilfer specific data.

Micro-botnets often use blended methods to access sensitive data. They can discreetly probe networks a few packets at a time, search for trade secrets using hijacked accounts, and disable antivirus by removing critical software files.

Micro-botnets can ferret out data much more efficiently than traditional botnets. Micro-botnets often use blended methods to access sensitive data. They can discreetly probe networks a few packets at a time, search for trade secrets using hijacked accounts, and disable antivirus by removing critical software files. A micro-botnet will attempt to perform these and other blended attacks while quietly traversing the network alongside normal traffic.

Practices to Help Find and Stop Micro-Botnets

It's obvious that the human element is an issue, and that botnets are evading traditional defenses to break into enterprise environments. To protect itself against micro-botnets, an organization must begin allocating more resources toward detecting botnets rather than focusing solely on preventing them. As discussed above, the sophistication of botnets has enabled them to get inside more often—simply put, traditional defenses don't always work. Not to say that prevention isn't needed, but detection of botnets already inside the enterprise, or one mouse click away, must take precedence. The mentality that a firewall, IDS, or malware protection software will take care of attacks creates an environment with a false sense of security. Organizations must do more to understand what's happening within their networks.

Knowing and understanding network activity will enable earlier identification and better responses to attacks. However, this goes beyond asset management and encompasses the understanding of all running processes on hosts, where those hosts reside, and the ports they use. It includes mapping the environment and maintaining up-to-date configuration details around client-side software.

If and when micro-botnets begin to show themselves, however subtly, you need to

notice the abnormal spikes in network traffic, weird open ports, and accounts suddenly gaining elevated permissions. If you're using a pattern scanner, turn up the sensitivity level and spend a little extra time determining what is or is not a false positive. It's good network hygiene to exercise log analysis to know what's really happening on the network. To help automate much of the log analysis, look for products such as those offered by LogLogic Inc., ArcSight Inc. or Tenable Network Security Inc.

Finally, training and educating users can't be taken lightly. Users must understand how to identify and report abnormal network behavior, and avoid falling victim to social engineering and phishing attacks. Training must be fun in order to gain users' attention, and it should include a process to validate that the users understand the lessons. To look out for and thwart micro-botnets, organizations must integrate better training with the above measures into their enterprise security strategies.

Marcos Christodonte II, MBA, CISSP, is an information security professional working for a consulting firm.

SSL/TLS SECURITY

How SSL-Encrypted Web Connections are Intercepted

Learn how SSL-encrypted Web connections are intercepted, using man-in-the-middle attacks and forged certificates.

BY SHERRI DAVIDOFF

ENCRYPTED WEB CONNECTIONS are routinely intercepted by enterprises for legitimate reasons. Unfortunately, attackers can use the same methods for tapping into "secure" connections, most often because of endpoint weaknesses.

In this tip, we'll examine how enterprises and attackers intercept Web connections that are encrypted using the Transport Layer Security (TLS) protocol or its predecessor, the Secure Sockets Layer (SSL) protocol.

A digital certificate, often used in conjunction with TLS/SSL, is just a little chunk of data describing an identity—such as the name and URL of an organization—signed with a digital signature. Signing is a complex mathematical operation based on the contents of the certificate and the signer's cryptographic key. If the values in the certificate are altered in transit, the digital signature will not match, and a browser will display an error message.

A digital certificate, often used in conjunction with TLS/SSL, is just a little chunk of data describing an identity—such as the name and URL of an organization—signed with a digital signature.

How do you know if a digital certificate is really owned by the person you think? It's all a chain of trust. When you go to Alice's website, for example, she presents you with her certificate. Alice's certificate has been verified and signed by her friend Bob. In turn, Bob's certificate has been verified and signed by his friend Charlie. Charlie is also a good friend of yours, and you trust him implicitly. Charlie in this case represents a root certificate authority (CA) for our public key infrastructure (PKI). When you see Charlie's signature on Alice's verifiable certificate chain, you trust that Alice is who she says she is.

