Security from Above:
How Cloud-based Security Delivers Up-to-the-Minute Network Protection

February 2010

THE NEED TO RECONSIDER SECURITY APPROACHES

The convergence of numerous trends is causing organizations to reconsider their approach to security. While widespread email viruses and worms have decreased, attacks via the web are on the rise. This is because web browsers consolidate many applications — including those used for email, instant messaging, and ecommerce — making the browser an attractive launch pad for attacks.

Web 2.0 and other complex web technologies also open the door to new two-stage web attacks and social-engineering exploits.[1] In fact, during the first quarter of 2009, Web 2.0 services and sites led with the highest number of all recorded hacking incidents at 21%.[2] These new methods of attack are particularly dangerous, because they can originate from trusted sources or become embedded within legitimate and authorized email and web content.

Two factors are driving the further growth of web-based malware threats. First, is that cybercriminals are financially motivated to spread malware and acquire web users' personal data. And they have the means to do so. Due to the proliferation of Web 2.0 and the dramatic progression of spam from plain text emails to the use of sophisticated and malicious social-engineering tactics, spammers can now readily infect devices used by unsuspecting victims. By using email as the invitation to web-based infections, spammers can easily locate and entice victims, and expose them to infections via botnets, spyware, malware, and blended threats that can then manage and further exploit the infection. All it takes is one malicious email,

[1] The Register, *Adobe Flash attack vector exploits insecure web design*, November 13, 2009 http://www.theregister.co.uk/2009/11/13/adobe_flash_wallop/

[2] Secure Enterprise 2.0 Forum, *Web 2.0 Hacking Incidents on the Rise in Q1 2009*, May 5, 2009 http://www.secure-enterprise20.org/node/39

one click of an employee's mouse and an organization's business and network are at risk for security breaches, regulatory violations, or theft of confidential information – or even an intrusion that turns the network into a source of Internet threats to infect other networks.

Second, cybercriminals can automate web-based attacks. Through modified packing and crypting techniques, and other obfuscation methods, attackers can now create thousands of new variants of the same threat with little effort. And because botnets now take advantage of new techniques such as Fast Flux DNS to create dynamic domains, malware sites can stay active for weeks or months at a time.

Moreover, the growth in the web itself enables those with malicious intent to launch attacks that reach a broader range of users via a growing number of attack vectors. Leading anti-virus technology provider, Kaspersky Lab, discovered over 33.9 million unique instances of malware in 2009, with more than 15 million new malware instances in the same period.[3] This coincides with massive growth in the number of registered domains, which according to VeriSign, reached 184 million in September 2009.[4] The number of attack source points is actually much larger when one considers Web 2.0 and the web-based features it delivers to social networking and media sites, such as user-generated content, dynamic content, and mashups.

How can organizations address the expanding threat landscape while maintaining a reasonable cost of security? Preventing users from tapping into the web's wealth of resources is an unrealistic strategy. Most organizations are not willing to sacrifice the productivity and marketing gains they realize from allowing their people to interact through leading web sites. Searches on Google, web-based instant messaging sites such as Meebo or MSN Messenger, and social networking sites like Facebook simply offer too much value to ignore.

To stay productive while fending off the growing number of threats, many organizations are leveraging cloud-based security solutions, including a new generation of reputation services, to strengthen their security posture. They view cloud-based security as the only practical means of keeping pace with the ever-changing threat landscape without over-burdening their IT budgets. This paper will describe the evolution of cloud-based security, focusing in particular on next-generation reputation services and their impact on organizations' security success within today's expanding threat landscape.

EARLIER REPUTATION SERVICES CAN'T KEEP PACE

Since the 1990s, reputation services have been helping organizations block unwanted or bad traffic to ensure that threats never enter the network. By identifying and blocking threats at the perimeter, reputation services help prevent attacks, reduce the on-premise IT footprint required to scan traffic, and lower the costs associated with the bandwidth, hardware, and other resources required to block threats. As web technologies and the web itself have grown more sophisticated, early generation reputation services have become less effective in identifying and blocking threats. To fully understand this loss of effectiveness, it's important to understand how these services have evolved.

