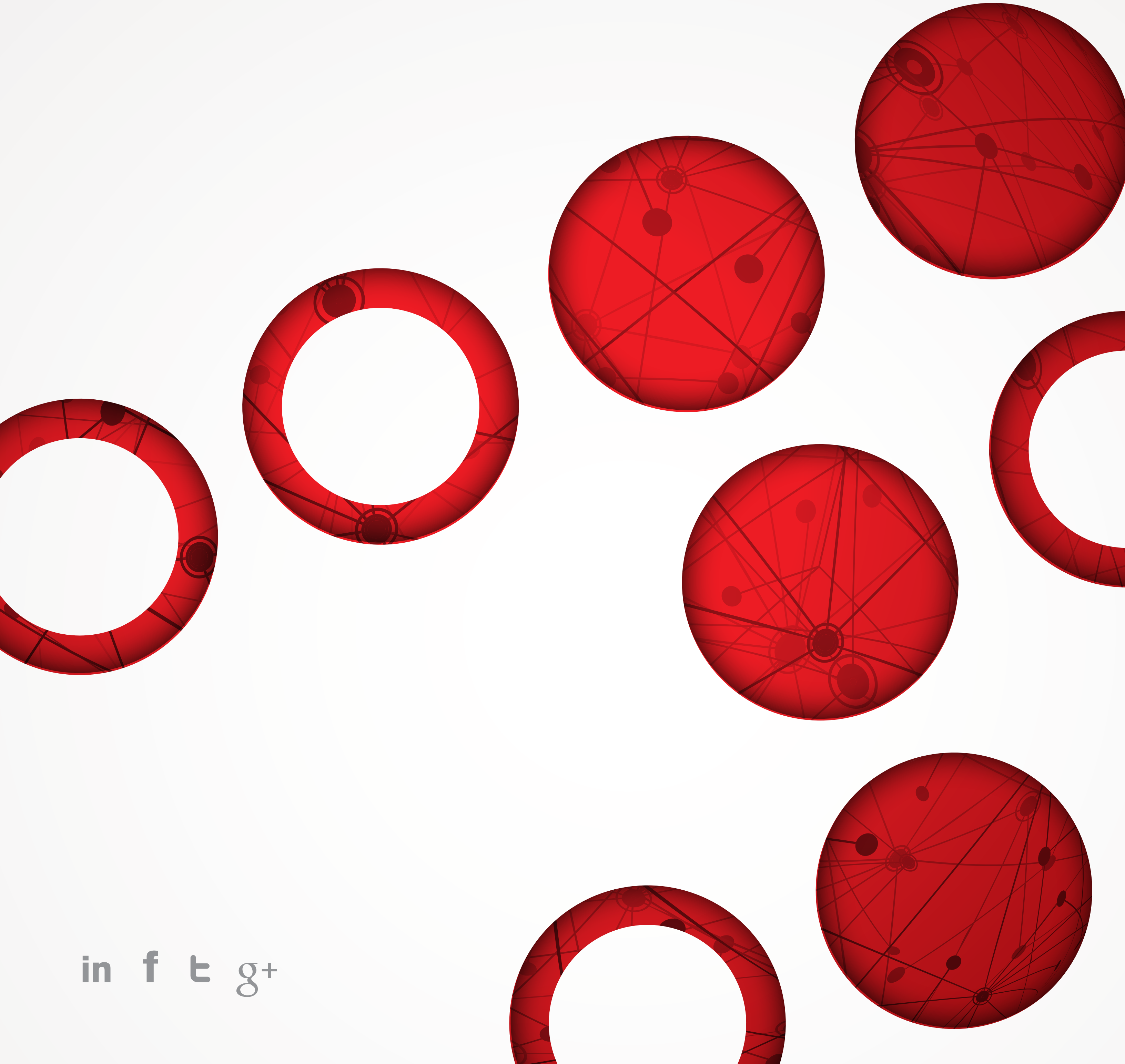
2015–2016

radware

GLOBAL APPLICATION & NETWORK SECURITY REPORT



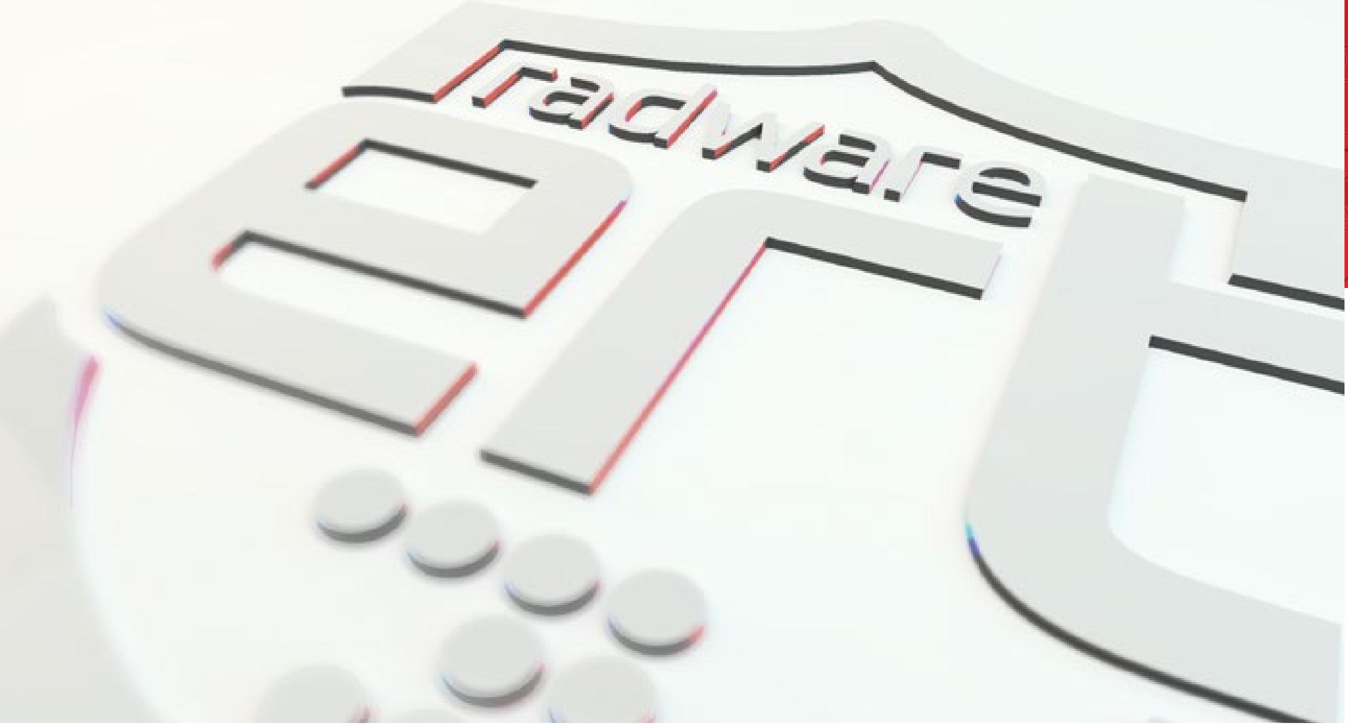
radware

GLOBAL APPLICATION
& NETWORK SECURITY
REPORT

2015–2016

Table of Contents

radware ert



01 Executive Summary

Radware's annual Global Application & Network Security Report outlines findings and analysis of our 2015 industry survey, reflects our Emergency Response Team's (ERT) in-the-trenches experiences fighting cyber-attacks and incorporates perspectives of two third-party service providers.

Designed to benefit the entire security community, this research provides a comprehensive and objective review of 2015 cyber-attacks from both a business and a technical perspective. It offers best practice advice for organizations to consider when planning for cyber-attack protection in 2016.

Top-Level Findings

Cyber-Attacks: No One Immune, Few Prepared

This past year's onslaught of cyber-attacks resulted in a both an operational and philosophical capitulation to two correlated facts: none are immune to cyber-attacks, and few are prepared. That echoed across our survey respondents, spanning enterprise verticals from financial services and critical infrastructure to cloud services.

Over 90% Experienced Attacks in 2015
More than 90% of respondents reported experiencing attacks in 2015. Only one in ten had not experienced any of the attacks covered in the survey.

Increased Attacks on Education and Hosting Industries
The Cyber-Attack Ring of Fire maps vertical markets based on the likelihood that organizations in these sectors would experience attacks. In 2015, several verticals faced consistent levels of threat, while both Education and Hosting moved from "Medium" to "High" risk. This means that organizations in these verticals are more likely to experience DoS/DDoS and other cyber-attacks and to experience such attacks at a higher frequency than in the previous year.

Are You Ready? Preparedness for Cyber-Attacks Varies

While more than 60% indicated being extremely/very well prepared to safeguard against unauthorized access and worm and virus damage, the same proportion of respondents indicated somewhat/not very prepared against advanced persistent threats (APT) and information theft. For distributed denial of service (DDoS), results split almost evenly between prepared and not prepared to protect against such attacks.

Protection Gaps Identified Across the Board

One-third of respondents cited a volumetric/pipe saturation weakness, and another quarter cited vulnerability to network and HTTPS/SSL attacks. Overall weaknesses are spread fairly evenly, suggesting a true protection gap for most organizations today.

Shift in Motives and Impact

Slowness Remains Main Impact of Cyber-Attacks

Historically, avoiding an outage justified new security investments. Yet the impact of attacks on systems was most often slowness, not a full outage, as reported by almost half of survey respondents. This combined with the over-provisioning of technology means that outages are often taking a backseat when assessing procurement decisions.

DDoS Remains Biggest Threat of all Cyber-Attacks

Similar to 2014, one-half of respondents indicated that DDoS attacks would cause the greatest harm to its organization. Unauthorized access follows as a close second.

Increase in Ransom as Motive for Cyber-Attacks

This year's survey results underscore a significant growth in ransom as motivation for attackers, which increased from 16% in 2014 to 25% in 2015. In addition, just over one-third of respondents experienced ransom or SSL/TLS-based attacks.

Consider the highly publicized attacks on Swiss-based encrypted email provider, ProtonMail. In November 2015, the company experienced consecutive attacks initiated with a ransom request by a new hacker group, The Armada Collective. Hoping to stop the attacks, ProtonMail paid a ransom, only to see the attacks continue with volumetric and burst attacks combining application and network vectors.

Tangible Concerns Expand

This year's survey results point to a shift in concerns from reputation loss to serving customers and ensuring application service level agreements (SLAs). Although reputation loss was still the biggest business concern after a cyber-attack, the percentage citing it as such decreased significantly from 47% in 2014 to 26% in 2105. More respondents are concerned about customer loss or service availability.

Better with Bots: Growing Need for Security Automation

This report outlines the rise of advanced persistent denial-of-service (APDoS) attacks. These attacks represent a clear and emerging threat demanding more advanced detection and mitigation and, more often than not, true partnership with DDoS mitigation service providers.

APDoS attacks involve massive network-layer DDoS attacks and focused application layer (HTTP) floods, followed by repeated SQLI and XSS attacks occurring at varying intervals. Typically, perpetrators simultaneously use five to eight attack vectors involving up to tens of millions requests per second, often accompanied by large SYN floods that can not only attack the victim but also the service provider implementing any sort of managed DDoS mitigation capability.

Today's Existing Solutions: Frequent Multi-Vendor and Manual

Today's threats drive demand for automated defenses and rapid analysis and mitigation. Yet, many organizations are still relying on a patchwork of solutions that require heavy manual intervention. Ninety-one percent of survey participants are using multiple solutions; only 6% are utilizing only one solution against cyber-attacks. Almost three-fifths indicated a medium degree of manual tuning required by its current solution, with some manual configurations.

Adoption of Hybrid Solutions Continues to Grow

Organizations reported brisk adoption of hybrid solutions that integrate cloud-based protection with on premise protection. In 2015, 41% of survey participants indicated utilizing a hybrid solution. In 2014, just 21% said the same.

Burst Attacks on the Rise

Burst attacks (within 60 seconds) are increasing. More than half of the three biggest attacks experienced lasted one hour or less, a significant increase from the 27% that said the same in 2014. It also indicates greater use of automated, bot-based attacks that generate large volumes of attack traffic in a short period of time, and maintain that as an attack campaign over a long period of time; essentially creating an APDoS.

Beyond Network: Similar Frequency for Network & Application Attacks

This year's report explores attack frequency—the frequency of attacks for top network and application vectors. While there is some variation in the different types of attacks, overall, there is a similar spread of frequency between network and application types of attacks. This is another indication that today's attack campaigns, specifically APDoS, involve multiple vectors from both the network and application layers and organizations must be able to protect themselves from both categories.

This report also describes how a major US-based airline dealt with the rise in automated attacks and the sophistication of application layer attacks. Bad bots that acted as faux buyers were created which caused the airline's inventory to essentially be held hostage. As a result, a number of flights were taking off with empty seats that should have been sold. The case demonstrates what the airline did to protect its applications from advanced bots and how website operators need more advanced user and client identification that can detect and block illegitimate users.

Building on this airline story and other such cases we predict another level of change: the rise of security automation and challenge security professionals to evolve for the new reality of "white-hat" bots.

What Changed in Security in 2015?

This year brought the rise of APDoS—the attack technique that deploys multi-vector attack campaigns targeting all layers of the victim's IT infrastructure: network, server and application. Attackers are demonstrating more patience and persistence, leveraging "low and slow" attack techniques that misuse application resources rather than those in network stacks. Attackers are using evasive techniques to avoid detection and mitigation; including SSL-based attacks and changing the page request in an HTTP page flood attack.

Years ago, DoS attacks mostly targeted the network through SYN, TCP, UDP and ICMP floods. From 2010 to 2012, there was an increase in more sophisticated application-level attacks and SSL encryption-based attacks. Recently, a specific type of DoS attack—the amplification reflective flood—has not only revived network attacks but also given attackers an edge over counterparts who target applications. Reflective attacks, including those using DNS, NTP and CHARGEN, became more active in 2013 and remained a persistent threat throughout 2014. The rise in reflective attacks has contributed to the Internet pipe as the major failure point in enterprise security.

The simplicity of launching such cyber-attacks and the variety of attack tools available are among the reasons why more organizations are suffering more attacks, such as DDoS. The question is no longer about preventing attacks. The attacks are going to happen. The imperative is now detection and mitigation.

Protection from Multi-Vector Attacks

In the face of evolving threats, organizations need to implement robust security solutions that fully protect against all types of attacks.

To target an organization's blind spot, attackers deploy parallel, multi-vector attack campaigns by increasing the number of attack vectors launched in parallel and targeting different layers of the network and data center. If only one vector goes undetected, the attack is successful and the result is highly destructive.

To effectively mitigate all types of DDoS attacks, organizations need a single vendor, hybrid solution that can protect networks and applications for a wide range of attacks. A hybrid solution integrates on-premise, real-time detection and mitigation with on-demand cloud-based protection to block volumetric attacks. A truly integrated solution includes all the different technologies needed, including DoS protection, behavioral analysis, IPS, encrypted attack protection and web application firewall (WAF).

As macro IT trends, such as migration to the cloud and adoption of IoT devices, continue to disrupt security effectiveness, this year's report also illuminates how security attacks are becoming more complex. This research confirms that motives, means and effectiveness of security attacks are on the rise—and highlights the need for greater agility to adapt quickly to evolving threats.

– Yaniv Hoffman
VP Technical Services, Radware

02

Methodology and Sources

Blending statistical research and front-line experience, this research identifies trends that can help educate the security community. This report draws its information from the following sources:

Security Industry Survey

The quantitative data source is an industry-wide survey, conducted by Radware with 311 individual respondents representing a wide variety of organizations globally. Building on prior years' research, the survey collected objective, vendor-neutral information about issues that organizations faced while planning for and combating cyber-attacks.

Within the sample, 45% of the companies are large organizations, each with annual revenue of more than US $500m. On average, responding organizations have just over 5,000 employees. More than 20 industries are represented with the largest respondents from the following: telecommunications/Internet/cloud service provider (24%), financial services (15%), computer-related products or services (14%) and government (6%).

The survey provides global coverage. Within the 311 respondents, 33% were from North America, 27% from Europe and 34% for Asia. In addition, just over half of the organizations (52%) conduct business worldwide.

Emergency Response Team Case Studies

Radware's Emergency Response Team (ERT) is dedicated security consultants that actively monitor and mitigate attacks in real time, providing 24x7 security services for customers facing cyber-attacks or malware outbreaks. As literal "first responders" to cyber-attacks, Radware's ERT members have extensive experience by successfully dealing with some of the industry's most notable hacking episodes. This team provides knowledge and expertise to mitigate the kind of attack that an in-house security team may never have handled. Throughout the report, the ERT team reveals how these in-the-trenches experiences fighting cyber-attacks provide deeper forensic analysis than surveys alone or academic research.

03

Cyber-Attack Ring of Fire

The Cyber-Attack Ring of Fire maps vertical markets based on the likelihood that organizations in these sectors will experience attacks. The Ring of Fire reflects five risk levels. As sectors move closer to the red center, such organizations are more likely to experience DoS/DDoS and other cyber-attacks and experience such attacks at a higher frequency.

Figure 1 illustrates that 10 verticals fall within the Cyber-Attack Ring of Fire. Red arrows reflect change since last year's report—indicating that the overall number of cyber-attacks, as well as the frequency and intensity of these attacks, increased in 2015. Several verticals face consistent levels of threat, while both Education and Hosting moved from "Medium" to "High" risk.

When any vertical shifts closer to the center of the Cyber-Attack Ring of Fire, companies in that industry are more likely to be the target of an attack. Mitigation assumptions should move in lockstep with risk level. When this does not happen, the likelihood of a cyber-attack resulting in a data center outage or service degradation increases drastically. Organizations in the verticals marked with a red arrow are wise to take swift action—adjusting mitigation strategies and solutions to reflect the new risk level.

Mitigation assumptions should move in lockstep with risk level. Organizations in verticals marked with a red arrow should take swift action—adjusting mitigation strategies and solutions to reflect the new risk level.

