GATEPOINT RESEARCH

Beyond the Firewall: Protection & Performance

New Technologies Demand New, Flexible Approaches to Web Security

“The cyber black market has evolved from a varied landscape of discrete, ad hoc individuals into a network of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states.”[1]

the Rand Corporation

Contents

Threats to Web and network resources are increasingly sophisticated and costly. Potential sources of threats have dramatically increased as cyber crime has evolved into big business. The Ponemon Institute’s annual survey finds that in 2013 the average annualized cost of cyber crime was $11.6 million for the organizations it analyzed, up from $8.9 million the previous year.[2]

The threat environment is facilitated by burgeoning black markets where criminals and others can trade in ready made attack tools, swap information on techniques and strategies, and monetize information they have collected such as credit card account data and personally identifiable information.

Organizations face great risk from increasingly frequent and sophisticated attempts to render Web properties unavailable and steal intellectual property or personally identifiable information. Technology is becoming more sophisticated—bots and botnets are not only bigger, they're smarter, and are hiding their identities. In addition, attackers are adopting new tactics that take advantage of protocol vulnerabilities to amplify attacks utilizing fewer resources.

DDoS, Web application, and DNS infrastructure attacks represent some of the most critical threats to enterprises today. "Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders,"[3] says the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

DDoS attacks consume resources thus preventing or slowing authorized access to a system resource or dependent systems including Web sites, Web-based applications, and databases. By marshaling often-hijacked computers and servers, perpetrators are able to direct an overwhelming volume of requests at a target system, crippling its ability to respond to legitimate requests. Perpetrators are continually escalating the volume of their assaults and can routinely direct tens of gigabytes of network traffic at a target.

More insidiously, attacks may combine methods such as a network layer DDoS attack with simultaneous Web application layer and data center attacks, hoping to distract security teams with a volumetric assault that camouflages intrusion through other system vulnerabilities. "Often times a DDoS attack will mask an application intrusion attack or an attempt to steal or manipulate data," says Dan Shugrue, director of product marketing for security solutions with Akamai.

According to Verizon's annual Data Breach Investigations Report, in 61 percent of the Web attacks it investigated the perpetrators were able to discover vulnerabilities within seconds or minutes.[4] In 72 percent of the attacks, data exfiltration began within days. In 52 percent of those attacks, the victims didn't discover the attack for months, sometimes even years.

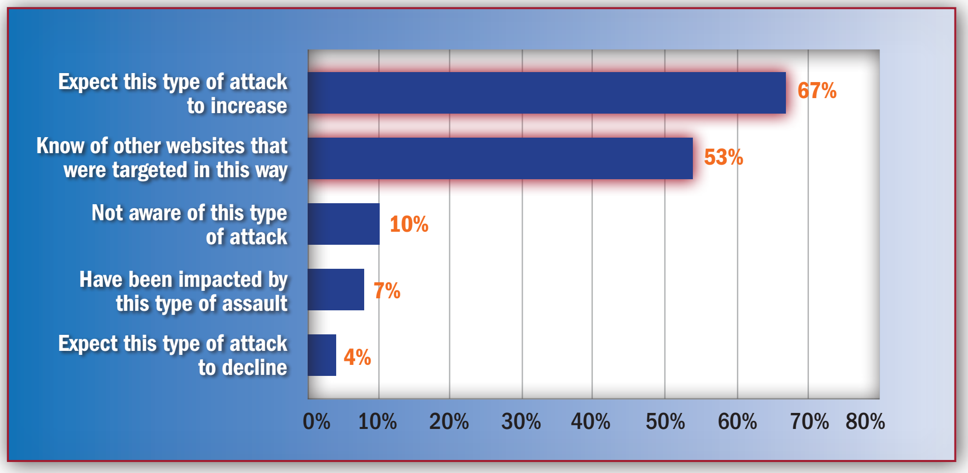
One reason attacks continue to increase in volume and sophistication is the knowledge sharing among attackers and the availability of tools to carry out such attacks. "Most of the attacks we are seeing now are executable even by people who don't necessarily know how to code or know much about network infrastructure," says Shugrue. Even novices can download an attack tool and type in a target URL to initiate an assault.

In an effort to determine how security executives perceive this new threat landscape, Akamai commissioned Gatepoint Research to survey senior IT security and operations decision makers on how they currently manage their organization's security posture, how they plan to deal with these new realities, and what impediments they perceive to their ability to meet these new demands.

Attack Concerns Escalate

Gatepoint's survey of more than 200 executives reveals that 67 percent of security executives expect an increase over the next three years in attacks that utilize a volumetric DDoS assault to bring down a firewall or distract security analysts, followed by an application layer attack to steal data. More than half say they are aware of other websites already experiencing this type of attack.