Early reputation services relied solely on DNS blacklists (DNSBL) of known spammer IPs, blocking traffic originating from those IPs. As malware began infecting legitimate domains, reputation services could not distinguish between spammer domains and legitimate domains that were spamming as the result of malware infections. This meant DNSBLs only addressed 50-80% of the problem IPs.

---

[3] Kaspersky Lab, "Cyberthreat Landscape 2009: Outcomes, Trends and Forecasts", Moscow, January 28, 2010
[4] VeriSign, *The Domain Name Industry Brief*, December 2009 http://www.verisign.com/domain-name-services/domain-information-center/industry-brief/

Most current reputation services analyze IP volume in conjunction with DNSBLs to gain further context around each IP address. While this boosted effectiveness, the development of botnets and dynamic IPs still rendered these reputation services only 70-80% effective — far too low for enterprise security standards.

Leaders in the reputation services industry recognized that their reliance on historical information as their only source of malware data would soon make them obsolete. To address the dynamically changing web threats faced by millions of organizations, leading providers are making acquisitions that will enable them to offer next-generation reputation services.

Early reputation services that rely on DNSBL's are akin to credit bureaus – they can only monitor the historically known, unwanted traffic.

As shown in Figure 1, next-generation reputation services provide a superior level of protection by combining DNSBL and volume analysis with content inspection, behavioral analysis, and feedback loops to detect and block malware, spyware, and malicious code before users ever see them. This proactive approach makes these next-generation reputation services 99.9% accurate, with a significantly more effective catch rate greater than 98% — enabling them to offer vastly greater security than that offered by early generation or current services. By identifying and addressing threats proactively, these services offer greater defense at the perimeter.

Figure 1: *Cloud-based security offers superior protection against attacks and threats. Early generation services act like a basic passport scan that considers only historical data. Most current reputation services can be likened to airport metal detectors which provide limited visibility into threats attempting to enter. Next-generation reputation services provide comprehensive scanning of those attempting to gain access, much like airport bio-thermal body x-ray scanners.*

CLOUD-BASED SECURITY LEVERAGES NEXT-GENERATION TECHNOLOGY

Next-generation reputation services are delivered from the cloud to provide greater levels of email and web security. Unlike many loosely termed "cloud applications" that are mere extensions or a re-naming of existing applications into cloud terminology, next-generation reputation services actually optimize their services *through the cloud*.

Anonymous, statistical data from participating customers' security devices, third-party DNSBLs, and reputation databases are fed to the cloud. Next-generation reputation services aggregate, analyze, and act upon this data — while identifying new threats in real time — to deliver unprecedented levels of security that no individual organization could deliver on its own. The cloud security service provider then

streams these threat updates across its network and customers' networks in real-time to ensure dynamic protection. This is the promise of cloud-based security – extending protection by aggregating real-time monitoring intelligence from thousands of global systems.

Next-generation reputation services incorporate numerous algorithms and techniques to combine historical information that exists within the cloud (for example, data on spammers and categorized web sites) with adaptive identification techniques and behavioral analysis. They analyze the behavior of every incoming message through several automated operations:

- Examining embedded links
- Inspecting headers and content
- Applying malware, spyware, crimeware, and spam signature scanning
- Performing URL filtering
- Behavior patterns of the connecting IP

As a result, they are able to determine the reputation and risk level of email and web traffic attempting to enter a customer's network. With nearly 100% accuracy, threats – including denial-of-service attacks and spammer probing – are vaporized at the connection level, reducing the burden on local appliances. Just as important, cloud-based security services can scale to support explosive traffic growth across the web.

CLOUD-BASED SECURITY IN ACTION

To fully appreciate the robust nature of next-generation reputation services, let's examine below the step-by-step process that occurs at a geographically dispersed organization when an email connection is made to the network from a non-trusted IP address (or from a compromised email).

Message traffic from email and the web arrive at the network perimeter from the Internet. The reputation service inspects all the traffic, ready to block all unwanted traffic at the connection level as a powerful first line of defense. All clean traffic is allowed into the network for processing and routing by a customer's point security solutions. If the customer's security appliance discovers any additional threats or spam as it examines content, sender information, and context, the content is blocked. The appliance then reports the discovery back to the reputation service, which in turn streams the feeds across the entire network.