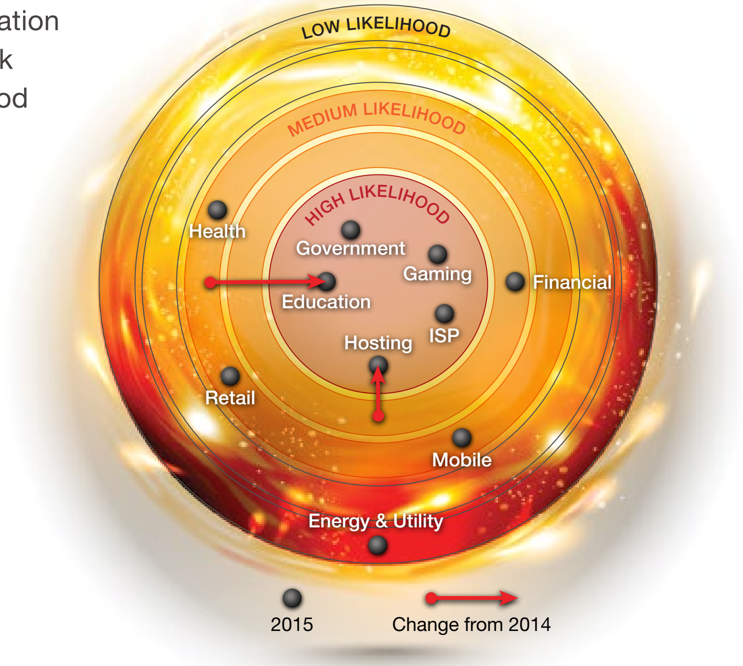


Figure 1: Cyber-Attack Ring of Fire

⚠ ⚠ ⚠ High Likelihood for Attacks

ISP

Following last year's trends, a growing number of ISPs are under attack as both primary and secondary targets. When an ISP is a secondary target, it is attacked solely because it provides services to the attackers' primary target.

Some attacks are financially motivated with groups such as The Armada Collective blackmailing large Internet Sercice Providers (ISPs) with threats of DDoS attacks unless ransom is paid via Bitcoin. These groups know that maintaining services is business critical for any ISP.

For ISP targets, attack vectors are mostly amplified UDP NTP/SSDP reflected floods and UDP fragmented floods.

Hosting

This year brought an increase in attacks against large hosting companies, some targeting end customers (website owners) and some targeting the hosting companies themselves. Motivations for these attacks vary. As with ISPs, some companies are threatened with a DDoS attack unless a ransom is paid through Bitcoin. Some are attacked due to the impression of offensive nature of the site they are hosting. In other cases, it seems that the attackers' objective is simply to cause damage to services that impact more than the company itself. For example, a DNS services attack on DNS hosting.

Attack vectors for these targets include HTTP/HTTPS floods, UDP fragmented floods, ICMP floods and various TCP floods, such as SYN-ACK, PUSH-ACK and TCP-RST.

Gaming

Gaming services continue to experience repeated attacks by hacktivist groups launching organized campaigns. In some cases, gaming companies are among a diverse group of targets; in others, campaigns are dedicated to specific gaming entities. Part of the appeal of targeting gaming services is that mandatory constant connectivity and availability of a centralized gaming platform creates a single point of failure. That makes for "efficient" attacks—with attackers able to cause more damage using fewer resources.

Attack vectors for these targets are usually SYN floods to specific ports that provide gaming services. However, attackers also used Tsunami SYN floods (SYN packet with data) several times, along with ICMP and UDP fragmented floods.

Tsunami SYN Floods

In October 2014, Radware's ERT detected a new type of SYN flood believed to be specially designed to overcome most of today's security defenses with a TCP-based volume attack. Within a 48-hour period, two unique targets in two different continents were targeted with this new technique and experienced very high attack volumes.

Although a normal SYN packet is characterized with 40-60 bytes per packet, this flood transmits very large SYN packet sizes (approximately 1000 bytes per packet), which complicate and defeat many defense algorithms. Attacks with these dimensions quickly consume bandwidth, with the initial attack targets experiencing pulses of 4Gbps to 5Gbps in attack traffic. This new type of attack has the ability to saturate its victim's Internet pipe faster than most attack types previously observed. We have aptly named this new volumetric flood "Tsunami SYN-Flood Attack."

It represents a new method "in the wild" that carries a tsunami-like volumetric attack over the TCP protocol. Normally, when perpetrators would choose a weapon to drive massive volume, they would need to settle on a UDP-based algorithm, as the stateless nature of this technology and small-sized packets are perfect for volumetric attacks, such as DNS, NTP and CHARGEN reflected floods. In this case, attackers have designed a volumetric attack based on TCP or stateful protocols, which can present a brand new danger: that with a TCP volumetric flood on a web server, a victim will not be able to deploy defenses similar to UDP-based attack to mitigate it.

Government

This year, government services were targeted and threatened through various campaigns of both hacktivists and terror groups responding to political climate. Attacks on government sites are not always politically motivated; many attacks are launched so that attackers gain notoriety and/or publically shame government sites for lacking “adequate security.”

In November 2015, several Thai government websites were hit by DDoS attacks, making them inaccessible for several hours. More recently, Turkish government sites were inaccessible in an ongoing attack on DNS services. Anonymous claimed responsibility for this 40 Gbps DDoS attack.

Attack vectors include UDP/TCP floods launched from tools distributed online, as well as brute-force attempts on special servers and websites.

Education

Cyber-attacks on school and other educational websites increased, as those who execute attacks on educational sites can gain notoriety and fame. Common attacks include hitting the mail server and targeting sites and services for submitting work and managing the admission process.

Both are “business” critical to any school—with downtime leading to day-to-day chaos and potential damage to an institution’s reputation. A growing number of “Help me DDoS my school” requests are popping up in dark corners of the Internet, making it easy for non-hackers to attack and inflict damage on school resources. In some cases, attacks targeting educational facilities represent student retaliation against the school and its policies.

Attack vectors for these targets include UDP amplified reflected floods, DNS Query flood, Web-Crawlers.

⚠ ⚠ Medium Likelihood for Attacks

Financial

As symbols of wealth and sometimes capitalism, financial institutions are frequently the target of hacktivist campaigns. All over the world, attacks on these institutions continue. Typically, these groups demand Bitcoin or another form of crypto-currency to stop the attack, as in the recent ransom-based DDoS attacks on Greek banks. 2015 brought an increase in both the average ransom amount and the number of groups attacking financial targets.

Financial services are also targeted to gain access to information they hold. Information gained through data breaches in banks and corporations can be used through extortion for financial gain. In December 2015, hackers leaked customer data after a United Arab Emirates Bank failed to pay the $3 million ransom the hackers demanded. In addition, the stolen information is often sold in black markets, leaving the banks with the task of managing the crisis of customer data retrieval and fraudulent transactions.

Attack vectors for these targets include very high-bandwidth UDP/TCP floods and connection floods, usually with several botnets exhausting link and service resources.

Health

In 2014, Boston Children’s Hospital became the first healthcare organization targeted by a hacktivist group. Following that incident, many other hospitals and healthcare centers were targets of various cyber-attacks—from extortion schemes, data stealing and HTTP floods to attack or abuse of a healthcare organization’s email servers. A Bitglass study discovered that sensitive information stolen from healthcare providers was up to fifty times more valuable than credit card data—yielding another spectrum of motivation for intrusion attacks, sometimes masked with DDoS attacks.[1] In July 2015, a data breach was uncovered at UCLA Health System affecting 4.5 million people. In this case, the hacking appears to have gone undetected since September of 2014.

Health insurance companies are another target in this segment, as they store a large amount of client information, even more than banks, making them a prime target for hackers. The hack of Anthem, one of the largest health insurance companies in the US, exposed the data of as many as 80 million customers, including many social security numbers.

Attack vectors observed included mostly UDP fragmented/NTP-Monlist floods, intrusion attempts and HTTP floods.

Retail

We observed cyber-attacks on retail businesses all over the world in 2015. The result: huge financial damage thanks to the little amount of service outage that is necessary to cause losses. Some of the attacks were launched with high bandwidth; reaching 40Gbps. Cyber-attacks against retailers are often used as a smokescreen for more sinister acts, such as ransom notices or large-scale data breaches. For retailers, one of the vulnerabilities is the use of CDNs, which are used to launch a large-scale attack that masks its origin with the CDN's identity.

Attack vectors for these targets include HTTP/HTTPS/Triple-Headers floods, TCP floods, SYN floods and connection floods.

Mobile

New smart-phone features create new vulnerabilities—giving individual hackers and hacking groups new ways to exploit mobile devices. That increases risk for both mobile users and mobile networks.

In addition, hacktivists targeted media companies because of objections to policies and nation state-funded groups targeted media companies because of objections to content.

Attack vectors for these targets include connection floods, SYN/empty connection floods and HTTP/S floods.

⚠ Low Likelihood for Attacks

Energy & Utility

For energy and utility companies, the threat landscape remains stable due to segregation of most of these companies' networks. Even so, this industry remains a valid target for DDoS attacks, particularly because of the damage a successful attack could cause. In recent years, the energy and utility industry faced advanced state-sponsored campaigns, including BlackEnergy, Energetic Bear, Mirage and Night Dragon, as well as numerous ongoing campaigns by China's PLA Unit 61398 and by Russia and Ukraine.

Recently, the Federal Bureau of Investigation (FBI) warned the United States to be on the alert for a sophisticated Iranian hacking operation whose targets include energy firms. The operation is the same as one flagged in mid-December 2015 as targeting critical infrastructure organizations worldwide. More than 50 victims uncovered, in 16 countries, including the United States.

[1] http://pages.bitglass.com/rs/bitglass/images/WP-Healthcare-Report-2014.pdf

04

Business Concerns of Cyber-Attacks

What are the motivations behind cyber-attacks? What solutions are used to mitigate such incidents? What are organizations doing to better prepare for future attacks? Radware surveyed security leaders to understand these business concerns related to cyber-attacks.

Attack Motivations

As in previous years, the majority of respondents (50% in 2015) claim to not know the motivation behind cyber-attacks. Thus, the data again suggests that most organizations are essentially in the dark when it comes to "why" of any attacks they have experienced. When motivations are unknown, it hinders an organization's ability to optimize preparation for future attacks.

The main known motivations—political/hacktivism and competition—have remained consistent in recent years. For the fifth consecutive year, political hacktivism holds the second spot in the survey, accounting for 34% of known attack motivations, with competition retaining the number three position cited at 27%.

Significantly, this year's survey also revealed an increase in ransom-oriented attacks, which account for about one-quarter of motivations (versus 16% in the prior year).

Most organizations are in the dark when it comes to the "why" of attacks. When motivations are unknown, it hinders the ability to optimize preparation for future attacks.

Which of the following motives are behind any cyber-attacks your organization experienced?

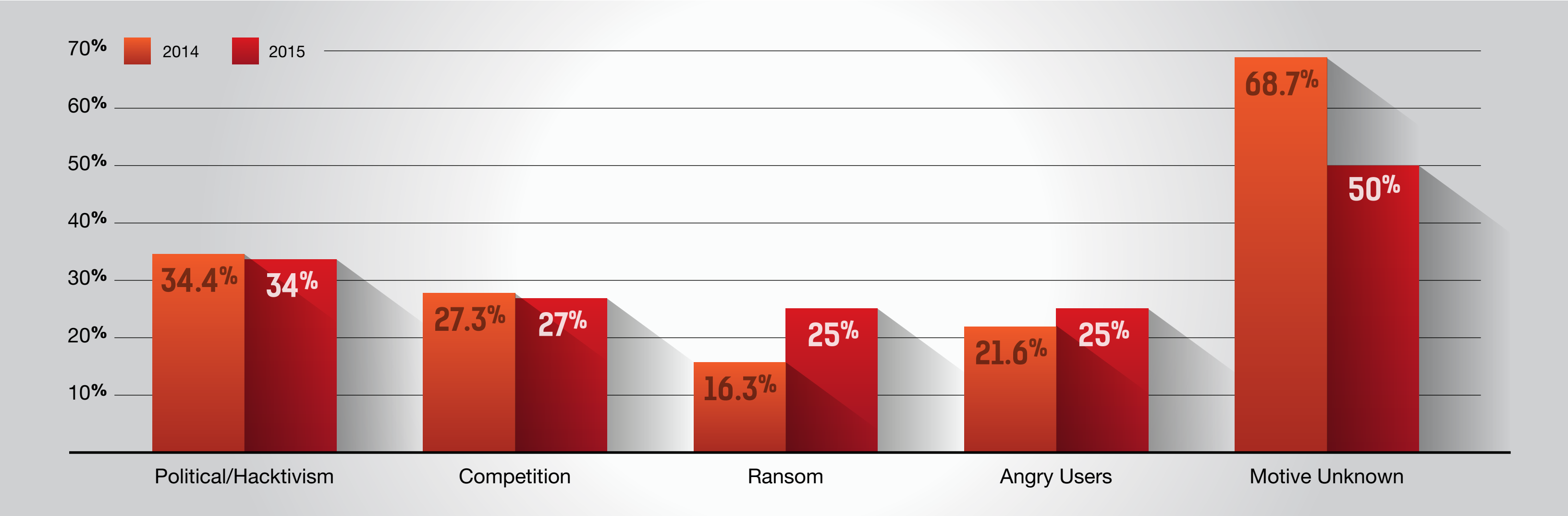


Figure 2: Most Common Motives Behind Cyber-Attacks

The Most Threatening Threats

As in 2014, DDoS remains the largest threat for organizations—as noted by half of respondents in the latest survey. DDoS ranked significantly higher than advanced persistent threats (APT), which decreased slightly to 35%.

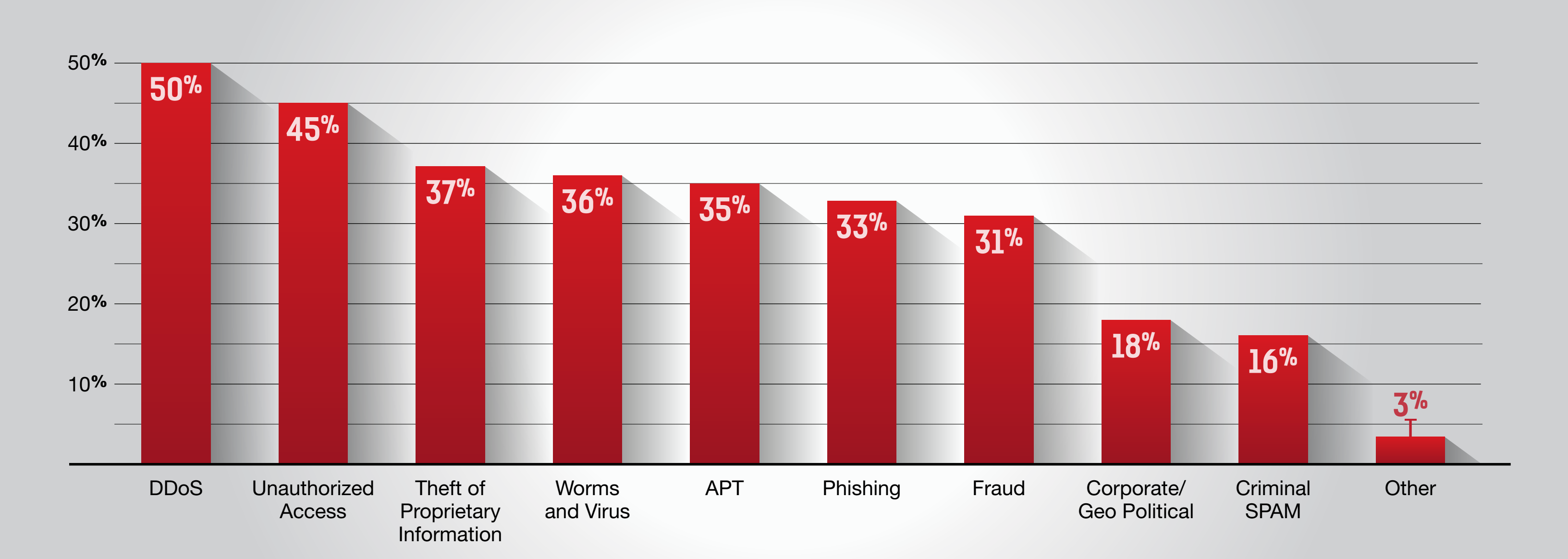


Figure 3: Attacks that will cause the most harm to businesses

We also asked about the types of cyber-attacks that organizations experienced in 2015. Those findings are consistent with the biggest threat, with half reporting DDoS attacks. The same proportion reported incidents with phishing, worms and viruses. The more significant finding is that only 9% have experienced none of these attacks. In other words, more than 90% of organizations were hit by cyber-attacks in the past year—underscoring that there is simply no escaping these threats.

> 90% of organizations were hit by cyber-attacks in the past year—underscoring that there is simply no escaping these threats.

What type of attack have you experienced?

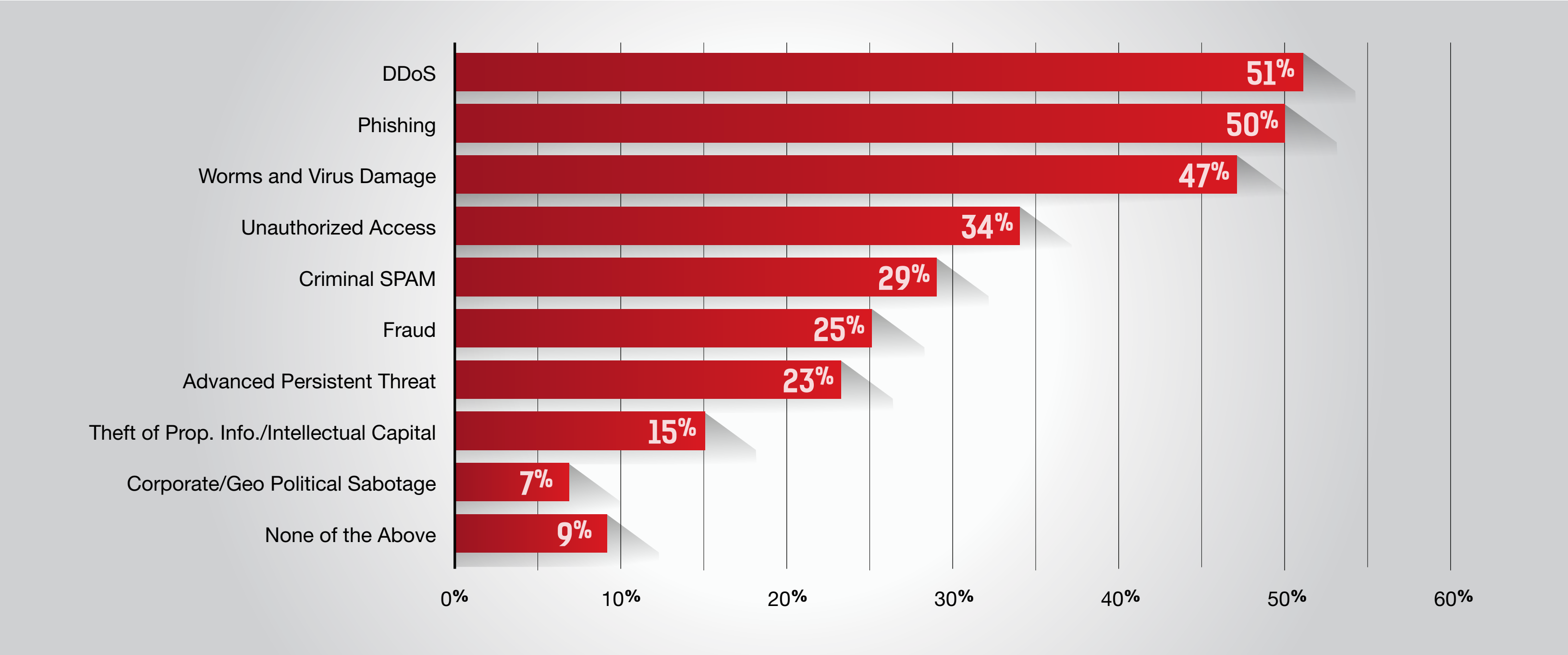


Figure 4: Types of Attacks Experienced By Organizations in 2015

Preparedness

When asked if their organization is prepared to fight cyber-attacks, respondents indicated that there are many entities that are not ready for the fight. While three out of five respondents feel extremely/very well prepared to safeguard against unauthorized access, as well as worm and virus damage, about three in five said they are somewhat/not very prepared against APT and information theft. For DDoS attack protection, the results are split evenly between those that are prepared and those that are not prepared.