In real life, your Web browser comes with pre-installed, trusted root CA certificates from network infrastructure companies such as VeriSign Inc. Your Web browser will automatically trust digital certificates issued by the pre-installed root CAs. Attackers, however, can exploit this trust.

How trustworthy are digital certificates?

Nobody's perfect—not even trusted root certificate authorities. In 2001, VeriSign mistakenly issued "code-signing digital certificates to an individual who fraudulently

claimed to be a Microsoft employee." According to the Microsoft Security Bulletin MS01-17, "the ability to sign executable content by using keys that purport to belong to Microsoft would clearly be advantageous to a malicious user who wanted to convince users to allow the content to run. The certificates could be used to sign programs, ActiveX controls, Microsoft Office macros, and other executable content."

Digital signatures can also be forged. In 2008, at the Chaos Communication Congress in Berlin, a group of researchers leveraged weaknesses in the MD5 cryptographic algorithm to create a "rogue" certificate with a valid root CA signature (Sotirov et al). This certificate had never been signed by the trusted root CA, but since it had a valid signature, it was trusted by all common browsers.

SSL interception tools

More commonly, attackers bypass TLS/SSL connections using man-in-the-middle techniques along with certificates that are generated on the fly.

Enterprises routinely intercept TLS/SSL connections. Why? Imagine you are an employee checking your Web-based personal email at work. Your company has strong incentive to peek into your traffic, to make sure you aren't leaking proprietary data or mistakenly downloading viruses. Enterprises frequently want to inspect all traffic flowing into and out of their network to prevent malware infections and protect their proprietary data.

Encrypted Web connections are routinely intercepted by enterprises for legitimate reasons. Unfortunately, attackers can use the same methods for tapping into "secure" connections, most often because of endpoint weaknesses.

To break a TLS/SSL connection and sniff employee traffic, enterprises often use an SSL proxy, such as ProxySG from Blue Coat Systems Inc.

To break a TLS/SSL connection and sniff employee traffic, enterprises often use an SSL proxy, such as ProxySG from Blue Coat Systems Inc. The SSL proxy intercepts traffic between an individual's computer and the outside world. When a user surfs to a "secure" site, the SSL proxy fetches the real Web server certificate and establishes a legitimate TLS/SSL connection between the proxy and the Web server. Then, the proxy makes a fake digital certificate on the fly, which looks similar to the Web server's certificate. It presents this fake digital certificate to the user, and sets up a second TLS/SSL session between his or her browser and the Web proxy. The user may receive a pop-up error message (and probably click it away) because the fake digital certificate is not trusted. Of course, if the organization takes the time to import the proxy's certificate as a trusted root in user Web browsers, then users won't see an error message at all.

The net result? There is a "secure" TLS/SSL session between the user's computer and the proxy, and a second "secure" TLS/SSL session between the proxy and the Web server. On the proxy itself, the individual's information can be viewed in plain text. The company can then automatically search the traffic for specific keywords, or screen it for malware.

Unfortunately, attackers can use the same techniques as enterprises to intercept

SSL connections. One particular free, publicly available tool makes this trivially easy. As with enterprise TLS/SSL interceptors, the attacker can use such a tool to automatically connect to the real Web server, capture certificate information, and generate a new certificate on the fly with the same information. It then presents the user with the new certificate and sets up an SSL connection. From that point on, there is a "secure" SSL session between the user's computer and the attacker, and a second "secure" SSL session between the attacker and the Web server. Another similar tool exists that removes the client SSL connection entirely, and uses social engineering techniques (such as lock icons) to trick users into thinking the connection is encrypted.

What can users do to protect against SSL interception attacks? Here are four key strategies:

1. Always use a trusted computer when surfing to sites with valuable information. If your computer is untrusted or has been compromised, then someone could have installed an illegitimate trusted certificate authority in your Web browser.

