WHITE PAPER: WEB SECURITY

The Tangled Web:

Silent Threats & Invisible Enemies

Symantec.cloud

White Paper: Web Security

The Tangled Web:

Silent Threats & Invisible Enemies

Contents

The Secret War

In the not so distant past, businesses used a simple technique to avoid computer viruses or malware: they cautioned their employees to "not-click" on dubious-looking email attachments. Those days are long gone. Today companies face network threats that are often unseen, narrowly targeted and much more difficult to detect.

Anonymity, deceit and subterfuge are now well-established weapons in the arsenal of cyber-criminals. These criminals target organizations with a variety of covert malware, spam and scams that drain employee productivity, steal sensitive data and negatively impact the corporate brand.

Techniques such as the use of rich media (flash and streaming content), open-source platforms, Web 2.0 collaboration tools, social-networking sites and highly available criminal "toolkits" are deployed to infiltrate corporate networks.

One widely used tactic is the delivery of malware through weblinks to compromised websites embedded in email attachments. When these links are followed by the user, malware is installed to their system and their network security is compromised. This mode of entry is proving to be a more efficient (and ultimately more lucrative) way for criminals to infiltrate corporate networks and bypass traditional scanners.

As users are being victimized by these Web-borne threats, they aren't aware that it is happening, usually because they simply visited a harmless-looking website. In a 2010 report, MessageLabs Intelligence indentified malicious web threats on 42,926 distinct domains, the majority of which were compromised, legitimate domains.[1]

This Symantec.cloud white paper focuses on the emergence of covert information theft as a key tactic of malware propagators. Most importantly, the paper highlights the crucial danger points for any business that doesn't defend itself against viruses which operate in the background.

Spyware

Perhaps the best-known undercover threat is spyware, which first appeared in 2005. Spyware is software that infiltrates a computer's hard drive without the user's knowledge.

Spyware usually gains access to a computer by camouflaging itself among other software (e.g. a free screen saver or a music file) which the user has agreed to download. Ironically, spyware is often concealed in downloadable software claimed to be "spyware-free" or "adware-free"—and even in many "anti-spyware" applications.

Once installed, the spyware secretly tracks the user's Web-browsing and website-visiting behavior, and then passes this information on to advertisers. The user's computer then finds itself deluged with pop-up advertisements related to their browsing behavior. All the while, the user remains oblivious to the fact that their machine has been infected.

"Spyware continues to be both a security and a system-management nightmare," says IDC Security Analyst, Brian Burke. "Theft of confidential information, loss of productivity, consumption of large amounts of bandwidth, corruption of desktops, and a spike in the number of help-desk calls related to spyware are overwhelming many IT departments."[2]

1-MessageLabs Intelligence: 2010 Annual Report
2-eWeek Security Watch, http://securitywatch.eweek.com/virus_and_spyware/idc_-_webborne_threats_rise_saas_follows.html, April 2009

Botnets

A robot network, or "botnet," is a network of computers that are infected with a malicious program that lets cyber-criminals control the machines remotely without the users' knowledge.

Typically, computers are "recruited" to botnets when users innocently click on an infected Web link or an email attachment containing a virus. Though nothing seems to happen, a malware program secretly downloads itself to the computer's hard drive. This enables the botnet controller or "herder"—often a member of an international criminal gang—to take control of the computer whenever they please.[4]

Using sophisticated malware, botnet gangs can easily breach corporate defenses and compromise business-based computers. Affected companies see corporate bandwidth over utilized and their networks operating sluggishly.They also find themselves helplessly involved in spamming and illegal activities that afflict Internet users worldwide. Infected machines may fall prey to threats that leak confidential, business-critical data, which can erode a company's competitive edge.[5]

"Botnets are a powerful tool for hackers. They can be used to send spam, harvest data and conduct distributed -enial-of-services attacks against websites. And the malicious software infecting PCs that are part of botnets is continuously being developed for other evil purposes."[3]

Jeremy Kirk, Computerworld.com

How do botnet owners earn money from infected computers? There are many ways for a botnet to perform multiple, simultaneous attacks such as: distributed denial of service (DDoS) attacks, spam, spim (phony communications that appear during instant messaging and steal IM user names), phishing, SEO spam, click fraud and distribution of adware and malicious programs. Any of these tactics can bring a cyber-criminal confidential data or allow them to offer criminal services that can be sold in the underground economy for big bucks.

Phishing

Phishing email messages—as well as variations called "pharming" or "whaling"—are schemes that trick people into sending money or providing personal information (e.g., name, address, user names, passwords, credit card details) that will be used for identity theft. A cyber-criminal who sends emails that contain authentic information about the user or their company greatly increases the odds of getting a "bite."

Phishing reels in unsuspecting users when a hacker sends an e-mail with an embedded Weblink inside and an invitation to go to a Website which the thief portrays as a well-known or trustworthy site.