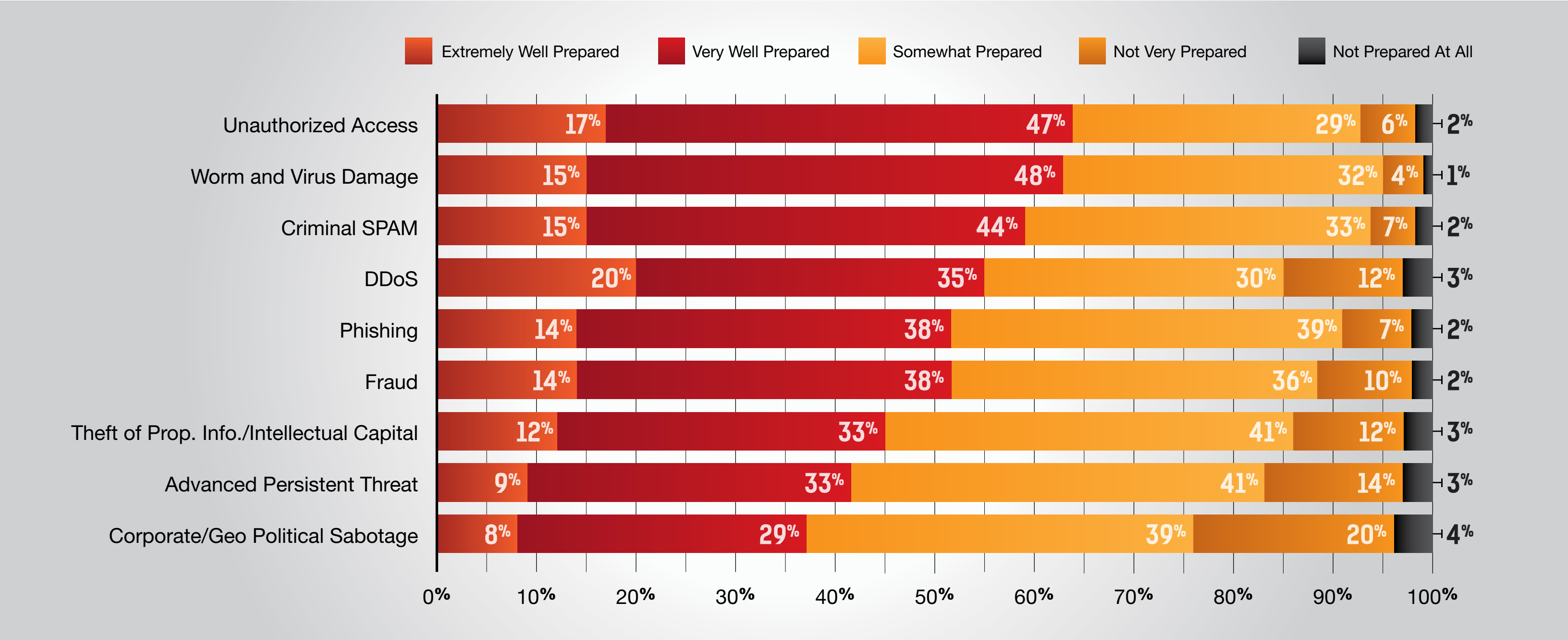


Figure 5: How Prepared Are Today's Organizations?

Respondents were also asked about the effectiveness of existing solutions in blocking cyber-attacks. Only one in four said its solution(s) was effective and blocked all attacks on the organization's systems, while the majority said its solution is somewhat effective or ineffective at blocking attacks.

When asked about where the protection weaknesses resides, one-third of respondents feel their organizations have a volumetric/pipe saturation weakness. Another quarter is vulnerable relative to network and HTTPS/SSL attacks. Overall, the weaknesses are spread pretty evenly, illustrating a true protection gap within most organizations today.

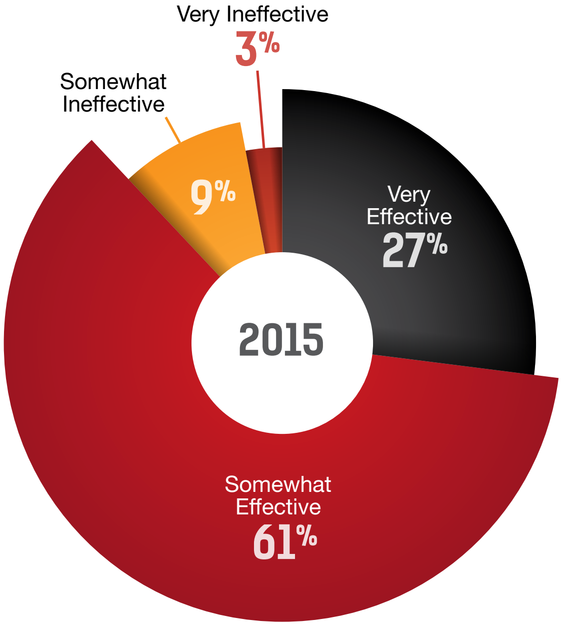


Figure 6: Effectiveness of Current Security Solution

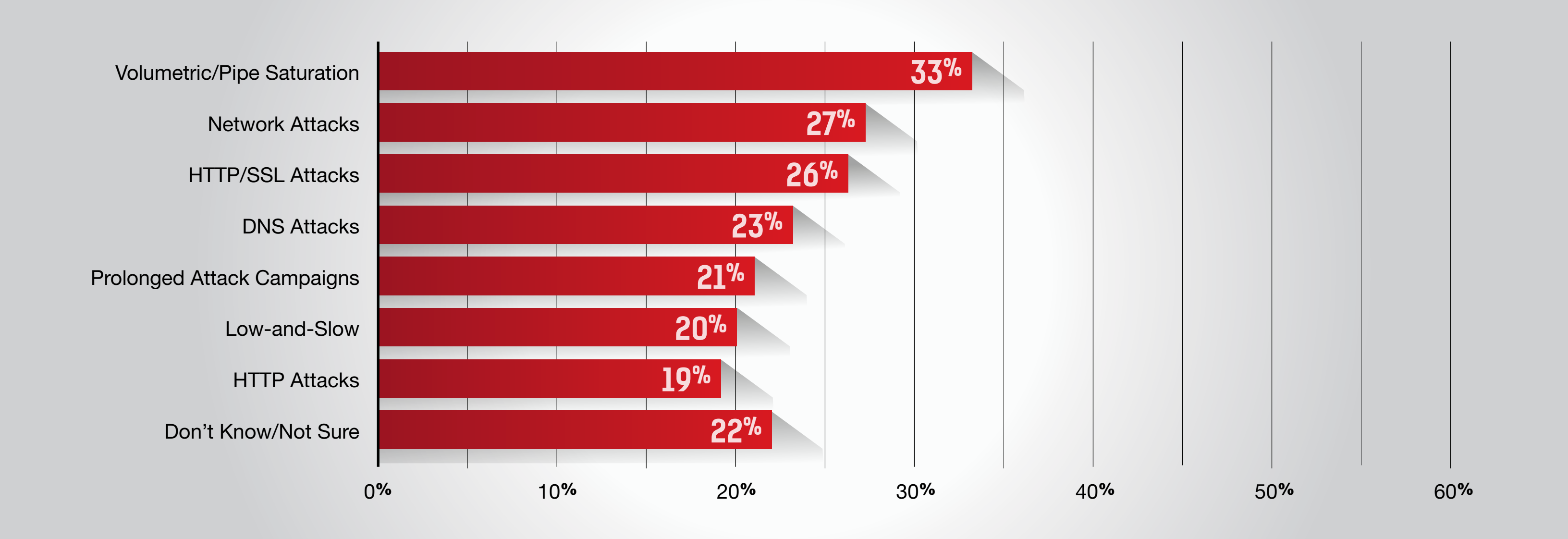


Figure 7: Weaknesses in Organizations Security Solution

Finding the Breaking Point

Respondents were asked about the average and maximum length of cyber-attacks experienced in the past year, as well as how long they can fight an around-the-clock cyber-attack. Our goal: to understand the average "breaking point" for organizations.

One-third of respondents (33%) said that the average attack was one hour. Over one in ten (11%) indicated its average security threat lasted three hours, and 15% indicated attacks that averaged a month; an increase from the 9% in last year's report.

About one-quarter of the respondents experienced attacks daily or weekly in the last year, but just as many experienced an attack only once or twice a year. In general, organizations expect attacks at a similar rate as what they experienced in the previous year.

What is the average security threat your organization experienced?

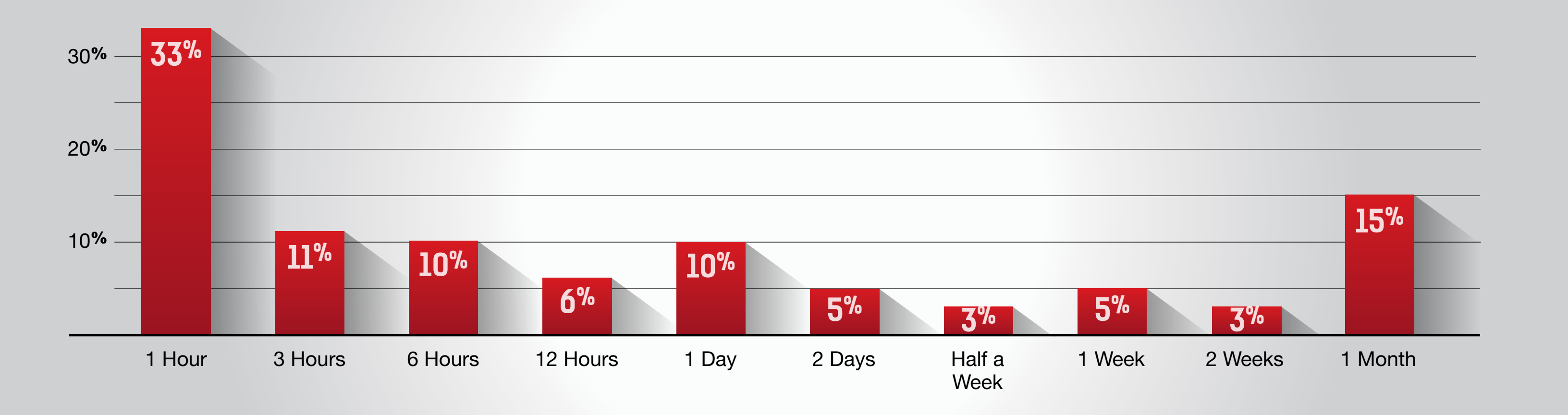


Figure 8: Average Security Threat Organizations Experienced

We also asked respondents about the maximum security threat duration their organization had experienced in 2015. One in five (about 19%) reported that it was one month. Nearly 17% told us that the maximum threat experienced was just one hour, with 12% indicating that the maximum threat duration was one day. That represents little change in the maximum threat duration findings from 2014.

What is the maximum security threat your organization experienced?

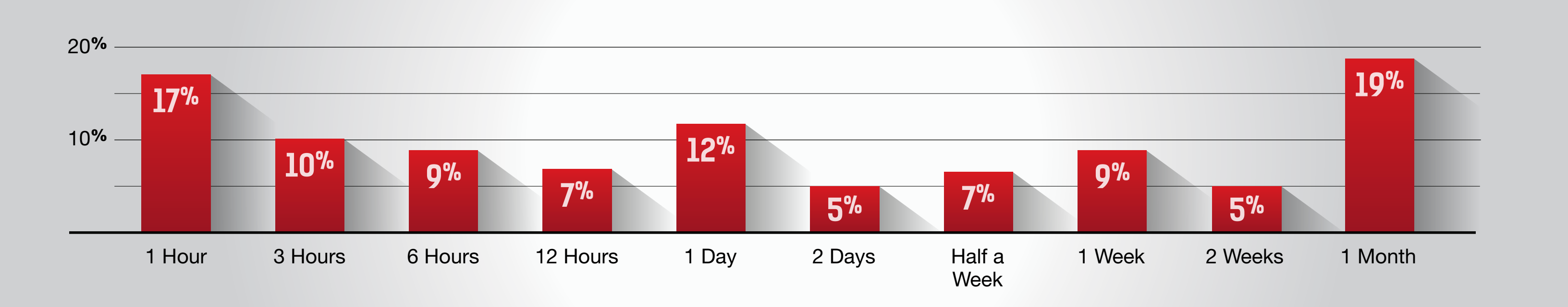


Figure 9: Maximum Security Threat Organizations Experienced

We also asked respondents how long they could effectively fight an around-the-clock attack. Almost half (46%) noted that they could only fight such a campaign for a day or less. Thirty-three percent said they are prepared to withstand an around-the-clock attack campaign lasting longer than a day. Twenty-one percent claimed to be able to fight such a campaign for more than one month.

How long can you effectively fight an around-the-clock attack campaign?

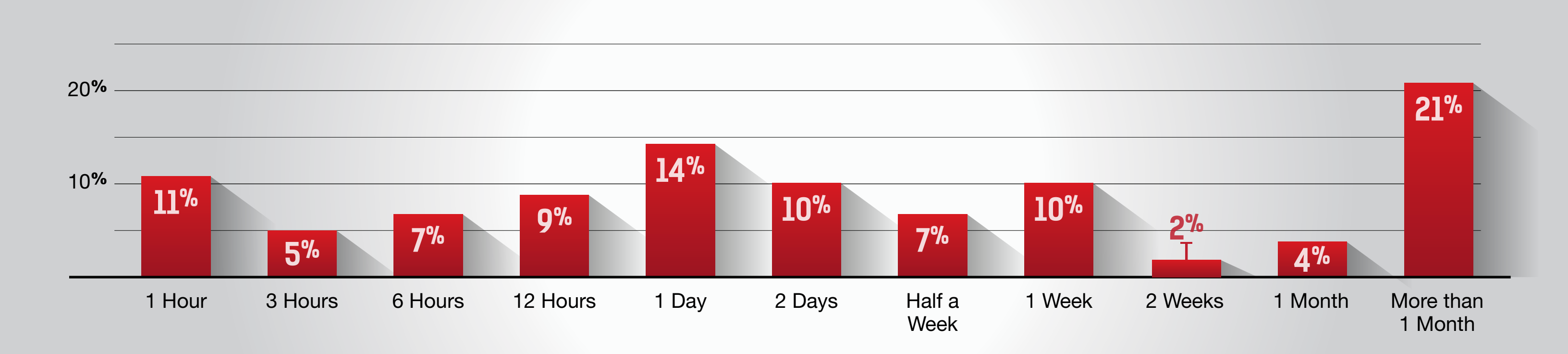


Figure 10: Time Organizations Can Fight A Round-the-Clock Campaign

Most Pressing Concerns

In our 2014 findings, respondents cited reputation loss and revenue loss as top business concerns vis-à-vis cyber-attacks. Our 2015 survey results point to a change in perspective—with 26% concerned about reputation loss (a drop of 21%) and 22% concerned about service outage and limited availability. This illustrates a shift in concerns related to cyber-attacks—that is, worrying less about reputation loss and more about serving customers and ensuring service level agreements (SLAs)

> This illustrates a shift in concerns related to cyber-attacks—worrying less about reputation loss and more about serving customers and ensuring service level agreements.

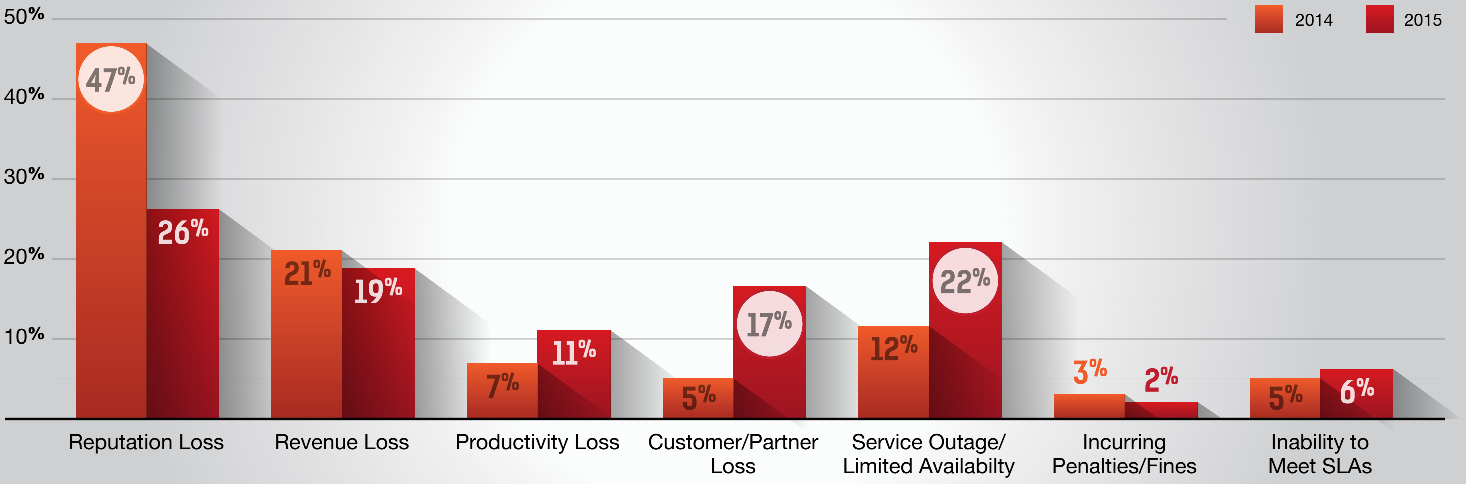


Figure 11: Top Business Concerns of Cyber Attacks

Budgeting and Planning

We asked survey respondents about how resources were deployed in response to cyber threats in the past 12 months. Once again, almost half of respondents reported investing in new or specialized technology (47%) and changing security processes, protocols and mandates (47%).