2. Consider using integrity-checking or rollback software to detect and eliminate unauthorized changes to trusted certificate authority lists.

3. Do not accept untrusted certificates. If possible, configure users' browser to automatically reject untrusted certificates.

4. Think before you click. Remember, even trusted CAs make mistakes. Train employees and home users to think critically about visiting websites.

TLS/SSL is like a nice sturdy two-by-four. Can you use it to build a secure infrastructure? Yes. Is it a secure infrastructure all by itself? No.

An entire industry has grown around SSL interception. Enterprises and law enforcement want to be able to tap into encrypted traffic just as much as attackers, so the incentives for stronger protections at the endpoints are mixed. However, with careful attention to detail, businesses and home users can detect and avoid TLS/SSL interception and bypass attacks.

Sherri Davidoff is the co-author of the new SANS class "Sec558: Network Forensics" *and author of* Philosecurity. *She is a GIAC-certified forensic examiner and penetration tester.*

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

CYBERWAR

Cyberwarfare and the Enterprise: Is the Threat Real?

Learn about methods to defend against cyberattacks, botnets, cyberaccidents and distributed denial-of-service attacks. BY SHERRI DAVIDOFF

IN JULY 2009, there was a great deal of press about a "massive cyberattack" supposedly originating from North Korea, targeting high-profile South Korean and U.S. websites. The attacks were reportedly launched by "tens of thousands" of infected computers "around the globe," which were used to launch a distributed denial-of-service (DDoS) attack. Oh, and the infected systems were supposed to self-destruct (presumably taking the world with them).

Most security geeks just scratched their heads and wondered how an average-size, rather unsophisticated botnet attack with relatively low impact managed to make it above the fold on the front page of the *Wall Street Journal*. A few public-facing government websites were slow or inaccessible for a few days, but there were no reports of financial damage or any serious service interruptions.

Why all the hype? Is cyberwarfare really something enterprise information security professionals should be concerned about?

Cyberwarfare is just a small component of a much bigger problem: the need to design a stable, global IT infrastructure.

The botnet that made headlines was tame, but in general, the potential for damage due to cyberwarfare (or cyberaccidents) is huge—not because of sophisticated enemies, but because our infrastructure is weak and not well maintained. In the U.S., critical infrastructure has come to depend on IT in ways that most people never realize. Skyscraper heating, cooling and access systems can be controlled via the Internet. Hospitals request heart transplants over VoIP phones. Those are just two examples, but there are many others that make it clear that a sophisticated, targeted cyberattack really could cause widespread chaos and even loss of life.

Cyberwarfare is just a small component of a much bigger problem: the need to design a stable, global IT infrastructure. Thoughtless teenagers have wreaked havoc on the Internet countless times without even trying. The Morris Worm of 1988, for example, caused greater devastation than the recent overhyped DDoS attacks, infecting thousands of major Unix machines. Our biggest problem is not that terrorists are out

to kill us all, but that even 23 years after Morris, our networked infrastructures are about as structurally sound as a Jenga tower.

Even purely accidental network outages have caused major damage to critical infrastructure. Back in 2002, Beth Israel Deaconess Medical Center's network was flooded and brought to a standstill due to an accidental spanning tree loop. Suddenly doctors and lab technicians could not view patient charts, lab results or fill prescriptions over the network. Eventually the emergency room was shut down and patients had to be shuttled to other hospitals.

What would happen if someone actually *tried* to disrupt critical systems using the Internet?

At the 2008 SOURCEBoston security conference, security researcher Dan Geer explored what could have happened with a piece of malware from 2001 called the Nimda virus. Just a few days after the September 11, 2001 terrorist attacks, Nimda spread across the Internet using five different infection vectors, infecting hundreds of thousands of computers within its first day. There is also another, older virus called E911, which caused infected systems to dial 911 over their modems repeatedly. Geer commented that, had the authors of Nimda considered including that functionality in their virulent code, Americans would have "gotten up the morning of Sept. 19 only to find there was no emergency service nationwide; it would have been turned off everywhere and all at once, like a light switch." That would have been just a few days after the nation was already reeling from a crisis.