Legitimate businesses that have been online for many years are often targeted for phishing attacks. By taking control of companies' domain name service (DNS) database records, phishers take advantage of the good reputation of these domains.[6]

The number of phishing scams is on the rise.They adversely affect businesses of all types including retail establishments, banks and other financial institutions, U.S. courts, the U.S. Internal Revenue Service (IRS), the U.S. Federal Bureau of Investigation (FBI) and other government agencies.

3-Computerworld, http://www.computerworld.com/s/article/9139787/Botnets_contributing_more_than_ever_to_click_fraud, October 2009.
4-MessageLabs Intelligence, "The Botnet Threat: Targeting Your Business,http://www.messagelabs.com/intelligence.aspx.
5-Ibid
6-MessageLabs Intelligence, "New Web Threats in 2009," http://www.messagelabs.com/intelligence.aspx.

"Some 5 million U.S. adults over the age of 18 lost money to phishing during the 12 months ending in September 2008, representing a 39.8% increase over the number of victims a year before, according to a recent Gartner survey. Many security measures implemented to stem phishing are not yet adopted widely enough to reverse this tide, and their effectiveness is partial, the degree of which depends on the solution."[7]

Social Networking

Social networking sites, once considered to be strictly consumer applications, are now thriving in the corporate environment. Companies rely on social networking to spread the word about their businesses, community events they sponsor and worthy causes they support. Corporate executives run blog postings on social media sites to voice their opinions or describe why their products are the best on the market.

Cyber-criminals use social media websites for a very different reason. These sites give them a new, effective way to infect corporate users' computers with malware. One popular approach is to create a fake profile on a social media website and use it to post malicious links that "phish" for corporate users.

In this form of phishing, spammers post blog comments on other members' pages; obtain the unsuspecting members' account information; then send messages from the phished accounts to other contacts. These messages distribute spam, including links to fake websites such as online pharmacies, casinos, financial-services firms and phony online colleges that offer worthless degrees.

"Corporations that effectively deploy social media will enjoy a significant competitve advantage. Still, questions remain about how to securely incorporate social media applications into the enterprise."

Brian E. Burke, Program Director
Security Products, IDC

Organizations must balance the business value of social media websites with the risks of many non-secure social media environments. The advances in Web 2.0 technologies demand a new generation of Web-security tools that go well beyond traditional URL filtering.[1] A 2009 IDC report states, "Corporations that effectively deploy social media will enjoy a significant competitive advantage. Still, questions remain about how to securely incorporate social media applications into the enterprise."[8]

Converged Threats

A converged threat consists of a combination of viruses, spyware, phishing, spam and other methods of attack that can disrupt networks or lead to theft of sensitive information. Converged threats don't come from a single mode of delivery—they can come from email, Web, instant messaging and even voice-over IP applications and environments.

An obvious solution to converged threats is to sever all ties with the Internet— disallowing employee Internet access reduces exposure to threat and attack. But since companies can't function without Internet access, the connection to the digital world must be maintained and protected.

Proper protection for converged threats includes maintaining a global awareness of the threat landscape from moment to moment; an ability to block or avoid potential threats; and quick reactions to new threats. Using proactive technologies to evaluate potential threats and block dangerous behaviors is important for managing a threat landscape in real time.

7-The War on Phishing is Far From Over; April 2 2009, Avival Litan, Gartner, Inc.
8-Ibid

The Anatomy of an Attack

A cyber-criminal conceals malware inside a website to take control of a user's computer without them knowing it. Once this has been achieved, the ways in which criminals can exploit the infected computer and its unfortunate owner are nearly unlimited. Any Web-based attack is comprised of three key components: the set-up, the hit and the aftermath.

The Set-Up

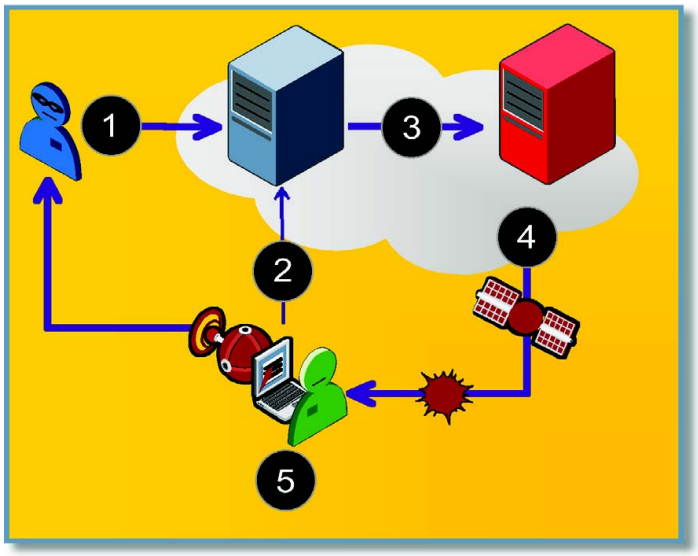
After the attacker chooses the reason for gaining access to users' computers (e.g., to steal sensitive data; to track browsing habits; or to recruit the machine to a botnet), they obtain the malware that they want to employ in the scam and place it on the Internet, often on an authentic, newly registered domain.