During the last 12 months how has your organization responded to cyber threats?

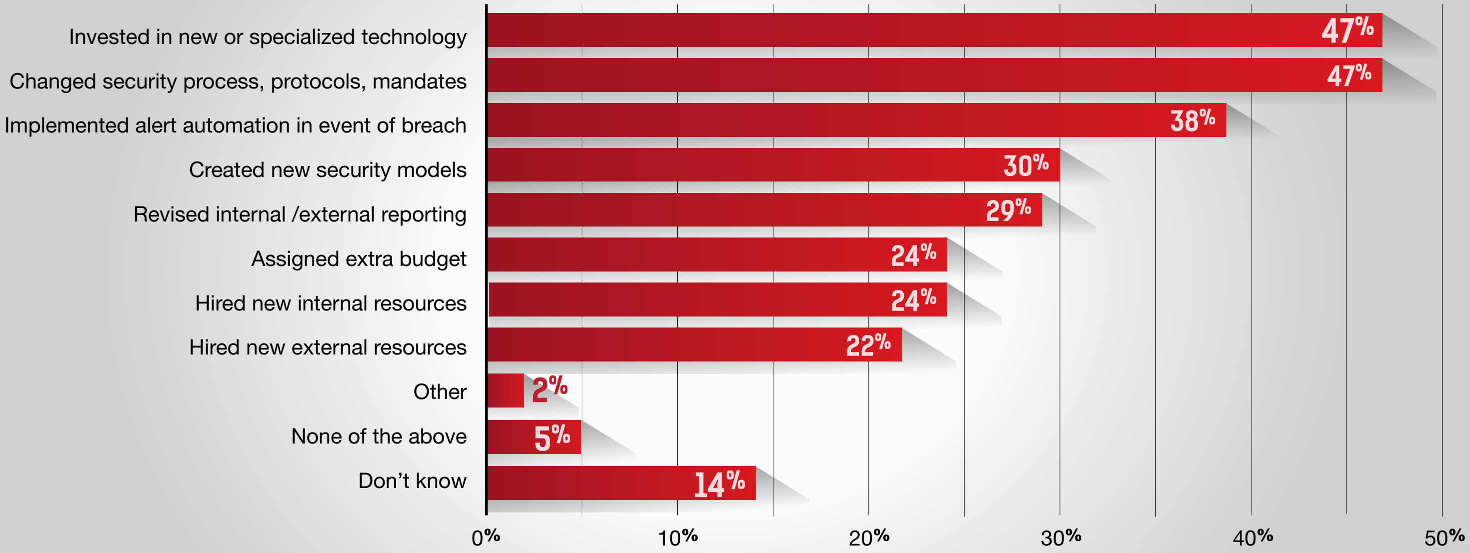


Figure 12: Organizations' Response to 2015 Cyber Attacks

Hybrid Protection for Cyber-Attacks

As predicted in last year's report, adoption of hybrid protection solutions continues to grow. This year, Radware refined the hybrid adoption calculation to focus specifically on organizations that have adopted, or are planning to adopt, a combination of on-premise DDoS protection with any cloud-based DDoS protection service (always-on cloud based service, on-demand cloud based service, CDN solution, or ISP-based or clean link service).

> Adoption of hybrid protection solutions increases, suggesting that hybrid solutions are the de-facto standard for DDoS protection.

Based on those parameters, 41% of 2015 survey participants indicated that their company is using a hybrid solution. In 2014, just 21% said the same. In addition, this year, another 44% indicated plans to adopt a hybrid solution, significantly reinforcing that organizations see the hybrid solution as the best approach. This number includes those that currently have a partial solution (only on-premise DDoS device or only cloud solution) with plans to add the other part of the hybrid solution. It also includes organizations that have neither an on premise DDoS device nor a cloud DDoS solution, but are planning to adopt both components of a hybrid solution.

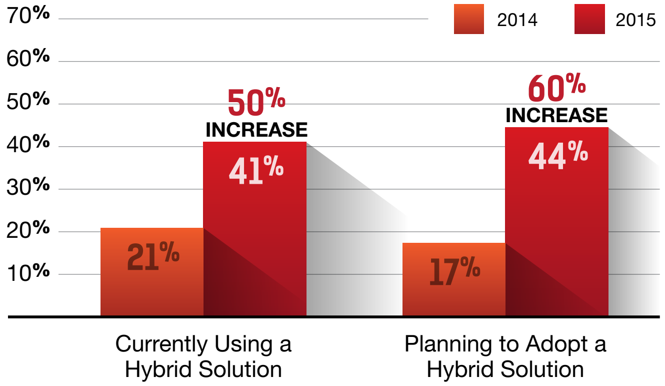


Figure 13: Significant increase in Current and Planned Adoptions of Hybrid Solutions

As seen in our survey, companies with the highest revenue, most employees, or worldwide scope are most likely to have a hybrid solution. There were no differences in use of a hybrid solution based on a company's geography or vertical market. Also, plans to add a hybrid solution are consistent across both revenues and company sizes further supporting the wide adoption across markets and industries. This suggests that hybrid solutions have become the de-facto standard for DDoS protection.

What solutions does your organization use against cyber-attacks?

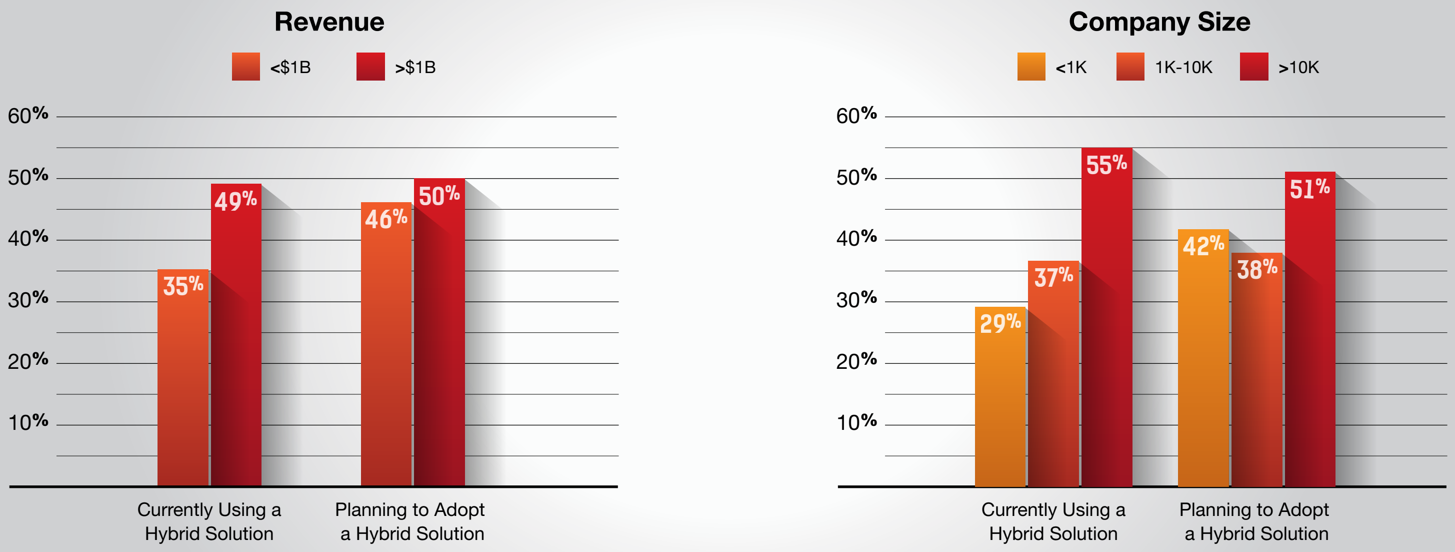


Figure 14: Adoption of Hybrid Solutions Continues to Grow

05

Attack Vector Landscapes

Combining the experience of Radware's ERT and responses to this year's security industry survey, this chapter reviews the attack vectors that proved popular in 2015.

Application vs. Network Attacks

At first glance, this year's research seems to indicate a change in the balance between application and network attacks. Unlike last year's survey—which showed largely equal incidence of network and application attacks—results from 2015 suggest a significant increase in network-based attacks. This is based on what respondents considered the three largest attacks their organization experienced in 2015. Digging deeper into the findings and it becomes apparent that network and application attacks actually still occur at a similar frequency. That is because of multi-vector, blended campaigns that include higher-volume network vectors alongside more sophisticated application vectors. Thus, while the three largest attack types reported by respondents are more likely to be network-based attacks, the threat of application attacks is still very much real. Regardless of attack type, in 2015, the most common impact on systems was slowness, as reported by almost half of survey respondents.

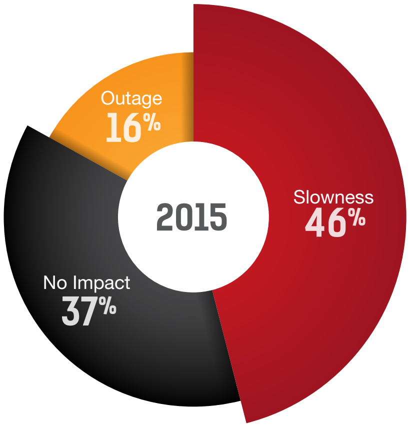


Figure 15: Impact of Attacks on Systems

In 2015, 65% of the three biggest cyber-attacks that organizations experienced were on the network, most frequently TCP-SYN flood. TCP-SYN flood attacks have risen to 24% from 18% in 2014. This year also brought an increase in ICMP attacks (14% in 2015 compared to 6% in 2014). Within application-based attacks in 2015, we saw fewer web attacks in the three biggest attack categories than in previous years, with web HTTP/S attacks decreasing from 23% to 15%. In addition, we are seeing DNS-based attacks drop to 13%—a level last seen in 2012 and 2011.

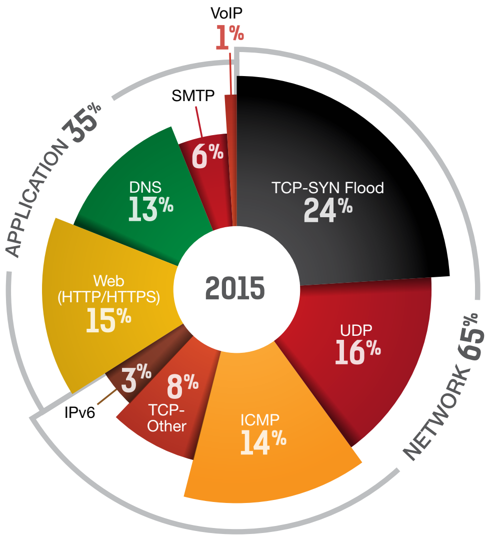


Figure 16: Biggest Cyber-Attacks in 2015

Frequency of Attacks

This year, attack frequency was also explored. More than one-quarter of respondents reported daily and weekly attacks on TCP-other, TCP-SYN, ICMP and UDP flood attacks in the past 12 months. Attacks on IPv6 networks represent the most infrequent network attack in 2015. At least one in five respondents experienced daily or weekly application attacks. Overall, we see a very similar spread of frequency between network and application types of attacks.

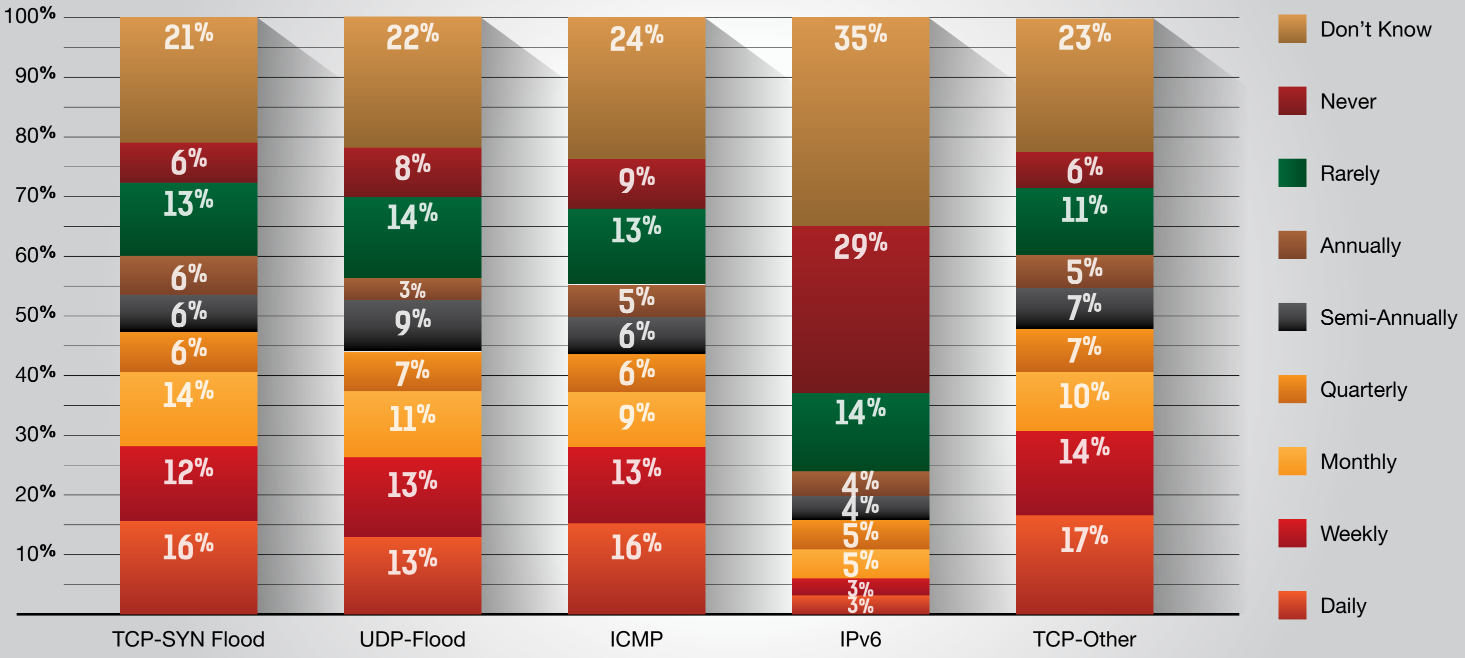


Figure 17: Frequency of Network Attacks in 2015

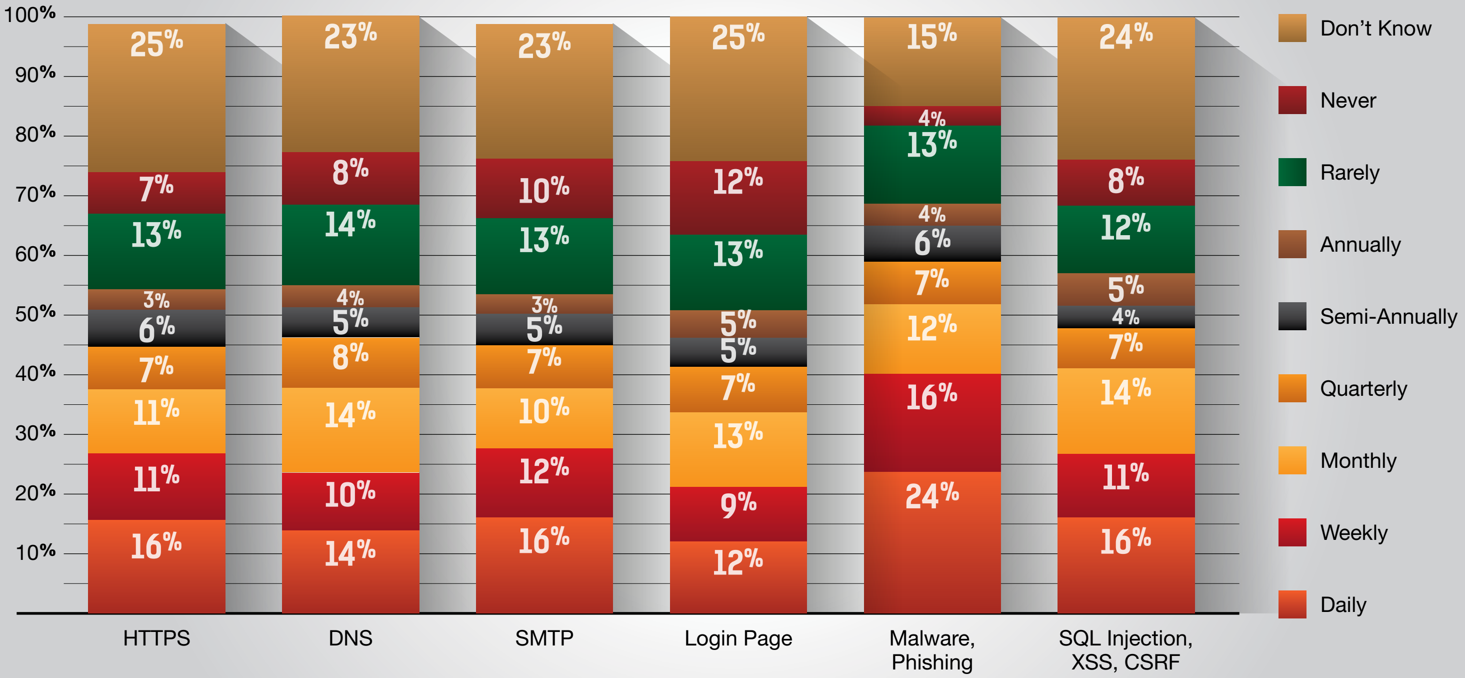


Figure 18: Frequency of Application Attacks in 2015

Multi-Vector Attacks

In 2014, nearly every attack campaign was composed of multiple attack vectors, and the trend away from single-attack vectors continues in 2015. Attacks are now advanced persistent DDoS campaigns. What's more, attackers are changing vectors based on mitigation in "burst-like" patterns, leading the way to smarter, automated attacks. Every year, attackers find new vectors of attacks, such as Portmappers, mDNS and RIPv1.