How to Defend Against Cyberattacks and Cyberaccidents

It's hard to know what the next cyber crisis will be, but here are a few best practices that enterprise security teams should consider to avoid becoming victims.

1. Prepare for outages. Map your organization's information flow. Understand what systems/services depend on having critical network functionality. In many cases, companies simply cannot function without the network anymore. We don't have physical pens and paper or staff training to process all of our information. Develop communication and fallback plans for short-term (i.e. 1-hour), medium-term (i.e. 24-hour), and long-term (ie. multiple-day) network outages. Test them out, when possible. Be realistic; plan for what you can, and understand your limitations.

Prepare for outages. Map your organization's information flow. Understand what systems/services depend on having critical network functionality.

With the economy's struggles, many businesses do not have the resources to devote to disaster planning. As my mother says, just do your best.

2. Maintain systems. Patch all equipment routinely, including servers, workstations and network equipment. Be sure to include third-party applications. Audit routinely. Collect logs centrally. Even if you don't have time to proactively address disaster recovery, at least make sure to properly maintain the systems you have. Don't be the low-hanging fruit.

3. **Share information.** This might seem counterintuitive, but we're all in this together. If everyone in a particular industry is seeing the same types of probes or unusual activity, that can help us all identify precursors to incidents and avoid major catastrophes. Sharing information about effective and ineffective defense techniques can help us all respond more efficiently.
4. **Be a good neighbor.** Don't neglect non-critical systems. Even if there's "nothing important" on that Windows server in the corner, you don't want somebody infecting it and using it to attack other sites.
5. **Don't overreact.** Huge headlines about yet-another-cyberattack have unnecessarily fueled the fire. Now it seems that a relatively unsophisticated botnet can create global fear and potentially affect international relations, giving malicious individuals yet another incentive. We all have our share of security problems, and cyberwarfare is certainly one. If we all stay cool, however, attackers will have one less reason to launch cyberattacks.

The threat of "cyberwarfare" has been dramatically overhyped, but we are afraid for valid reasons: our national infrastructure is a mess. Accidents have caused just as much damage as "cyberwarfare" or other intentional attacks. "War" is not the problem; mismanagement, disorganization and fear are the real threat.

Sherri Davidoff is the co-author of the new SANS class "Sec558: Network Forensics" *and author of* Philosecurity. *She is a GIAC-certified forensic examiner and penetration tester.*

TECHTARGET SECURITY MEDIA GROUP

SearchSecurity.com

EDITORIAL DIRECTOR Michael S. Mimoso

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

EDITOR Marcia Savage

NEWS EDITOR Robert Westervelt

SITE EDITOR William Hurley

SITE EDITOR Nicole D'Amour

EDITOR Marcia Savage

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle,
Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann
peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

TechTarget
Where Serious Technology Buyers Decide

"Technical Guide on Combatting Emerging Web Threats" is published by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

SPONSOR RESOURCES

Sunbelt Software

See ad page **2**

- Increasing Performance in Enterprise Antimalware Software
- The Case for Third-Party Archiving in Exchange 2010
- Should You Install Messaging Security Software on Your Exchange Server?

ESET

See ad page **4**

- ESET NOD32 Antivirus 4 Trial
- Pocket E-Guide: How to Prevent Rogue Antivirus Programs in the Enterprise
- Conficker by the Numbers

Imperva, Inc.

See ad page **8**

- Cutting the Cost of Application Security: An ROI White Paper
- Next Generation Web Application Firewalls (NG-WAF) | White Paper
- What is a Web Application Firewall?

M86 Security

See ad page **11**

- Closing the Window of Vulnerability in Today's Web Environment
- Web Exploits: There's an App for That
- Fight Malware Threats in Real Time with the M86 Secure Web Gateway

---