The Hit

Next, the attacker entices potential victims to download the malware. For this to happen, the victim must visit the infected website. They might arrive there during their normal Web browsing or be led there by phony advertisements, links in spam emails, instant messages, social networking sites, blogs or malicious links that appear on search-engine results.

In many cases, the victim is then lured into taking an action to unwittingly download the malware. These include a "click here to install" button; a "you're infected—click here to remove the virus" pop-up alert; or malicious files in areas where the victim intends to download music, software or movies.

In other instances, no action by the user is required for the malware to download itself. One example of this is a "drive-by download" in which a concealed malware program automatically installs itself on a computer simply because the user visited an infected website.



1. Hacker inserts malicious URL.
2. User visits good website.
3. User re-directed to bad website.
4. Bad website sends obfuscated exploit for vulnerability on user's system.
5. Malware is installed without the user noticing.

The Aftermath

Once the malware has installed itself on the victim's machine, it performs the tasks for which it was designed. This could happen immediately or the malware may lay dormant, ready to be activated later in response to commands sent by the cyber-criminal.

When it begins its misdeeds, the downloaded program can collect personal data, open ports that allow the attacker further access to the infected computer, change registry values, edit and/or move files, or modify settings for email, Web browser and other software.

These actions open up a range of options for the attacker. They can hold the victim hostage by locking them out of their own computer and demanding cash for a password to unlock it. They can recruit the computer to a botnet and command it to send spam, steal credit-card data or perform distributed-denial-of-service attacks. Or they can edit files so that when users visit frequently browsed Web pages they are redirected to malware-distributing websites.

Whatever the covert tactic used by cyber-criminals, the end result is the same—the user and the company they work for endure hardship in the form of security breaches, reduced productivity and loss of income.

The Advantages of the Cloud Security Model

According to Osterman Research, using on-premise Web security solutions means high costs for infrastructure, high labor costs for managing the security system and many hours of training for IT staff. Also, bandwidth is consumed by the requirements of the system and employee confidence in on-premise solutions is low.[9] A cloud Web security service, however, can provide a number of advantages for organizations of all sizes.[10]

Reduced Management Costs — Companies often underestimate the amount of labor required to manage an on-premise security system. Using an off-site cloud based service allows IT staff to generate more value for their organization by performing business-related tasks instead of managing the system.

Less Complexity and Uncertainty — A cloud solution can reduce the complexity and uncertainty caused by new threats and growing volumes of spam and spyware. Because cloud providers handle these problems and have a greater set of capabilities than most companies can maintain in-house, cloud services clients are better insulated from the growing array of attacks launched against them.

"A cloudd web security service can offer a number of advantages for organizations of all sizes."
Osterman Research

Maximum Levels of Protection — A cloud solutions provider can provide the highest levels of protection against malware because the provider updates its capabilities on a near-real-time basis and deploys a broad range of technologies. A cloud provider uses multiple anti-virus scanners and URL filters and can invest more resources into its infrastructure than most client companies can.

Using a Single Source — Deploying an assortment of solutions from different vendors is more expensive than using a single vendor's solution with the same capabilities. Also, managing multiple vendor solutions and relationships with several vendors is more cumbersome and time-consuming than a relationship with a single vendor with centralized management tools and support.

9-Osterman Research, Inc., "The Advantages of a Hosted Security Model " April 2008.
10-Ibid

Symantec MessageLabs Web Security.cloud Service

The Symantec MessageLabs Web Security.cloud solution operates at the Internet level to intercept Web-borne viruses, spyware and phishing threats. The service controls Web traffic through URL filtering, which enables companies to enforce Web and email Acceptable-Use Policies.

Symantec.cloud uses multiple signature-scanning engines plus proprietary Skeptic™ technology to provide 100% protection from sophisticated and targeted Web-based threats.

Web Security.cloud is delivered through a global infrastructure and include 24/7/365 customer support. The service is designed to meet the needs of small-to-medium sized businesses as well as large corporations and it works seamlessly with Symantec.cloud's Email Security and Email Encryption solutions.

To learn more about the Web Security.cloud service, please visit us at **http://www.messagelabs.com.**

More Information

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +44 (0)870 850 3014

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

About Symantec.cloud

Symantec.cloud uses the power of cloud computing to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging. Building on the foundation of MessageLabs market leading software-as-a-service (SaaS) offerings and proven Symantec technologies, Symantec.cloud provides essential protection while virtually eliminating the need to manage hardware and software on site.

More than ten million end users at more than 31,000 organizations ranging from small businesses to the Fortune 500 use Symantec.cloud to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging.

Symantec.cloud helps IT executives to protect information more completely, manage technology more effectively, and rapidly respond to the needs of their business.

For specific country offices and contact numbers, please visit our website.

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.MessageLabs.com

Symantec helps organizations secure and manage their information-driven world with **managed services**, **exchange spam filter**, **managed security services**, and **email antivirus**.

1/2011 21167350