TOP VECTORS

TCP-SYN **UDP** **HTTP/S** **ICMP** **DNS**

Given the increase in ransom-motivated attacks in 2015 (25% up from 16% in 2014), as well as the overall rise in encrypted attacks, we asked respondents about their experiences with these types of attacks. Slightly more than one-third reported experiencing either a ransom attack or an SSL or TLS-based attack. Experience with these attacks does not differ by company size or revenue, emphasizing that none is immune from these recent attack trends.

The increase in encrypted attacks contrasts sharply with the confidence organizations have in its existing SSL protection. About half of the respondents indicated that its security solution includes SSL attack protection, though they are uncertain of exactly what types. Only three in 10 said its solution provides complete protection from SSL-based attacks, and one-fifth reported that their solution does not include SSL attack protection.

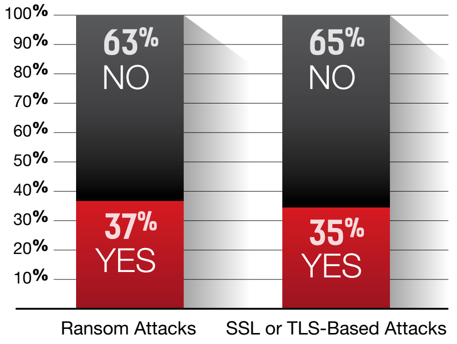


Figure 19: Ransom and SSl or TLS Attacks Experienced by Organizations in 2015

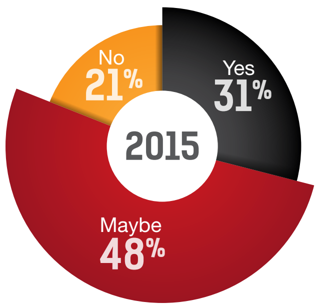


Figure 20: Availability of SSL Flood Attack Protection

Attack Size: Does It Matter?

In 2015, less than one in 10 server attacks qualified as "extra-large" (10Gbps and higher). The most common attacks—experienced by two in five respondents—were below that threshold. The number of 10Mbps to 100Mbps attacks increased in 2015 to 25% (compared to 7% in 2014), while the attacks ranging from 100Mbps to 1Gbps declined to 15% (versus 25% in 2014).

More than one-third of respondents indicated that the biggest attacks impacted the Internet pipeline, with nearly three in ten reporting impact on a server. One in five said the firewall was impacted. At 3%, load balancer impact was lower this year than in 2014 (10%). Otherwise, impacted systems have been consistent since 2012. One-third of respondents feel its organizations have a volumetric pipe saturation weakness; another quarter feel vulnerable to network and HTTPS/SSL attacks.

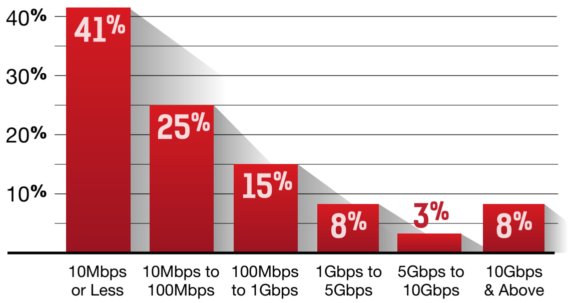


Figure 21: Availability of SSL Flood Attack Protection

As done in previous years, we asked about the potential bottlenecks during a DDoS attack. In a very consistent manner, the Internet Pipe, the Firewall and the Server are the top three likely points of failure in the organization's network. With the increase in volumetric attacks in past couple of years, the Internet Pipe continues to lead this year with 36% likelihood to become the bottleneck.

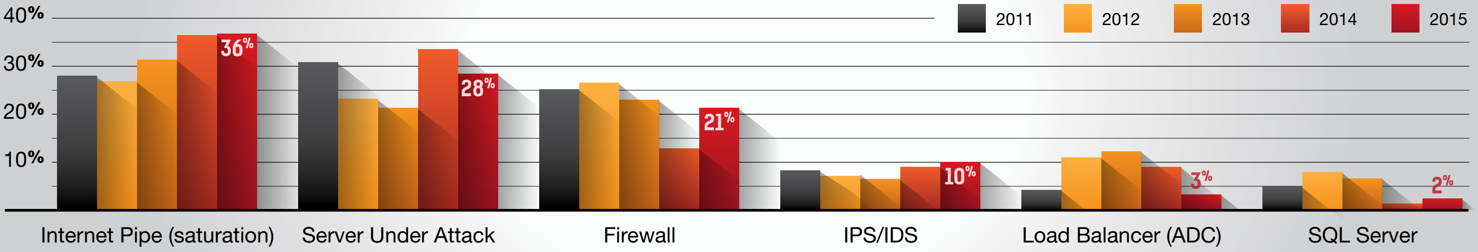


Figure 22: Three Biggest Cyber-attacks Suffered

06

Dynamic IP Addresses: Legitimate Traffic or Malicious Activity?

Cyber attackers have found an effective way to defeat IP-based defense systems: launch application-level attacks that originate from real—but dynamic—IP addresses. This chapter outlines some of the most common variations of dynamic IP attacks, explores challenges in defending against them, and points to best practices for thwarting these attacks.

Dynamic IP attacks target Layer 7, the application layer. Using real IP addresses, they establish a three-way TCP handshake and successfully bypass cookie and JavaScript challenges. These attacks are highly disruptive and difficult, if not impossible, for IP-based defense systems to distinguish between legitimate and malicious visitors.

To overcome traditional defenses, attackers commonly use headless browser software, such as PhantomJS or a Selenium WebDriver. They also employ multiple evasion tactics. To avoid triggering size- or rate-limiting thresholds, they split the load between dozens of IP addresses and constantly add new IP addresses. Human-like “behaviors” are incorporated—starting at different landing pages and mimicking human-like timings and patterns of movement. They can be especially difficult to detect when attacks are low rate and low volume and are spread over time and across a large pool of changing IP addresses.

Types of Dynamic IP Attacks

Some of the most common dynamic IP attacks include the following scenarios:

- **HTTP/S flooding**. This technique involves full-page reloads of dynamic content, fetching large elements and bypassing cache. Imagine 100 visitors arriving from what appear to be legitimate IP addresses and client headers. The empty browser cache issues a full-page reload that fetches about 50 HTML elements. After a minute, the process repeats with a new group of 100 IP addresses—resulting in 5,000 HTTPS requests per second.

- **Password brute-force attempts**. These often target HTTP, FTP, SQL, SSH and RDP. For example, 100 simultaneous clients, each with a unique IP, issue one request per second. After a minute, every client returns with a new IP address, generating 100 password attempts per second.[2]

- **Web scraping/data harvesting by gray marketers**. This technique can be used to attack online ticketing systems, enabling attackers to buy and sell tickets at a profit. Launching 500 clients with unique IPs, attackers monitor 500 tickets, waiting for a dramatic price drop to make a "bargain" purchase. Every client refreshes the pages every 10 seconds. After a minute, each of the 500 clients returns with a new IP—resulting in 500 bots online, each making 50 requests per second.

- **Web scraping/data harvesting by competitors**. This type of attack is similar to the one described above but is executed to collect competitive pricing and plagiarize content. In this type of dynamic IP attack, 100 clients with unique IPs issue 10 requests per minute, with each client crawling through a different category and clicking on items in random order. After three minutes, each client returns with a new IP. The result is the ability to "scrape" 1,000 items per minute.

- **Clickjacking**. This attack involves click fraud on a competitor's pay-per-click (PPC) advertisements. A common scenario: An operator remotely controls 1,000 malware-infected PCs. Every day, the malware generates 1,000 faked clicks on a competitor's PPC affiliate ads, leading to 30,000 monthly clicks. The competitor must then pay the affiliate regardless of whether or not a purchase is made. At one cent per click, the attack drums up $300 for the affiliate.

Methods of Execution

Attackers commonly use one of four methods to gain access to a large pool of IP addresses: malware botnets, lists of SOCK proxies, VPN services or cloud services.

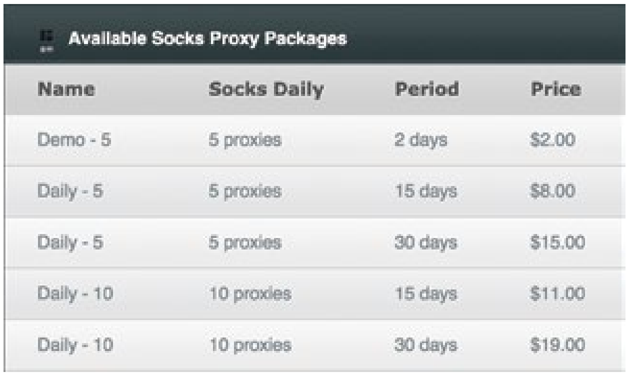
Malware Botnets

The notorious botnet created by the Linux XOR.DDoS malware has been responsible for thousands of DDoS attacks and hundreds of thousands of SSH brute-force attempts. The vast majority of targets infected by this malware are personal home routers or modems, all of which receive dynamic IPs from the respective Internet service providers.

Another example is the recently discovered LinuxEllipses malware, which infects the Linux host. In a sophisticated technique, it installs an anonymous proxy server that carries out future attacks. This malicious behavior further increases the prevalence of dynamic IT attacks.

Lists of SOCK Proxies

A huge number of SOCK proxies lists are floating publicly on various amateur forums (see Figures 23 and 24). New lists are submitted every day, with numerous offers from sellers of "verified and working" lists. Some sites have transformed this into a business of renting SOCK servers for a specific duration. Various attack scripts and tools can use lists of SOCK proxies to generate traffic over thousands of real clients.



Available Socks Proxy Packages

Name	Socks Daily	Period	Price
Demo - 5	5 proxies	2 days	$2.00
Daily - 5	5 proxies	15 days	$8.00
Daily - 5	5 proxies	30 days	$15.00
Daily - 10	10 proxies	15 days	$11.00
Daily - 10	10 proxies	30 days	$19.00

Figure 23: Example of virtual private networking (VPN) services

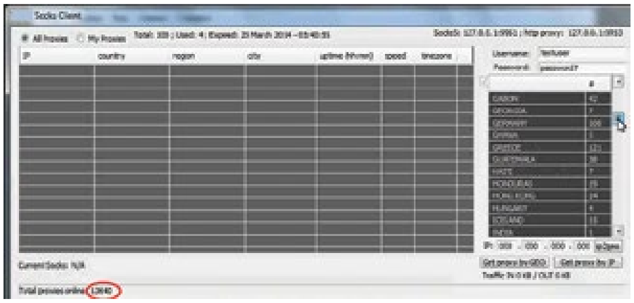


Figure 24: Example of SOCK proxy list

VPN Services

A variety of companies offer virtual private networking (VPN) services—including Hotspot Shield, TunnelBear, Private Internet Access, HideMyAss and CyberGhost, to name just a few. With hundreds of servers spread all over the world, these providers offer a pool of more than 100,000 IP addresses.

In mid-2015, the free "Hola VPN" browser extension was used to carry out a DDoS attack against the popular 8chan image board. More than 50 million users around the world use Hola to mask their true locations—bypassing censorship and gaining access to geo-blocked content, such as Netflix and BBC programming.

Cloud Services

Many cloud providers offer a free tier for developers and users who want to run small-sized servers and applications on cloud infrastructures. Such cloud providers are often the target of hackers, who are continually seeking access to more servers and services for launching malicious activity.[3]

In the quest to attract more customers, many cloud providers offer a simple and easy process for creating a new account. This ease of use has a dark side: insufficient security validations that enable hackers to abuse the cloud services and generate massive quantities of fraudulent accounts. Those fraudulent accounts can then be used to launch network attacks.

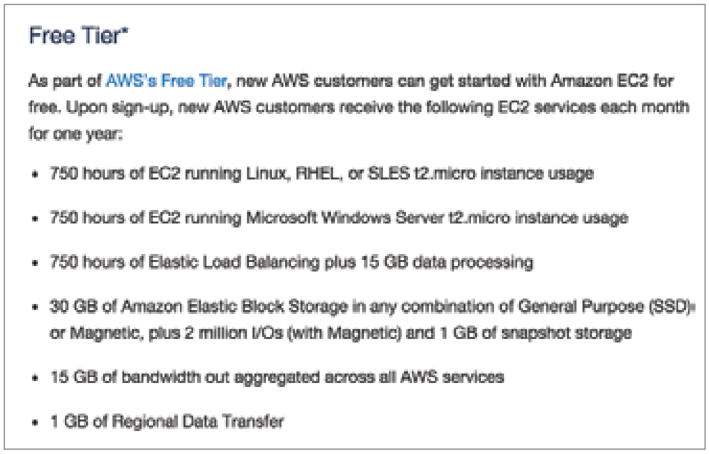
Existing cloud customers also can be the target of hackers, who welcome opportunities to obtain leaked or stolen API keys. Hackers can then use those keys to programmatically manipulate cloud services, such as Google AppEngine and Amazon Web Services (AWS). When such API keys fall into the wrong hands, they can be abused—as evidenced by a web developer who recently lost a reported $6,500 in just a few hours after his Amazon API keys were accidentally leaked on the public Internet.[4]

Simulating an Attack

One of the best ways to grasp this growing threat is by simulating a dynamic IP attack. This simulation is built around four core steps:

1. Register and activate an Amazon EC2 account

Amazon offers a nice free-tier package for new users during their first year (see Figure 25). During new account creation, Amazon enforces several mechanisms for preventing abuse of its services. These mechanisms include the need for a valid credit card and the ability to pass an account verification process via email or phone.



Free Tier*

As part of AWS's Free Tier, new AWS customers can get started with Amazon EC2 for free. Upon sign-up, new AWS customers receive the following EC2 services each month for one year:

- 750 hours of EC2 running Linux, RHEL, or SLES t2.micro instance usage
- 750 hours of EC2 running Microsoft Windows Server t2.micro instance usage
- 750 hours of Elastic Load Balancing plus 15 GB data processing
- 30 GB of Amazon Elastic Block Storage in any combination of General Purpose (SSD) or Magnetic, plus 2 million I/Os (with Magnetic) and 1 GB of snapshot storage
- 15 GB of bandwidth out aggregated across all AWS services
- 1 GB of Regional Data Transfer

Figure 25: AWS Free Tier

Amazon has done an excellent job ensuring that all EC2 resources have well-defined quotas—including a limit of five elastic IP addresses per instance, as well as extra costs for a high number of IP remaps.

Once the account is established, the API and SSH keys can be used to configure two servers: a WordPress backend and a PhantomJS headless browser.

[2] Note that brute-forcing also can be amplified, as explained in the article, Brute Force Amplification Attacks Against WordPress XMLRPC – https://blog.sucuri.net/2015/10/brute-force-amplification-attacks-against-wordpress-xmlrpc.html

[3] IAT 2015 featured an excellent analysis of this topic in a session titled CloudBots: Abusing Free Cloud Services to Build Botnets in the Cloud – http://www.bishopfox.com/news/2015/09/itac-2015-cloudbots-abusing-free-cloud-services-to-build-botnets-in-the-cloud/

[4] https://www.humankode.com/security/how-a-bug-in-visual-studio-2015-exposed-my-source-code-on-github-and-cost-me-6500-in-a-few-hours

3. Set up a headless-browser server (Ubuntu Linux or PhantomJS) on Amazon

Even on an Amazon m4.xlarge Linux instance, building PhantomJS from source code can take more than 30 minutes and possibly several hours. Some quick online searches uncovered a very fast and elegant solution that leverages a readymade, docker-ized version of PhantomJS. Simple instructions are available on the Docker Hub.[5]

In mere minutes, it is possible to create a Linux Amazon instance from scratch, update it and install a PhantomJS docker container. The next step: customizing a sample PhantomJS script for loading a web page so it has simple userAgent spoofing (see Line 14 in Figure 26). This customization makes it appear to be a Chrome browser running on a Mac.

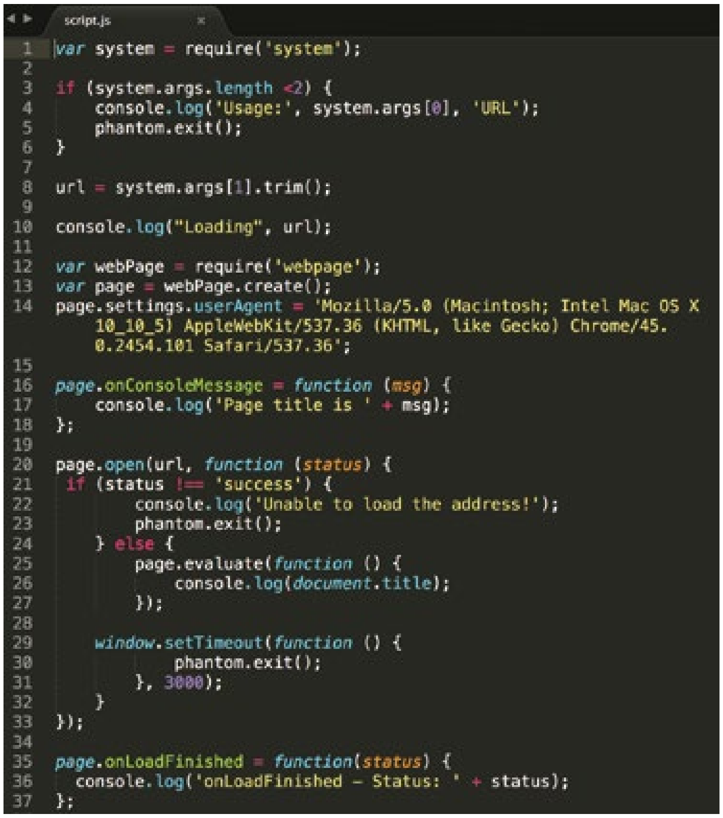
4. Write an automated script for dynamically rotating the headless-browser IP address

The Amazon EC2 API can be used to write a simple script that releases the existing IP address, allocates a new one and associates it with the running instance.