The reputation service analyzes the data and generates a result that depends, in order of priority, on the reputation for that specific sender at that IP address, for the domain originating from that IP address, and the reputation of the IP address itself. The service then returns a reputation score to the security device. Depending upon the threshold configured by the customer, the email security device can either allow or reject the connection.

Other customer appliances in the network can "ask" the cloud about new threats from connecting IPs before they analyze them locally. This approach means that local appliances will process less data, so that email and web traffic is transferred quickly and bandwidth capacity remains high.

Since the reputation score is critical to the acceptance or rejection of the email, next-generation services place a tremendous emphasis on getting the score right. They can collect information from over a billion sources, including port 443 connections from web, email, and network devices; third-party synchronizations, such as spamhaus and SORBS (Spam and Open Relay Blocking System); and honeypot domains, to name a few.

All this enables the superior catch rate that isn't possible with early generation reputation services.

WHY THE CATCH RATE MATTERS

Consider an organization that receives one million emails per month. DNS Blacklisting would eliminate approximately 50-80% of unwanted messages. This leaves upwards of 250,000 unwanted messages entering the network. Even if a reputation service considers IP traffic volume data, the 70-80% catch rate would still let up to 150,000 unwanted messages slip through the perimeter.

A next-generation service – with a more than 98% catch rate – allows only 17,000 messages to enter the network for further in-depth inspection, resulting in a significant increase in threat protection and cost savings.

Bringing Cloud-based Security Concerns Down to Earth

With cloud-based computing services, organizations have to share sensitive data with third-party providers, such as those offering SaaS. With next-generation cloud-based security, devices only share anonymous data about malicious traffic – no sensitive data is exposed.

BENEFITS OF CLOUD-BASED SECURITY

Next-generation reputation services are exponentially more effective than early generation services and help customers make the most of their existing security appliances. In doing so, they provide organizations with four major benefits:

- ***Faster, more dynamic security***: By aggregating millions of pieces of information from around the globe in real time, cloud-based security offerings provide an up-to-the-minute picture of threats and the ability to stop them.
- ***Less processing on local devices***: Cloud-based services analyze spam, offloading local devices of intensive processing and bandwidth consumption so they can focus on new threats.
- ***Automatic updates***: Because cloud-based services push updates out via the cloud and propagate them to customer premise equipment, they eliminate the need for customers to manually download updates.
- ***Cross-community customer benefits***: Cloud-based services can detect patterns and geographically isolate threat sources to prevent them from impacting customer devices in other geographies.

WHY THE TIME IS RIGHT FOR CLOUD-BASED SECURITY

As more and more business occurs over the web, those with malicious intent are keeping pace and developing innovate ways to launch attacks. To date, companies have relied on reputation services to help thwart these attacks, but earlier reputation services are unable to provide sufficient protection in the face of today's complex threats.

Combining real-time threat data from local security appliances with cloud-based security intelligence offers the best possible option for complete attack management and prevention.

The ideal solution combines processing and analysis in the cloud with data provided by local devices and real-time monitoring intelligence from multiple global systems. This next-generation cloud-based service leverages proprietary algorithmics and advanced features to deliver the world's most effective reputation service, with a more than 98% catch rate. By offloading local email and web security appliances, the cloud-based service alleviates local devices of the need to process or archive unwanted traffic. This results in lower costs for network processing and bandwidth. And the benefits extend to all participating customers, since the cloud-based service can dynamically protect them from newly discovered threats in real time.

Combining real-time threat data from local security appliances and cloud-based security intelligence offers the best possible option for complete attack management and prevention.

NEXT STEPS

To see how a next-generation, cloud-based reputation service works – and to check your own domain or IP reputation – visit http://www.reputationauthority.org.

For more information on the powerful WatchGuard XCS family of email and web security products with built-in WatchGuard ReputationAuthority™, visit www.watchguard.com/xcs.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of extensible threat management (XTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest appliances – the WatchGuard XTM 8 Series and XTM 1050 – provide high performance and fully extensible, enterprise-grade security at an affordable price. WatchGuard extensible content security (XCS) appliances deliver comprehensive email and web traffic protection for security, privacy, and compliance. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.