What is your view of converged attacks that utilize a volumetric DDoS attack to bring down a firewall or distract security analysts, followed by an application layer attack to steal data?



Those executives are worried about the implications of the growing threat. Not only that, they understand the implications: 95 percent expect attacks at the network and application layer to cause system downtime and damage to the brand and 89% indicate that attacks divert resources from business needs while 69 percent expect to lose data during Web attacks.

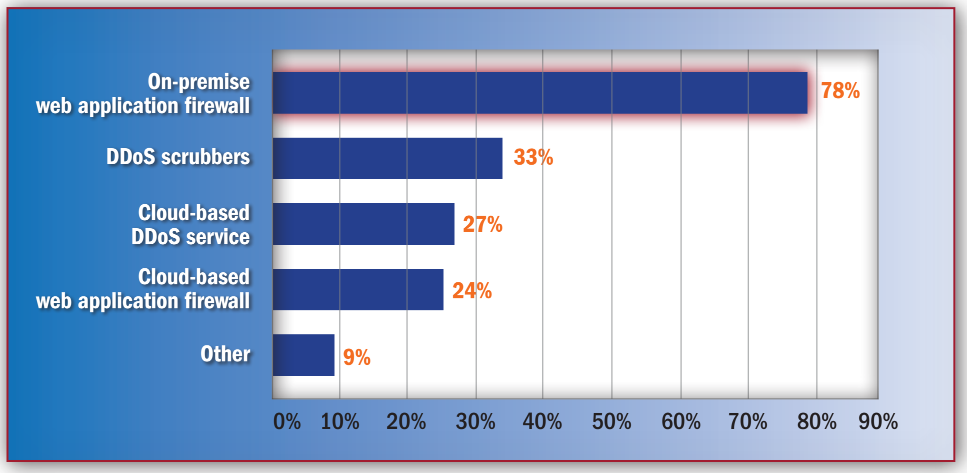
According to 75 percent of respondents, the most "pain" in the event of a successful attack is the disruptive impact on the organization's ability to meet its business goals and strategic objectives as well as the blocking of customer and partner access to Web sites. In addition to lost revenue, which 83 percent of those surveyed see as a key risk of attacks, the indirect costs may be staggering, ranging from actual costs of a data breach—such as regulatory fines, litigation, purchasing credit monitoring services for customers—to those that may be harder to measure though just as damaging, such as losing a customer and the indirect costs of brand damage.

Industry data shows that executive concern is more than justified. The number of DDoS attacks increased by 22 percent from 2012 to 2013, according to the Prolexic Q2 Quarterly DDoS Attack Report.[5] Those attacks may mask SQL injection and cross-site scripting attempts to attack a Web application or forward logic to a database in an effort to compromise the information stored within. Even a "minor" SQL injection attack on a single unsanitized field in a Web report cost one financial organization more than $196,000,[6] according to the NTT Innovation Institute.

Many Organizations Unprepared

A majority of survey respondents today utilize in-house only resources for security monitoring and remediation. The most common strategies incorporate firewalls, network appliances and/or intrusion protection solutions. On-premises firewalls, for which 78 percent of respondents rely on, may not hold up against volumetric DDoS attacks, while a distributed network architecture firewall service can scale automatically, on-demand, offering the capability to defend against massive-scale attack as they are unable to scale to counter the threat of massive attack.

Which security measures do you currently utilize?



Akamai's Shugrue says many organizations invest in Web application firewalls, but fail to regularly update their firewall rules or may not have even gotten around to fully deploying this defense. In other cases, he adds, information security teams attempt to counter growing application layer attacks by increasing the number of rules their on-premise Web application firewall processes on incoming requests; but with the volume of traffic that businesses experience, applying too many rules can sap server processing power so the defensive tactic may slow down Web sites.