For a sample code, see Figure 26. The next step: executing the script in a loop and writing the IP change to a log file. Figure 28 shows about 25 IP changes of an Amazon instance named "tiny1" over a one-minute period.

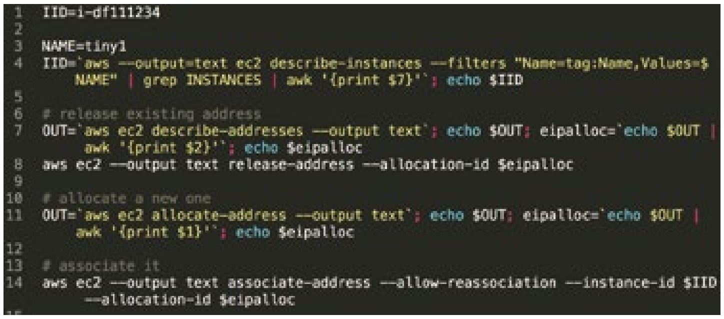
The bottom line? It takes only a few seconds to assign a new IP address to a running host.

After about 15 minutes, the script has been able to generate more than 300 unique IP addresses (see Figure 28).



```
script.js
1   var system = require('system');
2
3   if (system.args.length <2) {
4       console.log('Usage:', system.args[0], 'URL');
5       phantom.exit();
6   }
7
8   url = system.args[1].trim();
9
10  console.log("Loading", url);
11
12  var webPage = require('webpage');
13  var page = webPage.create();
14  page.settings.userAgent = 'Mozilla/5.0 (Macintosh; Intel Mac OS X
        10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.
        0.2454.101 Safari/537.36';
15
16  page.onConsoleMessage = function (msg) {
17      console.log('Page title is ' + msg);
18  };
19
20  page.open(url, function (status) {
21   if (status !== 'success') {
22          console.log('Unable to load the address!');
23          phantom.exit();
24      } else {
25          page.evaluate(function () {
26              console.log(document.title);
27          });
28
29      window.setTimeout(function () {
30              phantom.exit();
31          }, 3000);
32      }
33  });
34
35  page.onLoadFinished = function(status) {
36    console.log('onLoadFinished - Status: ' + status);
37  };
```

Figure 26: Headless browser sample script



```
IID=i-df111234

NAME=tiny1
IID=`aws --output=text ec2 describe-instances --filters "Name=tag:Name,Values=$
    NAME" | grep INSTANCES | awk '{print $7}'`; echo $IID

# release existing address
OUT=`aws ec2 describe-addresses --output text`; echo $OUT; eipalloc=`echo $OUT |
     awk '{print $2}'`; echo $eipalloc
aws ec2 --output text release-address --allocation-id $eipalloc

# allocate a new one
OUT=`aws ec2 allocate-address --output text`; echo $OUT; eipalloc=`echo $OUT |
    awk '{print $1}'`; echo $eipalloc

# associate it
aws ec2 --output text associate-address --allow-reassociation --instance-id $IID
     --allocation-id $eipalloc
```

Figure 27: Dynamic IP allocation using AWS API

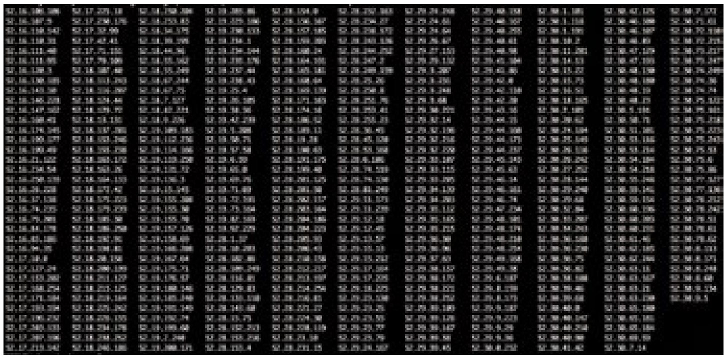
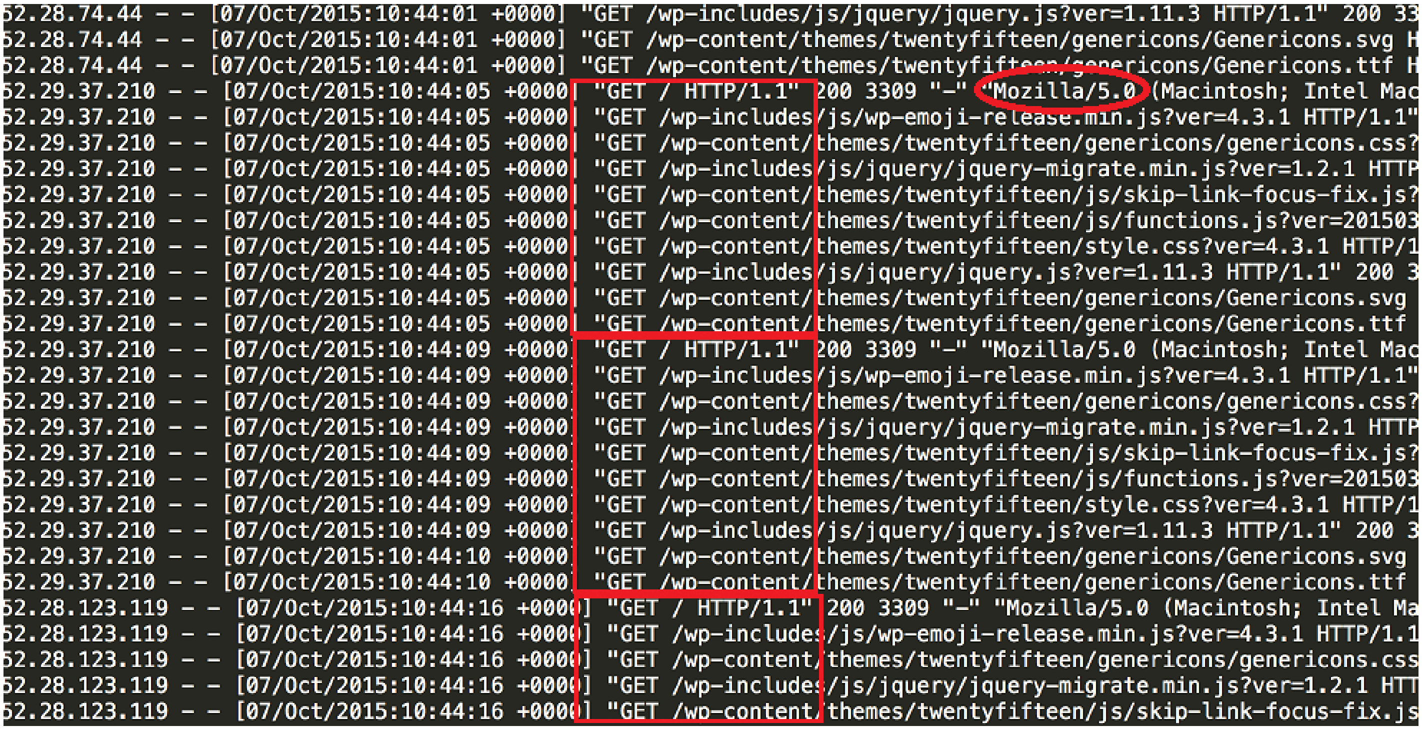


Figure 28: List of dynamically generated IP addresses

[5] Find the instructions at https://hub.docker.com/r/rosenhouse/phantomjs2/

With the ability to easily generate dynamic IP addresses now proven, the next step in the simulation is to conduct tests using the PhantomJS headless browser. Figure 28 shows the Web Server logs of requests coming from the PhantomJS headless browser. PhantomJS renders the JavaScript WordPress homepage—generating about 10 requests per page load. Notice how the client IP address changes between different iterations of a page load.



```
52.28.74.44 - - [07/Oct/2015:10:44:01 +0000] "GET /wp-includes/js/jquery/jquery.js?ver=1.11.3 HTTP/1.1" 200 33
52.28.74.44 - - [07/Oct/2015:10:44:01 +0000] "GET /wp-content/themes/twentyfifteen/genericons/Genericons.svg H
52.28.74.44 - - [07/Oct/2015:10:44:01 +0000] "GET /wp-content/themes/twentyfifteen/genericons/Genericons.ttf H
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET / HTTP/1.1" 200 3309 "-" "Mozilla/5.0 (Macintosh; Intel Mac
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-includes/js/wp-emoji-release.min.js?ver=4.3.1 HTTP/1.1"
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-content/themes/twentyfifteen/genericons/genericons.css?
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-content/themes/twentyfifteen/js/skip-link-focus-fix.js?
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-content/themes/twentyfifteen/js/functions.js?ver=201503
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-content/themes/twentyfifteen/style.css?ver=4.3.1 HTTP/1
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-includes/js/jquery/jquery.js?ver=1.11.3 HTTP/1.1" 200 3
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-content/themes/twentyfifteen/genericons/Genericons.svg
52.29.37.210 - - [07/Oct/2015:10:44:05 +0000] "GET /wp-content/themes/twentyfifteen/genericons/Genericons.ttf
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET / HTTP/1.1" 200 3309 "-" "Mozilla/5.0 (Macintosh; Intel Mac
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-includes/js/wp-emoji-release.min.js?ver=4.3.1 HTTP/1.1"
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-content/themes/twentyfifteen/genericons/genericons.css?
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-content/themes/twentyfifteen/js/skip-link-focus-fix.js?
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-content/themes/twentyfifteen/js/functions.js?ver=201503
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-content/themes/twentyfifteen/style.css?ver=4.3.1 HTTP/1
52.29.37.210 - - [07/Oct/2015:10:44:09 +0000] "GET /wp-includes/js/jquery/jquery.js?ver=1.11.3 HTTP/1.1" 200 3
52.29.37.210 - - [07/Oct/2015:10:44:10 +0000] "GET /wp-content/themes/twentyfifteen/genericons/Genericons.svg
52.29.37.210 - - [07/Oct/2015:10:44:10 +0000] "GET /wp-content/themes/twentyfifteen/genericons/Genericons.ttf
52.28.123.119 - - [07/Oct/2015:10:44:16 +0000] "GET / HTTP/1.1" 200 3309 "-" "Mozilla/5.0 (Macintosh; Intel Ma
52.28.123.119 - - [07/Oct/2015:10:44:16 +0000] "GET /wp-includes/js/wp-emoji-release.min.js?ver=4.3.1 HTTP/1.1
52.28.123.119 - - [07/Oct/2015:10:44:16 +0000] "GET /wp-content/themes/twentyfifteen/genericons/genericons.css
52.28.123.119 - - [07/Oct/2015:10:44:16 +0000] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTT
52.28.123.119 - - [07/Oct/2015:10:44:16 +0000] "GET /wp-content/themes/twentyfifteen/js/skip-link-focus-fix.js
```

Figure 29: Web Server log file showing the headless browser requests

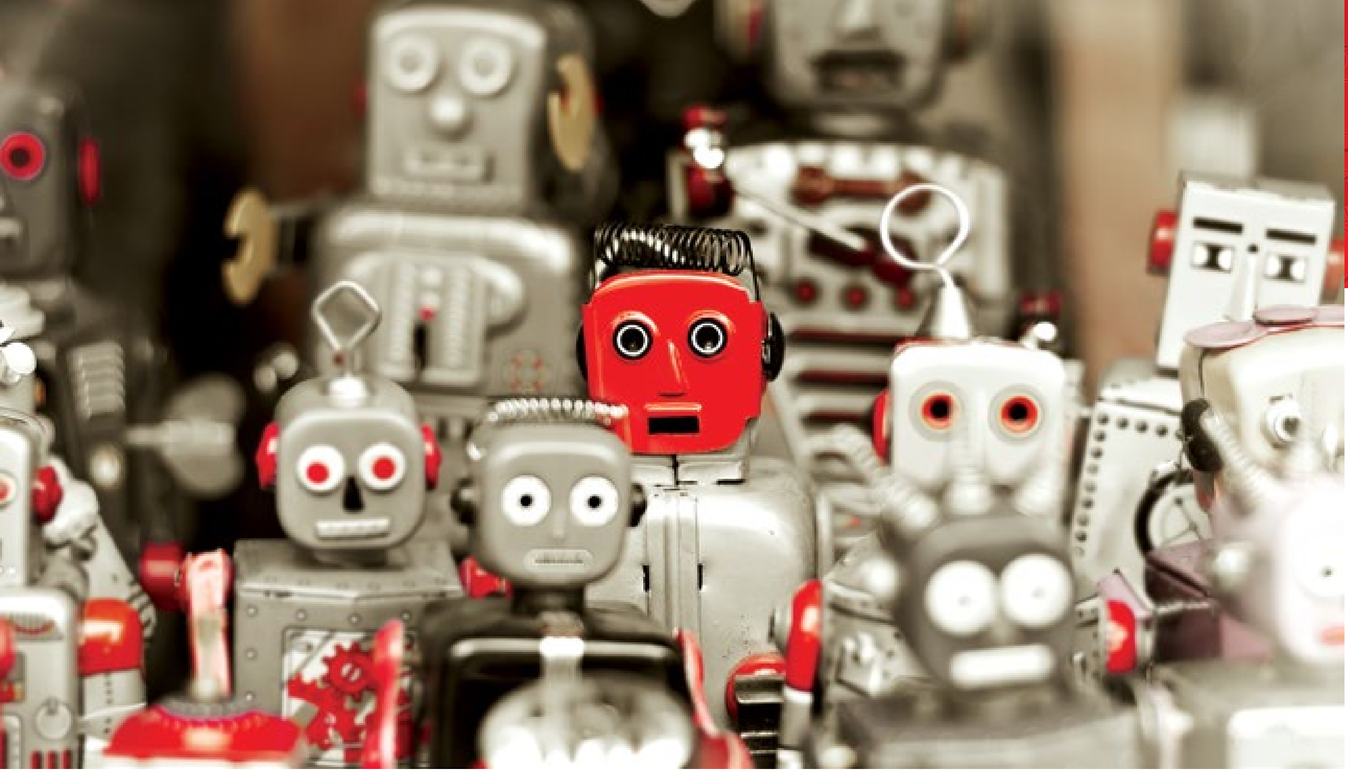
Comparing these logs with lines belonging to real clients, it becomes clear that they are nearly identical. That can be challenging if seeking to block headless browsers that behave like legitimate users.

This test is only one example of the many that can be conducted with a powerful tool such as PhantomJS.

Defending Against Dynamic IP Attacks

It is not unusual for dynamic IP attacks to be overlooked. After all, these attacks are challenging to defend against, and most defense systems are not capable of acting against attacks that so closely resemble real user patterns. Even so, Radware expects focus and attention on these attacks to grow as organizations become more aware of the risks.

If traditional cyber and application protection systems cannot thwart dynamic IP attacks, what can organizations do to protect themselves? The answer lies in advanced defense systems that leverage behavioral-based detection mechanisms. These sophisticated capabilities help in identifying malicious bots, headless browsers and other dynamic IP attacks. Ideally, behavioral-based defense should offer an advanced host fingerprinting mechanism, which goes far beyond IP-based detection to identify—and block—malicious actors in real time.



07

Battle of the Bots: Choosing the Right Weapons

Bot-generated attacks targeting web application infrastructure are increasing in both volume and scope, with the list of attack vectors—and associated risk profiles—growing. This chapter explores the challenges associated with detecting and thwarting bot-generated attacks—particularly the complexity involved in distinguishing the good bots from the bad.

The Good

Not all bots are bad. Various bots and computer-generated traffic are essential to supporting access on the web. Some of the most obvious examples are search engine bots—including Googlebot, Baidu Spider, BingBot and Yandex Bot.There are also other scenarios of legitimate computer-generated traffic. For instance, B2B apps, automated services and provisioning scripts may practically be bots that generate legitimate REST API calls.

> Bot-generated attacks targeting web application infrastructure are increasing in volume and scope. The list of attack vectors—and associated risk profiles—is growing.

The Bad

Bad bots, on the other hand, generate various attacks in support of a variety of objectives. Among the most common: web attacks, such as SQL injections and Cross-Site Request Forgery (CSRF), web scraping, web application DDoS, brute-force attacks on login pages for password cracking, comment spammers, clickjacking and fraud.

Some bot-generated attacks are static; others are dynamic over time. These attacks can also comprise both. For example, a DDoS attack can include a static, and relatively easy to detect, HTTP or HTTPS flood. But it can also be more fluid, with a URL containing dynamic user inputs so that CDNs will forward the dynamic requests to the origin.

The Ugly: Distinguishing Humans and Machines

Bots are not the only vehicle for targeting web applications to achieve malicious objectives. A community of human users can introduce challenges in detecting and mitigating these attacks. How can organizations differentiate human activity from that of a bot or computer? One tool is the Turing test—a test of a machine's ability to exhibit intelligent behavior equivalent to that of a human.

In his 1950 paper, *Computing Machinery and Intelligence*, Alan Turing proposed that a human evaluator would judge natural-language conversations between a person and a machine designed to generate human-like responses. The conversation would be limited to a text-only channel, such as a computer keyboard and screen. If the evaluator cannot reliably distinguish the machine from the human, the machine is said to have passed the test.

In June 2014, the Russian chatter bot Eugene Goostman won a Turing test competition held at the Royal Society of London. During a series of five-minute-long conversations, the bot convinced 33% of the judges that it was human.

In a type of "reverse" Turing test, a computer is expected to determine whether it is interacting with a human or another computer. A common practical implementation of a reverse Turing test is the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

The Ugly: Detecting Advanced Bots

Simple, script-based bots are not much of a challenge to detect and block. The same cannot be said of more advanced bots. Those based on headless browser technology, such as PhantomJS, dramatically complicate the detection process by:

- **Mimicking user behavior**. Using a browser-based plugin, several tools are able to mimic user behavior. Techniques include running JavaScript, downloading images and other referenced content, and following links graphically.
- **Passing challenges**. Some services are relaying CAPTCHA challenges to low-cost human "solvers."
- **Serving up dynamic IP addresses**. Changing the source IP address enables tools to maintain a low rate of activity per IP—thereby evading IP-based detection systems.

Given those challenges, how can organizations enhance detection of advanced bots?

Suiting Up for Battle

One of the most important weapons in the bot battle is IP-agnostic bot detection. Successful detection of attack source requires correlation across sessions. That's because bot-generated traffic may seem harmless—even legitimate—at a discrete, HTTP transaction level. But the continuous nature of these attacks makes them a clear risk.

