WHITE PAPER: WEB SECURITY

Next Generation of Web Exploits

When Good Sites Go Bad

Symantec.cloud

White Paper: Web Security

Next Generation of Web Exploits

When Good Sites Go Bad

Contents

Introduction

Rapid developments in enterprise information technology, web-enabled applications, and mobile communications have introduced productivity gains that have enabled many organizations to do far more with fewer resources than ever before. While these are overwhelmingly positive outcomes that have generated tremendous economic value, these developments have also introduced complexity and new opportunities for cyber-criminals to penetrate enterprise systems to wreak havoc.

In many – perhaps most – cases the damage that is done by malware developers is not immediately observed. Malware can lurk like a predator waiting for an opportunity to inflict maximum damage on its victims. These new trends have redefined the nature of threats, attacks and vulnerabilities, which in turn is prompting organizations to revisit their cyber-security strategies.

Many organizations are consequently coming to the conclusion that the traditional approach of purchasing discrete point solutions for anti-virus, firewall, patch-management and other tools to protect the organization is inadequate to meet the challenges posed by the new threat landscape. The reasons for this conclusion:

- **New threats tend to be blended in nature.** Cybercriminals are now leveraging multiple "threat vectors" – the paths or tools used to attack their targets. Whereas malware attacks in the past may have been limited to a single assault on email systems, for instance, today cyber-criminals are integrating spam, phishing sites, and even reputable sites that have been compromised, to penetrate and exploit enterprise systems.
- **Point solutions can affect system performance.** In response to the increasingly sophisticated nature of threats to which organizations are exposed, more and more protective code must be pushed out to endpoints, placing a burden on enterprise systems that is negatively affecting performance.

A new and innovative alternative to traditional on-premise point solutions are "hosted" solutions from security application providers that intercept malware before it even affects a protected end-point or server. Hosted security services, also known as Software-as-a-Service (SaaS), allow multiple customers to use the same application hosted in the cloud on a shared infrastructure. This is an approach to computer security that is catching the attention of companies of all sizes, as they seek ways to address complex multi-vector attacks while mitigating the performance overhead that premise-based security places on enterprise systems.

This strategy has been deployed effectively by Symantec.cloud, which uses the power of SaaS to provide essential protection while virtually eliminating the need to manage hardware and software on site. In this report, we examine the new nature of threats, vulnerabilities and attacks, and explore the role that hosted security strategies can play in managing core risks to organizations of all sizes and across all industries.

Understanding the New Professional Enemy

Once considered a game among hackers who sought notoriety in highly public disruptions of computer systems, malware development is today a big business that is driven by international organized crime who pockets billions of dollars every

year from unsuspecting individuals and organizations. Many of these players are also involved in serious efforts to infiltrate networks for espionage and cyber-terrorism.

As technology continues to evolve, attacks have become more sophisticated and targeted. Malware today is often well disguised, hiding behind fake websites – or even legitimate environments that have been compromised. According to industry analysts, approximately 4,000 new, legitimate websites per day are tricked into hosting malware. It is not surprising that as a result, 65 percent of all adults have been victims to a cybercrime. In a study by Norton and StrategyOne that surveyed 7,000 Internet users in 14 countries.[1]

- Half of respondents reported they had been victims of viruses or malware.
- Ten percent said they had been involved inadvertently in online scams.
- Nine percent were tricked by phishing sites.
- Seven percent had their social networking profile hacked.

In short, it is getting difficult to distinguish between legitimate and corrupt sites. While some criminals are, in fact, creating new websites for the sole purpose of serving up malware, the bigger threat to enterprises comes from established and reputable websites that have been compromised and are serving up malware without their knowledge.

Enterprise users therefore are more likely to encounter a malicious web page by going about their normal business looking for work related content than they are to be infected or attacked by going to disreputable websites. Indeed, 2009 analysis from Symantec.cloud and MessageLabs Intelligence found that more than 80 percent of malicious web attacks take place via legitimate, compromised sites.[2] In early 2010, some 49 websites of Republican and Democratic lawmakers were hacked after President Barack Obama's State of the Union address.[2]

In this environment, deploying a disconnected set of point solutions to protect email, web-surfing, instant messaging, and other communications tools that have emerged in the enterprise seems archaic. Traditional single point anti-virus scanning systems are based on signatures that look for certain codes that had already hit their peers. Today, organizations are more likely to be subject to more targeted attacks that are less likely to be detected. Many criminals are realizing that mass attacks don't pay off and they're willing to put the time into writing a customized piece of malware that is specifically targeted to go after a select group of companies or individuals. The ultimate aim of a targeted attack is to gain access to sensitive data or internal systems. During a six-month period in 2010, Symantec tracked an average about 73 targeted attacks each day, a staggering number given the amount of customized malware that's necessary for this. These numbers come one year after Symantec detected 2.9 million zero-day attacks in 2010.

Any organization that possesses sensitive and valuable data can be an attractive target. The danger of targeted attacks is the stealth deployment of malicious code on the recipient's computer, often hidden within legitimate-looking documents such as .PDF, .DOC, .XLS and .PPT files. The recipient only has to open the attachment and the computer is compromised.