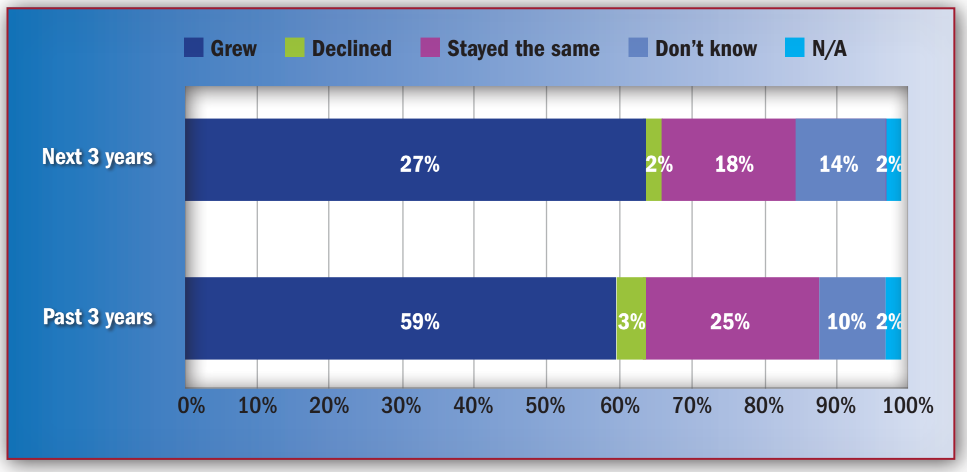
Addressing the Challenge

To scale to meet today's threats, homegrown defenses require additional capital and human resource expenditures to keep up with cyber criminals who are able to marshal the resources of rogue bots. One industry report found that 78 percent of organizations have just one or two staffers dedicated to application security.[7] A third of respondents in the Gatepoint Research survey say that staffing resources are insufficient to be able to improve their security posture and eliminate risk, while 17 percent say senior management at their companies does not believe the risk justifies the costs of investing in new Web security solutions and services. Organizations aren't sitting still in the face of these threats, though. Enterprises are devoting ever more dollars to their defenses. Most of the survey respondents indicate their security budgets have been growing and will continue to grow, with 59 percent citing an increase in security budgets over the past three years and 63 percent predicting growth over the coming three years. Just 2 percent indicate security budgets have decreased over the past three years and 3 percent anticipate a decline in the years ahead.

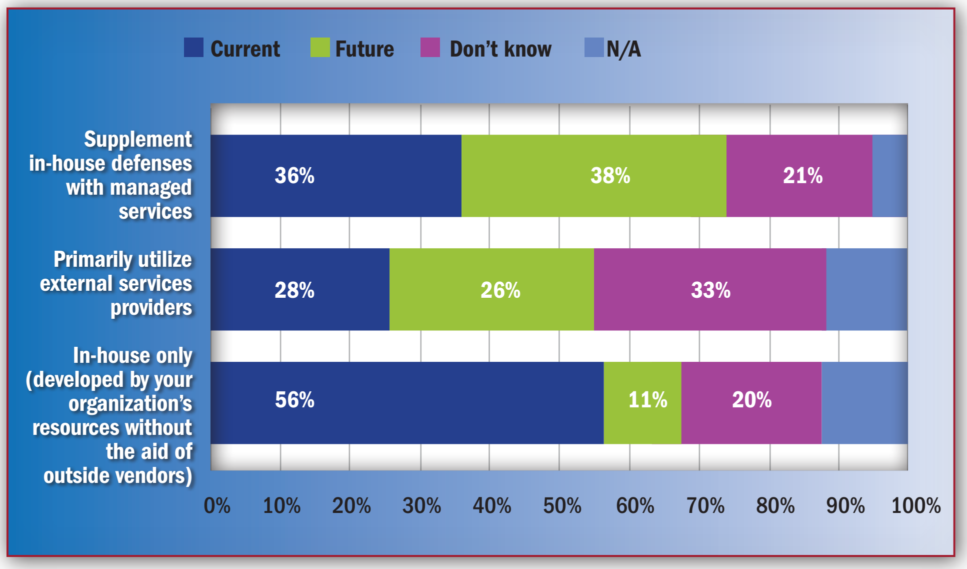
It's clear that decision makers are beginning to rethink how they should combat the growing threats. While a majority (56 percent) of those surveyed indicate they are reliant today solely on in-house resources to meet the needs of 24x7 security monitoring and remediation, only 11 percent indicate they plan to go it alone in the future.

Some of those surveyed will rely entirely on outside services providers, while 74 percent will, or already are, using managed services to supplement in-house resources. Among those who have already made the shift, 27 percent are currently utilizing a cloud-based DDoS service and 24 percent are using cloud-based Web application firewalls.

How has your web security budget changed over the past 3 years and how do you anticipate it will change over the next 3 years?



How do you currently or in the future expect to meet the needs of 24x7 security monitoring and remediation?



Building a Cloud-based Defense Strategy

Cloud-based services provide organizations with a competitive edge over the bad guys. The cloud provides scale and consolidates threat intelligence that can offer protection from increasingly large and sophisticated DDoS attacks and Web attacks such as SQL injections.

Cloud-based solutions are able to identify and mitigate suspicious traffic without compromising performance or availability of the origin server. If the solution is running on a robust, global platform, it has the scale to handle spikes in malicious traffic that are increasingly commonplace. Cloud-based service providers have visibility into many different Web sites, often across many industry sectors, and are able to spot emerging patterns, alert their customers to new threats, and update their service platforms to combat the threats.

Furthermore, cloud-based solutions can deliver significantly enhanced protection without requiring investment in new IT security infrastructure, helping to contain costs. Rather than incurring large upfront CAPEX to implement a do-it-yourself defense, cloud enables organizations to convert their security investments a lower monthly OPEX, while buying into a larger global infrastructure with resources they'd never be able to match internally.