Consider, for example, a user attempting to log in to a web application and failing to provide the correct credentials for three consecutive attempts. That could be the result of simple human error. But if a bot generates 10,000 such login attempts, it represents an obvious brute-force attack. Detecting the bot requires the ability to correlate bot activities across different transactions and TCP connections as well as from different sources.

It can be highly challenging to correlate bots' dynamically changing IP address behavior with web client activity over time. Not only is IP-based detection insufficient, it may actually conceal the bigger threat picture. Thus, it can prevent prompt detection of the problem and its source. To correlate attack source activity across sessions without relying on the source IP address requires device fingerprinting.

Capturing Distinctive Fingerprints

Device fingerprinting technology offers the ability to identify browsers or automated web client tools through a process of information collection. This technology involves various tools and techniques to identify the web tool. As part of device fingerprinting, some examples of collected information include:

- Operating system specifications (type and version)
- TCP/IP configuration
- Underlying hardware attributes, such as system clock
- Browser-based attributes

Some types of information, such as the TCP/IP fingerprinting, can be passively collected without obvious querying of the client machine. However, browser-based fingerprinting requires active collection of information through client-side script or executable processing. The practical and common means of collecting such information: JavaScript processing on the client side.

While a cookie can be used for in-session tracking, the device fingerprint allows for cross-session, IP-agnostic tracking. Although the identification process is IP agnostic, the geographic and origin context of the web client can be very informative.

Dozens of browser attributes can be collected on the client side to form the device fingerprint. In addition to the user-agent string, JavaScript allows for collection of more detailed browser information—including browser fonts, plugins and screen resolution. While some attributes may seem to be common, the power lies in the consolidation and combination of information, which yields a sufficiently distinct "fingerprint."

That raises an important question: How distinct does each fingerprint need to be? Consider that the current world population estimates 7,370,613,276. Uniquely identifying an individual from the entire population requires 33 bits of information:

$$\log2\ (1/7{,}370{,}613{,}276) < 33$$

Thus, maintaining a fingerprint that can differentiate between 1,000,000 unique users who access the secured environment requires 20 bits of information:

$$\log2\ (1/100000) < 20$$

In its study of modern browser fingerprinting, the Electronic Frontier Foundation (EFF) reported that on average, user-agent HTTP header strings alone contain about 10.5 bits of identifying information. In other words, when choosing a random person's browser, only 1 in 1,500 other Internet users will share that person's user-agent string.

While virtual machines and virtual desktop infrastructures (VDIs) duplicate environments with similar attributes, the standard browser used by a human user usually offers a highly distinctive fingerprint with 18 bits of information.[6] Additionally, although fingerprints tend to change over time, some browser attributes, such as plugins, are more likely to change than others, such as screen resolution. When detecting web attacks, device fingerprints are typically captured over short timeframes of several days—helping ensure the stability of the fingerprint.

Putting Prints to Work

While IP-based tracking of attack sources supports non-intrusive detection, device fingerprint–based tracking offers another level of detection. IP-agnostic source tracking detects bots operating in a dynamic IP environment—and detects activity behind source NAT (sNAT), including enterprise networks and proxies. In other words, even if the bot keeps changing its source IP address, its device fingerprint will not change.

When deploying device fingerprinting technology, it is important to be mindful of varying attributes across different attack vectors. For example, an application DDoS attack may or may not be targeting specific resources. Meanwhile, a data-focused scraping attack is usually targeting specific web pages where information can be extracted. Assess threats and deploy device fingerprinting where it makes the most sense. That could be only in points of interest or risk in an application, or it could be a global implementation across domain resources. Above all, keep "the good" in mind when dealing with "the bad" and "the ugly." The ability to differentiate good bots should be a crucial capability of any device fingerprinting solution.

[6] To test this with your own browser, visit this page: https://panopticlick.eff.org/

08

Hacktivists: Techniques and Attack Vectors

Hacktivists do not see digital boundaries and will stop at nothing to bring down targets in the name of social or political change. When oppressive governments silence citizens, hacktivism can be an important vehicle for driving change. In other cases, hacktivists wreak havoc for more questionable motives. For organizations targeted by hacktivist attacks, the "why" is far less important than the "how" of mitigating and recovering from the technical and reputational damage inflicted by these attacks. With hacktivists now recruiting digital "armies" for their causes, they have become a significant force.

While a lone hacktivist can be problematic, hundreds working together is another challenge altogether. Hacktivists are a problem for more than security personnel. Using just basic techniques, hacktivism can fuel complex challenges for even the most seasoned public relations teams. That's because hacktivists' ultimate motive is often to show the public that a target is not nearly as secure as they had imagined. Hacktivists can successfully cripple networks—and reputations—with simple techniques, such as data dumps and malware. How can organizations combat the hacktivism threat? As with so many challenges, the first step is a better understanding of who they are and how they operate.

Organizing Principles

Most hacktivist operations form when a group of people strongly disagree with a social or political act and decide to take digital action against the target. The group begins by identifying key elements associated with the target and organizing material designed not only to educate the public about the target's actions, but also to incite emotional reactions. The hacktivist group then issues news releases, videos and pastes on a number of different sites about its operation.

In the past, many hacktivists have been arrested. Today's groups have learned from those mistakes, and are now careful to manage the risks as they work to publicly shame and deface a target. While hacktivists remain difficult for many to defend against, the way they organize is generally predictable.

To broaden their reach and impact, these groups issue "new blood" packages with details on how other hacktivists can support the operation. These packages typically have a friendly tone inviting people to help drive change through a variety of means, including making phone calls and organizing people and information. One of the most popular tactics: TweetStorm campaigns. Those who retweet and repost the message—known as "boosters"—help generate awareness among a wider audience. Organizers often run multiple accounts in hopes of amplifying their message.

Ultimately, the actual hackers in the operation deface digital entities, steal and dump data, and launch DoS attacks against the target. Following execution of those plans, operation leaders monitor reactions and outcomes, poised to fan the flames further as needed.

Balancing Privacy and Publicity

Hacktivists are paranoid—and rightfully so, as they risk personal freedom for the causes they support. In the past few years, the average hacktivist has become much more privacy savvy. They learned from the mistakes of others and go to great lengths to maintain anonymity. Among the most common tactics: proxies, virtual private networks (VPNs), Tor and the Invisible Internet Project (i2p) for private communication and browsing. When emailing, most use PGP encryption; for private messaging, they use XMPP services with ORT, TorChat or Bitmessage.

All the while, hacktivists are learning how to mask their attacks using Tor and hidden services, and many are now using full-disk encryption and file encryption as standard operating procedures. Some are even pushing the anti-forensic movement with USBKill and similar tools, which immediately shut down a computer if the USB is removed.

Even as they diligently cover their digital "tracks," hacktivists welcome the chance to communicate publicly about activities. Doing so is crucial to recruiting boosters and followers—yet also introduces the risk of revealing too much information about their next move. Often, hacktivists post lists of targets on websites, such as Ghostbin and Pastebin. These lists may include information about the attack, objectives of the operation and justifications for the attack, along with targeting information and documents, links to tools and instructions on how to use them. To publicize this information, hacktivist groups use centralized accounts on Twitter, Facebook and other social media sites to push information to wider audiences.

Tools of the Trade

In executing attacks, hacktivists use a variety of tools based on skill level. They vary from easy-to-use point-and-click tools with graphical interfaces to scripts and precompiled tools found in a number of distributions, such as Kali and BlackArch.

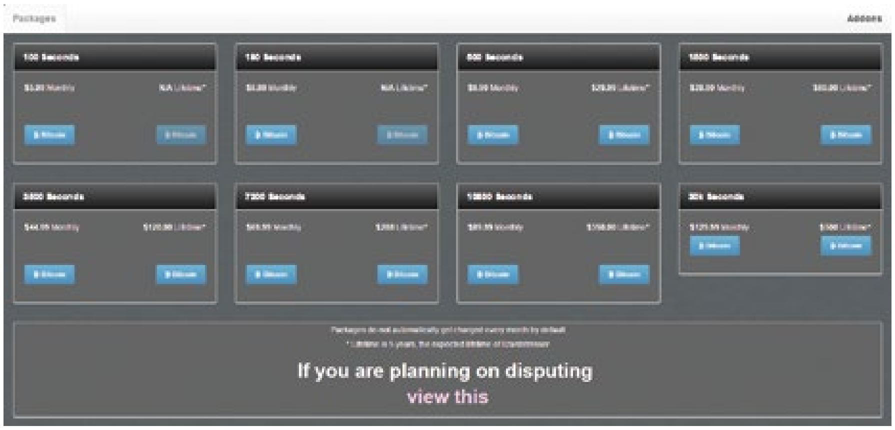
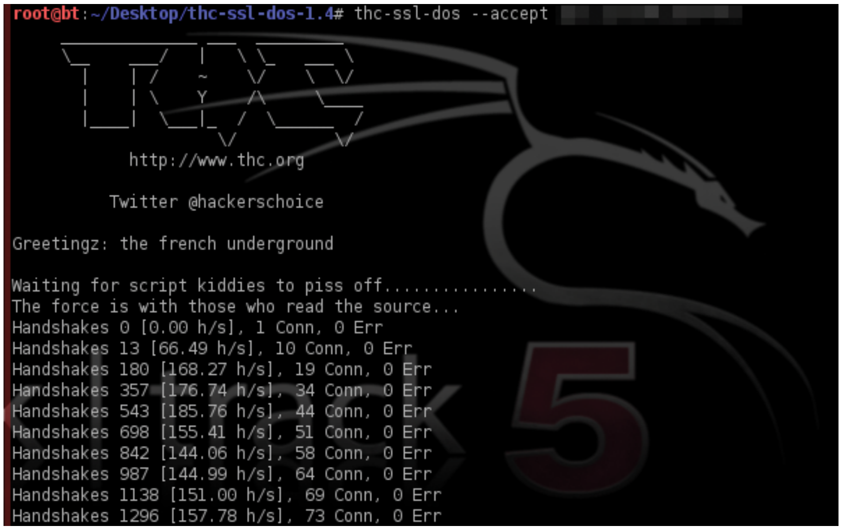


Figure 30: Lizard Squads Lizard Stresser Service

Hacktivists may even use paid services from renting botnets to buying a DDoS attack via stresser/booter services. Many stresser services use multi-vector attacks utilizing UDP, NTP, SSDP, ESSYN, XML-RPC, Chargen, Dominate and SSYN protocols.

Hackers use multi-vector attacks in an attempt to confuse and overwhelm defense measures. Two main vectors of attack are network-based and web application–based attacks. Network-based attacks include DoS, brute force and SSL, among others. Web application attacks, meanwhile, use injection, CSRF and XSS to target a victim's services. These attacks are easy to access, easy to distribute and easier to use. Even the most non-technical person can participate in these types of attacks with little to no knowledge of how the attack works.

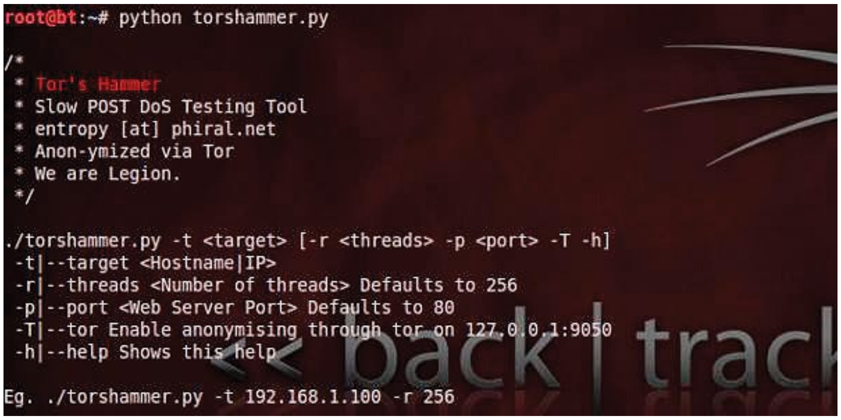
Two main tools hacktivists use: THC-SSL-DOS and Tor's Hammer. These two DoS tools are easy to access and use. THC-SSL focuses on SSL protocol misuse. Tor's Hammer is a Layer 7 tool that can use the Tor network to mask the attacker's origin.



```
root@bt:~/Desktop/thc-ssl-dos-1.4# thc-ssl-dos --accept [redacted]
     ______________ ___  _________
     \__    ___/   |   \ \_   ___ \
       |    | /    ~    \/    \  \/
       |    | \    Y    /\     \____
       |____|  \___|_  /  \______  /
                     \/          \/
            http://www.thc.org

          Twitter @hackerschoice

Greetingz: the french underground

Waiting for script kiddies to piss off................
The force is with those who read the source...
Handshakes 0 [0.00 h/s], 1 Conn, 0 Err
Handshakes 13 [66.49 h/s], 10 Conn, 0 Err
Handshakes 180 [168.27 h/s], 19 Conn, 0 Err
Handshakes 357 [176.74 h/s], 34 Conn, 0 Err
Handshakes 543 [185.76 h/s], 44 Conn, 0 Err
Handshakes 698 [155.41 h/s], 51 Conn, 0 Err
Handshakes 842 [144.06 h/s], 58 Conn, 0 Err
Handshakes 987 [144.99 h/s], 64 Conn, 0 Err
Handshakes 1138 [151.00 h/s], 69 Conn, 0 Err
Handshakes 1296 [157.78 h/s], 73 Conn, 0 Err
```

Figure 31: THC Denial of Service Tool

THC-SSL-DOS is a low and slow attack. A hacking group called The Hacker's Choice (THC) originally developed it as a proof of concept to encourage vendors to patch a serious SSL vulnerability. THC-SSL-DOS, as with other "low and slow" attacks, requires only a small number of packets to cause denial of service for a fairly large server. It works by initiating a regular SSL handshake and then immediately requesting for the renegotiation of the encryption key, constantly repeating this server-resource-intensive renegotiation request until all server resources are exhausted.



```
root@bt:~# python torshammer.py

/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * entropy [at] phiral.net
 * Anon-ymized via Tor
 * We are Legion.
 */

./torshammer.py -t <target> [-r <threads> -p <port> -T -h]
 -t|--target <Hostname|IP>
 -r|--threads <Number of threads> Defaults to 256
 -p|--port <Web Server Port> Defaults to 80
 -T|--tor Enable anonymising through tor on 127.0.0.1:9050
 -h|--help Shows this help

Eg. ./torshammer.py -t 192.168.1.100 -r 256
```

Figure 32: TorsHammer Denial of Service Tool

Tor's Hammer is a slow-rate HTTP POST (Layer 7) DoS tool created by phiral.net. The first public occurrence of this tool dates back to early 2011. Tor's Hammer executes a DoS attack by using a classic slow POST attack in which HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5 to three seconds). Similar to the former R.U.D.Y. (R-U-Dead-Yet) tool, the slow POST attack causes the web server application threads to await the end of boundless posts in order to process them. This causes the exhaustion of the web server resources and causes it to enter a denial-of-service state for any legitimate traffic. A new functionality added to Tor's Hammer is a traffic anonym capability. DoS attacks are executed through the Tor Network by using a native socks proxy integrated in Tor clients. This, in turn, enables attack launch from random source IP addresses, making it nearly impossible to track the attacker.

Web applications are also susceptible to a number of vulnerabilities. Injection and XSS attacks are two of the most popular web application attacks. SQL injections are used to steal protected data. XSS is used to inject client side scripts into web pages. There are a number of easily accessible tools available to aid hacktivists in these attacks—such as Havij, SQLninja, SQLmap, Xenotix, XSSer and a number of other plugins.

SQL injection is a code injection technique used by attackers to steal protected data from SQL databases. The user sends data to execute unintended commands on the system. This can allow an attacker to dump the database. In combination, DoS attacks can mask the data exfiltration from a SQL injection.

Cross-site scripting (XSS) is another type of security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. By inserting JavaScript into trusted sites, attackers can access cookies, session tokens or other sensitive information. Malicious JavaScript inserted into an attack page via XSS can even enlist the users visiting the page into a browser-based botnet.

Here to Stay

Hacktivists are the digital activists of our era, and are not going away any time soon. They can now take a stand on social and political issues on a global scale—without digital boundaries. Arguably, the most dangerous aspect of hacktivism is the intent. While many fight for political and social change, others will use these operations for personal and financial gain.

Importantly, hacktivist groups are not as "leaderless" as they might have everyone believe. Motivation of a group's leaders can be difficult to discern. Leaders could be propagandists, or foreign powers attempting to subvert a group into carrying out an attack for them. However, what all operations share is the exploitation of a "gang" mentality to build momentum and scale—tapping into the social fad and feeding some people's desire to feel important. Expect to see more attacks becoming fully automated, making it increasingly difficult to detect and mitigate. The first step in prevention is to understand how hacktivist operate and evolve. This knowledge will help with preparations for defending networks against future attacks from hacktivists.

Un‘fare’ Advantage: Bots Tie up Airline Inventory

Picture a service counter overcrowded with what appears to be legitimate customers. They only appear to be legitimate because none of them intends to make a purchase; rather their objective is to overwhelm the provider’s resources and prompt other customers to go elsewhere. They succeed—with prospective buyers avoiding the gridlock and spending money with a different provider.

Addressing that kind of competitive tactic in the physical world might be simple enough. In the cyber world, the task is entirely different—and far more complex.

For a major US-based airline, this type of cyber-attack occurred with alarming frequency. Someone had created bad bots, programming them to “scrape” certain flights, routes and classes of tickets. With the bots acting as faux buyers—continuously creating but never completing reservations on those tickets—the airline was unable to sell the seats to real customers. In essence, the airline’s inventory was held hostage, and a growing number of flights were taking off with empty seats that could have been sold.

To its credit, this airline had made significant investments in information security tools and resources. Even so, it found itself unable to distinguish between good bots that help it prosper in e-commerce and malicious ones that were costing it revenue and profit. That’s because many of today’s most severe security threats leverage bots and other traffic sources that can avoid detection by mimicking user behavior. This dynamically changes the source IP addresses or operating behind anonymous proxies and content delivery networks.

In the first half of 2015, this airline's executives made a strategic decision to invest in newer, more holistic technologies. One of the most important capabilities: device fingerprinting technology that could help the airline's systems distinguish good-guy bots from the faux-buyer bots—and thwart the bad bots' attempts to lock up inventory. Device fingerprinting provides a more accurate means of identification than IP address and can be used to block malicious users and whitelist known legitimate users. It also can form the foundation of device reputational information for further security uses.

