CYREN

EXECUTIVE OVERVIEW

The CISO Series

Web Security at the Front Lines of Cyber Defense

Today's Internet threat space is very dynamic. Globally there are thousands of malevolent actors disseminating hundreds of millions of threats each day. Companies that are unprepared for these threats can suffer serious repercussions. The National Cyber Security Alliance has reported that roughly 60% of those companies go out of business within six months of a loss of data due to a security breach.

We are long past the days of innocuous script kiddies unleashing computer viruses just because they can. Today's actors represent well-funded cybercrime syndicates, hacktivist organizations, and even nation-states. Their intentions are to steal data that can be monetized, such as credit card data; disrupt the normal operations of businesses, utilities, and government agencies; and steal vital intellectual property such as product designs or business plans.

The web is the primary vector for these attacks. Even the most dangerous cybercriminals and hackers induce their targets through phishing emails, waterhole attacks, social media and "malvertising" (compromised web ads) to click on links that are malicious. At that point, malware is silently dropped onto the computer or mobile device, and this becomes the springboard into the organization's broader network.

Once an attacker has a foothold on a company's network, they know how to escalate their privileges and keep thier actions under the radar until the time is right to fulfill thier intended goals. Whether it is to steal information or commit financial fraud, they have free reign to do what they want—undetected until it's too late.

Every Organization Can Be a Target

Large organizations aren't the only ones at high risk. According to the Verizon 2013 Data Breach Investigations Report, 40% of the confirmed breaches investigated in 2012 were companies with fewer than 1,000 employees. Companies with fewer than 100 employees represent the single largest segment of breach victims.

"Small and medium-sized businesses (SMBs) are handicapped in defending themselves because they don't have the financial and technical resources to address the challenge," according to Charles Kolodgy, Research VP for Security Products at IDC.

Simply put, attackers see SMBs as low hanging fruit. Smaller companies may not have millions of records that can be monetized, but they do have payroll accounts, online banking and cash transfer systems, and customer records with personally identifiable information (PII). For a well skilled hacker, it's child's play to tap this information and siphon it out in order to drain bank accounts and completely disrupt business.

WHY WEB SECURITY?

- Internet threats are constantly evolving with the web being the primary attack vector
- Once malware gets a foothold on a network an attacker can gain free reign
- Mobile computing and BYOD complicate the security landscape
- Every organization is at risk, but especially SMBs that may lack technical and financial resources for information security
- Big Data analysis of current threats is the best approach to developing actionable intelligence
- Real-time intelligence primes existing security infrastructure to prevent attacks

Mobility, cloud computing, and user-owned devices (BYOD or bring-your-own-device) make it impossible to define the network perimeter.

Malware gives an attacker a foot in the door to launch his attack on a company's network. There are several ways to deliver malware to unsuspecting victims—all of which can easily catch a person off guard. The most common malware delivery methods include emails with malware attachments, drive-by downloads from compromised websites or malicious web ads, and malicious mobile apps.

Practically any worker unknowingly can unleash malware onto their company network. Anyone who reads email, surfs the web, or uses mobile apps on a smart phone is a potential target. That's why it's vitally important to protect end-user devices—whether company or end user owned—to stop malware.

Security Solutions Must Evolve to Keep Up

It's a real arms race in the battle to defend against the ever-increasing threat landscape. Traditional security solutions like firewalls, signature-based anti-virus, and blacklisting are largely ineffective against the sophisticated and stealthy techniques attackers use today. Consider that signature-based anti-virus and anti-malware solutions can lag behind new exploits by weeks, leaving systems quite vulnerable in the interim.

Security vendors today utilize Big Data systems to analyze tens of millions of data points about threats that emerge daily on the Internet. This kind of analysis provides the near real-time intelligence required to feed security defenses that can turn away threats before they ever get into a company's network.

"A dynamic sensor grid is required to effectively stay on top of a dynamic threat space," says IT security analyst Richard Stiennon. "Only with a massive collection and analysis capability can a solution get close to providing complete coverage."

An effective web security solution must include automated collection and analysis of new websites and web pages and ensure that they are accurately categorized. Threat intelligence must be updated and disseminated to security solutions in near real-time to ensure continuous enforcement of an organization's policies.

Expert researchers must be able to quickly discover and dissect the most sophisticated threats and evaluate executables for malicious behavior before they can infect the network. Importantly, a web security solution must be capable of protecting an organization's workers at all times, regardless of where they are or what device they are using.

CYREN at a Glance

Every day, CYREN analyzes more than 12 billion Internet transactions that pass through their GlobalView™ Cloud. This high volume of transactions ensures that CYREN has a near real-time and comprehensive view of what is happening on the Internet. The technology is able to discern the shifting patterns and behaviors—the DNA, if you will—of malicious code and activity, empowering CYREN web, email and anti-malware solutions to respond in-kind with proactive protection for users.

CYREN WebSecurity is an innovative cloud-based solution that empowers business of all sizes by protecting their end-users web activity—regardless of where they are and which device they use. Delivered through a global network of value-add partners, CYREN's web security solution is optimized for SMBs and because the security functions are delivered as-a-service, there is no equipment to buy, install, or maintain.

CYREN'S DIFFERENTIATORS

- CYREN's GlobalView Cloud engine enables the company to collect and analyze billions of transactions every day and CYREN's patented Recurrent Pattern Detection (RPD) technology detects and classifies all types of email-born threat patterns in real-time.
- The cloud platform is a force multiplier for SMBs; CYREN has the technical expertise to handle web and messaging security that SMBs have difficulty acquiring.
- With CYREN WebSecurity, branch offices, workers at home or on the road, and mobile device users all get the same protection and web browsing policy coverage as their colleagues connected to the company network.
- Delivered as-a-service through an extensive partner & reseller network, CYREN's solutions are easy to setup and customize.
- A company can define its own policies according to its specific security and compliance environment.

This Executive Overview is sponsored by CYREN. For more information on CYREN visit www.cyren.com