Organizations with finite resources can't easily adapt to ever-increasing volumes of DDoS traffic, for example, but a cloud services provider can provide on-demand scale to deal with vast spikes in malevolent traffic aimed at crippling servers. While a local DDoS appliance can typically handle no more than 1 gigabit per second and will not stop most DDoS attacks today, a service provider such as Akamai, which delivers daily Web traffic reaching more than 10 terabits per second, is able to absorb attacks measured in tens or even hundreds of Gbps with relative ease.

Unlike inflexible, on-premise devices, a cloud-based solution can absorb DDoS traffic targeted at the application layer, deflecting all DDoS traffic targeted at the network layer, and authenticate valid traffic at the network edge. A cloud-based Web application firewall can help detect and deflect threats in HTTP and HTTPS traffic, issuing alerts or blocking attack traffic closer to its source. An additional layer of security protection may involve cloaking an enterprise's origin from the public Internet, preventing direct-to-origin attacks without impeding the quick and reliable delivery of content.

Defending the Enterprise's Growing Web Reliance

The Web is at the heart of business today—workers, customers, partners and other external stakeholders depend on availability. When Web sites slow or go offline, or worse yet, if customer data is stolen, a company risks business reputation, customer loyalty and lost revenue, in addition to the costs that will be required to get everything back up and running. Some organizations may have hundreds of Web sites and applications at risk at any time, creating a broad profile that attracts cyber criminals, terrorists, and mischief.

Service providers utilizing cloud-based solutions can provide the scalability, expertise and responsiveness that can mean the difference between business as usual and being crippled by unexpected assaults. With greater visibility into the global threat landscape, on-demand scale and an always-on posture, organizations can rely on a more proactive and resilient defense. For more information on combatting growing cyber threats, go to **www.akamai.com/security**.

GATEPOINT RESEARCH

Knowns and Unknowns

While most readers undoubtedly feel like they've been using the Web forever, from a security perspective there are new lessons to be learned every day.

Early in 2014, it was learned that a DDoS assault was launched that exploited "a seemingly innocuous feature of WordPress, [the] content management system that currently runs approximately 20 percent of all websites," observed Akamai's Bill Brenner in a blog examining the issue.[8]

According to PC World, "The WordPress bug ticket related to the pingback DDoS issue was originally created in 2007 and reveals that WordPress' developers tried to partially mitigate the problem with several patches over the years, last time in WordPress 3.6, which was released in August." Nonetheless, an estimated 160,000 WordPress sites were exploited in March 2014 to direct a DDoS assault against an unnamed but popular WordPress site that was disabled for several hours.[9]

Larry Cashdollar, a member of Akamai's CSIRT team, analyzed the vulnerability and noted in an advisory that, "Essentially this is an open proxy allowing any malicious user to use a WordPress site to direct layer seven attacks at a target. This can also be abused to target internal systems if the webserver is hosted on an internal network."

One of the adverse impacts of the Web is that such vulnerabilities may in fact be known to a select few who view them as innocuous, until someone with malicious intent discovers how to leverage the vulnerability and unleash it on the vast number of unknowing innocents.

[1] Source: "*Markets for Cybercrime Tools and Stolen Data*," Lillian Ablon, Martin C. Libicki, Andrea A. Golay, 2014. RAND Corporation. http://www.rand.org/pubs/research_reports/RR610.html

[2] Source, "*2013 Cost of Cyber Crime Study: United States*," October 2013. Ponemon Institute.

[3] Source: "*Cyber Threat Source Descriptions*." https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

[4] Source: "*2014 Data Breach Investigations Report*," Verizon

[5] Source: "*Prolexic Q2 Quarterly DDoS Attack Report*," www.prolexic.com/attackreports

[6] Source: "*Ntt Innovation Institute Announces The Availability Of The 2014 Global Threat Intelligence Report*," March 27, 2014. NTT Group. http://www.ntti3.com/ntt-innovation-institute-announces-the-availability-of-the-2014-global-threat-intelligence-report/

[7] Source: "*The State Of Web Application Security: An Ians Custom Report*," August 2013. IANS. http://resources.idgenterprise.com/original/AST-0100099_IANS_WhiteHat_Custom_Report.pdf

[8] Source: "*Anatomy of Wordpress XML-RPC Pingback Attacks*," Bill Brenner, March 31, 2014. https://blogs.akamai.com/2014/03/anatomy-of-wordpress-xml-rpc-pingback-attacks.html

[9] Source: "*Over 160,000 WordPress Sites Used as DDoS Zombies*," PC World, Lucian Constantine, March 11, 2014. http://www.pcworld.com/article/2106940/large-ddos-attack-brings-wordpress-pingback-abuse-back-into-spotlight.html