In addition to targeted attacks, cybercriminals are increasingly infiltrating the fastest growing online and mobile channels. For example, sites like Twitter and Google serve up a tremendously high number of malicious links. In July 2010, an IT security company performed a study across Bing, Google, Twitter and Yahoo over a two-month period, reviewing some

1-http://www.symantec.com/about/news/release/article.jsp?prid=20100908_01
2-http://thehill.com/homenews/house/78523-house-investigates-website-hackings

25,000 trending topics and nearly 5.5 million search results. Researchers found that Google served up twice the amount of malware as Bing, Twitter and Yahoo combined.[3]

To further complicate matters, a growing number of enterprise users are accessing social media and web 2.0 applications – such as widgets, wikis, Twitter and Facebook – at work. In some cases, these are sanctioned activities. In others, they may not be allowed. In 2010, Twitter sent out warnings to its users that "a malicious link is making the rounds that will post a tweet to your account when clicked on." This exploit followed an earlier attack, which included a cross-site scripting (XSS) vulnerability that allowed several XSS worms to spread throughout the site.[4]

The end result is that most organizations are operating in an environment that is very difficult for IT to monitor so that they can ensure endpoints are fully protected. Consequently:

- The environment to secure has become more complex;
- The points of attack have become more numerous; and
- The ingenuity of malware developers is growing more sophisticated.

Symantec.Cloud Services

In response to these trends, Symantec.cloud offers a comprehensive security and management solution comprised of a variety of integrated components, including:

- Symantec Endpoint Protection.cloud
- Symantec MessageLabs Web Security.cloud
- Symantec MessageLabs Email Security.cloud
- Symantec MessageLabs Instant Messaging Security.cloud

Symantec.cloud uses the power of cloud computing to provide essential protection while virtually eliminating the need to manage hardware and software on-site. The solution is particularly appealing for managing an organization's evolving and growing distributed workforce because it provides comprehensive, reliable coverage for email, Web, IM and endpoints like laptops and servers, but does not require expensive on-premise equipment, complex management or extensive expertise. Employing Symantec Endpoint Protection.cloud on your devices means regular, accurate scanning for active infections.

Regular scans and real-time monitoring in combination with enforcing an acceptable usage policy with the help of Symantec.cloud solutions means organizations will be protected from threats lurking in various Internet sites that employees visit, the URLs they click on, the emails and IMs they receive and send, or executables and downloads they activate.

Doing this on a dedicated basis at the physical device level cannot only be complicated and expensive, but can also introduce network latency and hamper processing performance. Symantec.cloud solution, by contrast, offers a service level agreement (SLA) guarantee that scanning and filtering of Web data will not exceed 100 milliseconds in our environment. Actual scanning performance is typically half of this time.

3-http://www.barracudalabs.com/wordpress/index.php/2010/07/28/barracuda-labs-2010-midyear-security-report/
4-http://www.informationweek.com/news/storage/disaster_recovery/showArticle.jhtml?articleID=227500862&queryText=twitter%20exploits

How Cloud Services Work

Symantec.cloud uses three scanning engines in its web scanning infrastructure. It utilizes the two best commercial antivirus scanning engines and it uses an engine called Skeptic™ heuristic engine, a proprietary Symantec.cloud technology that has been in development over the past 10 years. Skeptic scans and analyzes emails, web requests and instant messages for potential malware threats. It looks for unknown malware variants so the data it sees is scored against a variety of factors and rule sets that have been in development for over a decade. Once a new threat is identified, it is blocked and a signature is created which is shared, in real-time, with the other protocols being scanned by Skeptic.

The Skeptic engine was critical to the company's success earlier this year in combating the email-borne 'Here You Have' Imsolk worm that struck many large enterprises, including NASA and Walt Disney Co. When this malware infected a single computer, the worm attempted to disable the local security software, while propagating throughout the enterprise and to all known contacts in the victim's address book. The threat was hosted on the Web but propagation took place through email, IM, and mapped network drives.

The heuristic rule that triggered the detection of this virus by Skeptic was added in 2008, two years previous to the attack. The mass mailer worm was detected first in email using Skeptic's heuristics and was blocked before it reached our clients networks. Information on the threat was shared in real-time with the Symantec MessageLabs Web Security.cloud and Symantec MessageLabs Instant Messaging Security.cloud security services. If a customer only had MessageLabs Web Security services, they were still protected from the threat. At the peak of the "Here You Have" attack, Symantec.cloud was blocking over 2,000 malicious emails per minute. In total, 106,390 copies were blocked.[5]

Conclusion

The cyber-security profession is a cross-roads. Just as colleagues in other parts of the IT organization are exploring the pros and cons of cloud computing to address cost, go-to-market and governance challenges, the security profession must evaluate new ways to address the sky-rocketing complexity and scope of today's threats to enterprise systems.

Traditional approaches to defending against today's threats are neither scalable nor integrated enough to effectively manage the risk exposure that organizations must more effectively address. Symantec.cloud solutions represent an alternative to traditional security measures that can scale up to thwart the complex nature of today's attacks while rationalizing the cost structure needed to respond to today's threats.

5-

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