Similar to this airline, any business that conducts a high volume of online transactions can be a target of bots that exhaust application resources, illegitimately scrape sensitive information from websites and seek vulnerabilities by abusing application logic. To protect applications from advanced bots or even collective human threats, website operators need more advanced user and client identification that can detect and block illegitimate users.

To help combat this threat, companies have been ushering in technology that can track and precisely detect malicious end-user devices regardless of the source IP address. Device fingerprinting generally uses dozens of device characteristics in a unique way to identify and distinguish it from all others. Using this proprietary tracking, a company can generate device reputational profiles that include historical behavioral information to aid in the detection and mitigation of threats—from DDoS and intrusions to fraudsters.

> Device fingerprinting uses dozens of device characteristics in a unique way to identify and distinguish malicious end-user devices regardless of the source IP address.

As this airline discovered, accurate device-level identification enables effective protection from traffic that can elude security measures based on IP address. This includes malicious traffic coming through content delivery networks (CDNs) with whitelisted IPs and traffic using dynamic hosting configuration that results in a new IP address each time the device accesses the Internet. Device fingerprinting can also improve identification of malicious users accessing the Internet through Network Address Translation (NAT) devices that result in many devices sharing the same IP address, and anonymous proxy services that make it difficult to block IPs without potentially blocking legitimate users and devices.

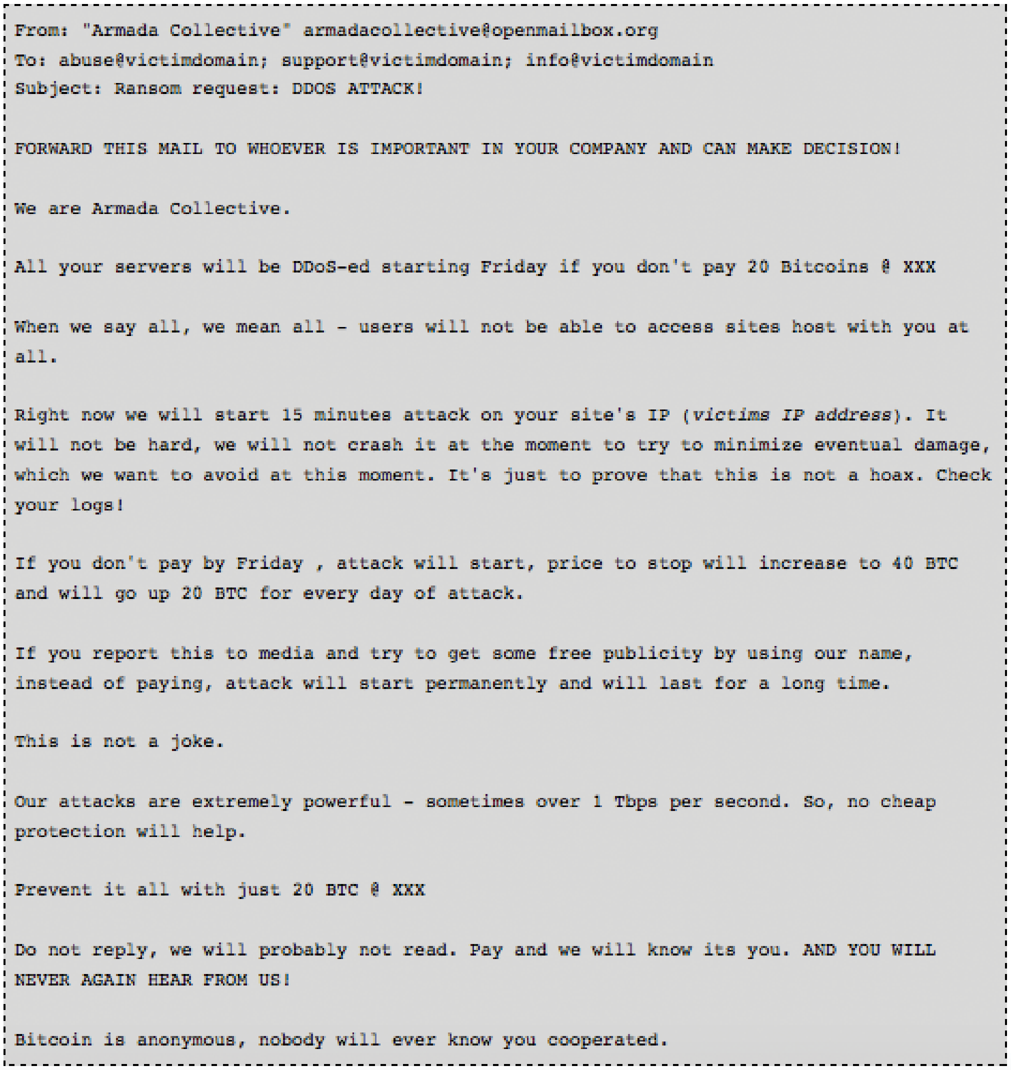
Today, device fingerprinting technology has resolved the airline's challenge—and is helping other e-commerce organizations overcome similar threats from competitors and hackers.

ProtonMail Overcomes Back-to-Back Attacks: Highly Sophisticated DDoS Attack Quickly Follows Ransom Threat

ProtonMail was created to provide privacy to activists, journalists, whistleblowers and other at-risk groups. In November 2015, the Swiss-based encrypted email provider experienced back-to-back attacks from two different sources—one seeking financial gain and another aiming to undercut ProtonMail's central mission. Here is a recap of the series of events and guidance for how any organization can prepare for similar attacks.

Timeline of Events

November 3, 2015 – Slightly before midnight, ProtonMail received a blackmail email from The Armada Collective (see Figure 33). Like DD4BC, The Armada Collective blackmails companies for Bitcoin under the guise of a DDoS attack.[7] In keeping with The Armada Collective's standard modus operandi, following this threat was a DDOS attack that took ProtonMail offline for about 15 minutes.



```
From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at
all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It
will not be hard, we will not crash it at the moment to try to minimize eventual damage,
which we want to avoid at this moment. It's just to prove that this is not a hoax. Check
your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC
and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name,
instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap
protection will help.

Prevent it all with just 20 BTC @ XXX

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL
NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.
```

Figure 33: Example of blackmail email from The Armada Collective

[7] Neomailbox, VFEmail, Hushmail, Fastmail, Zoho and Runbos are among the other email service providers affected by the ransom attacks.

November 4, 2015
11 a.m. – The next DDoS attacks hit ProtonMail's datacenter, and its upstream provider begins taking steps to mitigate the attack. However, within a few hours, the attacks take on an unprecedented level of sophistication.

2 p.m. – The attackers directly assault the infrastructure of ProtonMail's upstream providers and the datacenter itself. The attack on the company's ISP exceeded 100Gbps targeting not only the datacenter, but also routers in Zurich, Frankfurt and other locations where the ISP has nodes. The coordinated assault on key infrastructures successfully brings down both the datacenter and the ISP, affecting not only ProtonMail but also hundreds of other companies.

3:30 p.m. – Under intense third-party pressure, ProtonMail grudgingly pays the ransom to the Bitcoin address 1FxHcZzW3z9NRSUnQ9Pcp58ddYaSuN1T2y. As ProtonMail later noted on its company blog, "This was a collective decision taken by all impacted companies, and while we disagree with it, we nevertheless respected it taking into the consideration the hundreds of thousands of Swiss Francs in damages suffered by other companies caught up in the attack against us. We hoped that by paying, we could spare the other companies impacted by the attack against us, but the attacks continued nevertheless. This was clearly a wrong decision so let us be clear to all future attackers – ProtonMail will NEVER pay another ransom."

November 5 – 7, 2015 – ProtonMail suffers from ongoing, high-volume, complex attacks from a second, unknown source.

November 8, 2015 – ProtonMail begins working with Radware's Emergency Response Team and implements its attack mitigation solution. Service is restored shortly after.

"In order to mitigate the DDoS attack against us, we partnered with Radware, one of the world's premier DDoS protection companies. In Radware, we found a solution that was capable of protecting ProtonMail without compromising email privacy," noted Andy Yen, CEO of ProtonMail. "Given the magnitude of the attack we faced, we knew that we would have to work with the best, and Radware's BGP redirection solution fit our requirements. During our hour of need, there were many companies who attempted to charge us exorbitant amounts, but Radware offered their services at a reasonable rate in order to get us online as soon as possible. With Radware DefensePipe, we were finally able to mitigate the attack on ProtonMail."

November 9 – 15, 2015 – Attacks continue at a high volume, reaching at much as 30Gbps to 50 Gbps at peaks throughout these days. These attacks are successfully mitigated by Radware.

Changing Motivations

In last year's report, Radware cited a rise in cyber hostage taking as one of the most critical information security concerns. Reflecting back on 2014 and looking ahead to 2015: "While there is a long history of cyber ransom activity, 2014 brought a new level of threat in criminal attacks. Nefarious groups have begun taking digital assets or services hostage—commandeering these resources until certain demands, which may or may not be financial, are met. In at least one case, this hostage-taking has led to business failure."

Radware's latest research further underscores that motivations continue to change (though they are still widely unknown). Publicity and outright vandalism are no longer the primary motivators. Instead, attacks are now focused on financial gain, protecting ideological differences, gaining competitive leverage or impacting a war adversary via a cyber-attack.

At 2:34 p.m. on November 15, a short 2Gbps UDP spike occurs and is blocked. A few minutes later, the attack resumes on UDP. Traffic reaches 7Gbps and is again mitigated. By 11:01, attack volume increases to 17 Gbps, reaching up to 40 Gbps. Again, ProtonMail and Radware continue mitigation. The attack vector then changes, with about 10Gpbs hitting infrastructure policy on DP2. Some is matched by DOSS signature DNS reflection, along with ICMP flood; both are successfully mitigated. At 3:20 a.m. on November 16, a short spike of attack, with 150Mbps of traffic coming through was identified and thwarted by Radware.

“We are happy to announce today that after several days of intense work, we have largely mitigated the DDoS attacks against us,” the company reported on its blog on November 10. “These attacks took ProtonMail offline making it impossible to access emails, but did not breach our security. At present, attacks are continuing, but they are no longer capable of knocking ProtonMail offline for extended periods of time. As our infrastructure recovers over the next several days, there may still be intermittent service interruptions, but we have now largely restored all services. Our successful recovery was only possible due to the valiant efforts of IP-Max and Radware, and we would like to sincerely thank them.”

Assessing the Attacks

Following the attacks, ProtonMail worked with MELANI, a division of the Swiss federal government, to exchange information with other companies also attacked. It became clear that the attack against ProtonMail occurred in two stages and was arguably two separate campaigns. The first was the volumetric attack targeting only the company’s IP addresses. The second was the more complex attack targeting weak points in the infrastructure of ProtonMail’s ISPs.

As noted on the ProtonMail blog, “This second phase has not been observed in any other recent attacks on Swiss companies and was technically much more sophisticated. This means that ProtonMail is likely under attack by two separate groups, with the second attackers exhibiting capabilities more commonly possessed by state-sponsored actors. It also shows that the second attackers were not afraid of causing massive collateral damage in order to get at us.”

Lessons Learned

While it is impossible to predict the next target of a ransom group, organizations need to proactively prepare networks and have an emergency plan in place for such an incident. If faced with a threat from a blackmail group, it is important to take the proper steps to mitigate the attack. As ProtonMail’s experiences underscore, organizations under attack should consider:

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe.

- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.

- A cyber-security emergency response plan that includes an emergency response team and process. Identify areas where helped is needed from a third party.

- Monitor security alerts and examine triggers carefully. Tune existing polices and protections to prevent false positives and allow identification of real threats when they occur.

10

Third-Party Viewpoints

To complement the security industry survey and in-the-trenches ERT experience, this year's report includes submissions from two service providers: Atos and Bell Business Markets. Explore their points of view on information security and fresh ways to think about today's challenges.

An ISP Perspective from Atos: Attackers Think About Value—Do You?

Too often security is focused on silos and products. Too seldom does it regard the big picture, which is almost invariably about preserving value or money. Inversely, attackers often seem to have their priorities "straight" with one target in mind; and it isn't the intrusion protection system (IPS) or a server, per se. It's money. Sometimes they pursue that goal through extortion and ransom ("pay us or we take down your web site"). Other times, they sell exfiltrated intellectual property or passwords on the Dark Web. In other instances, they launch a DDoS attack simply to distract security staff while they steal money through illicit digital transactions.

It adds up to an important question: Is tackling security in a piecemeal fashion—focusing on server integrity software, next-generation firewalls, advanced threat detection appliances and so on—the optimal way to erect an impenetrable "wall" of security?

Clearly, security products such as DDoS mitigation appliances must be acquired and implemented. However, it is becoming imperative to approach security by first considering the value that is at stake—and determining how that value could "leak" out of the company. With that understanding, an organization must assume that hackers are already in. The question therefore is not "How do we keep them out?" but rather "How do we know they are in, and what do we do once they are?"

As a managed services provider, Atos continually contemplates, refines and delivers against that query. We recognize that security is about understanding the entire context in which a business operates—knowing where its core and most valuable information is, as well as how to respond to any attack once it occurs.

The history of IT and IT security is full of an evolving series of products designed to keep a company secure. Far more recent is the understanding that detection is insufficient; preparation and remediation are at least as important. In other words, it's not just about avoiding injury, but also stopping the bleeding ASAP.

DDoS attacks offer a prime example. Given the ease with which DDoS attacks can be launched—a fact well illustrated in other parts of this report—the acquisition and operation of world-class DDoS products and services is not optional. Atos offers DDOS mitigation powered by Radware. An Atos customer experienced an attack in excess of 10Gb and we were able to mitigate this attack rapidly, using Radware to both detect and mitigate this attack. For another customer that provides an 'email in the cloud' solution, Atos is using Radware to help protect this email service and ensure that user communications are uninterrupted. Atos is also seeing a continuous uptick in demand for DDOS mitigation services. But it must also be remembered that DDoS attacks themselves are not always the ultimate goal. The goal is often financial: to hold a company to ransom, or to distract security staff while pilfering funds.

The security market is now using terms like "breach detection systems" and "security analytics" to describe how businesses must think about security in 2016. The focus is no longer merely prevention; it's combining information from multiple sources to determine if an attack is occurring, what is at stake, and how to both prioritize and remedy it. This is especially pertinent in today's environment, with highly advanced malware now available for sale, readymade and ready to go—along with attacks that can be extraordinarily complex, requiring months to fully launch and even longer to discover.

Coping with today's style of attacker requires a different kind of approach, which Atos offers to our clients. The starting point is business value—where are the greatest business risks? Many companies might not even know, for example, where their most important documents actually reside physically—on which server(s) and where those server(s) are physically located. Less likely is knowing who has access to those documents, and even less likely still is knowing, with certainty, who has accessed those documents and when.

With a clear understanding of business needs, companies must implement some kind of correlation tool ("advanced analytics"). Correlation has become mandatory because of how modern malware functions—not necessarily intruding or making itself known, but operating just below the radar. Thus, each individual security product may not alert, but the overall picture (one type of behavior or activity in one environment, and a different type in another environment) might require further investigation when seemingly benign activities are correlated together.

Today, Atos supports an integrated security approach, where multiple security information sources, including DDOS, are combined into our SIEM. From the SIEM, Atos provides a variety of additional security management services, including our SOC and CSIRT services.

One reason to invest in security products is not so much to prevent attacks by themselves, but to serve as feeds into the main "security brain," the SIEM. This is not to say that individual tools are not needed or that they aren't as useful as they used to be. In fact, all of these tools are as mandatory as ever—as much of this document shows, DDoS attacks have never been more serious.

But in addition to those tools—and advanced analytics to pull them all together—a world-class defense also requires two other components. The first is a team of experts who actually know what attacks look like in

2016. These are people who work within a security operations center (SOC). They are able to diagnose suspicious activities and separate the noise from the genuine threats. Software can often help here, but software by itself cannot reliably diagnose all situations. The second requirement: practiced, well-rehearsed attack and recovery scenarios. It is not enough to know that an attack is occurring (or has occurred); equally important is knowing what to do next.

A multidisciplinary team can help deliver both of those components. Security and operational personnel will often have specialties (firewalls, day-to-day server management or identity management, for instance), and each individual alone may not be able to understand or remediate the threat. In fact, it would be rare for any individual to be able to identify and then remediate a threat on his or her own. Teamwork is essential since one person may know about networking while another in a completely different role would know about applications. The network pro would not be the person to execute (or even know how to execute) changes to the application to remove the threat.

What companies need are interdisciplinary teams with the experience and know-how to both design and interpret advanced analysis. This core team would be responsible for proactive and reactive risk management processes—seeing warning signs early and then remediating problems once they occur.

When Every Second Counts for Bell Business Markets: Three Keys to Effective DDoS Protection

What do small and mid-sized retailers, large enterprises, financial institutions and government departments have in common online? They're all looking to deliver an exceptional customer experience—one that maintains (and enhances) both brand reputation and consumer confidence. System uptime, application performance and website availability all have a direct impact on the customer experience. When DDoS attacks disrupt those touchpoints, the relationship with the customer is affected. Often, the consequences are severe: loss of trust, loss of sales and even financial penalties due to missed SLAs.

Organizations looking to protect themselves from DDoS attacks—and in a way that limits the amount of latency involved (which can affect mission-critical, time-sensitive transactions)—need to take into account three key considerations:

- Scope of protection
- Speed of processing
- Location of scrubbing facilities

Scope of Protection

An organization needs to be able to detect and mitigate DDoS attacks quickly and effectively. This makes low latency a must-have requirement when looking at DDoS protection services. At the same time, it's important to remember that DDoS attacks can target more than just network bandwidth. As noted in Radware's 2015-2016 Global Application and Network Security Report, network and application attacks occur at similar frequency. This underscores the importance of protection and mitigation capabilities that can defend against all types of attacks.

Speed of Processing

As the scope of detection and mitigation increases, processing speed becomes critically important. When incoming traffic can be inspected with sub-second latency, an organization can ensure a more consistent user experience. Such low latency isn't always possible. In some cases, there will be a need to trade speed for thoroughness, especially with inspection measures that require validation from a transaction request's source to reduce or eliminate false positives. For these organizations, the tradeoff is acceptable, as no one wants legitimate (and often revenue-generating) transactions blocked.

Location of Scrubbing Facilities

Cloud-based scrubbing services offered by third-party providers generally do a good job of filtering any attack traffic sent its way. Yet redirecting traffic to a third-party provider comes with a potentially steep latency cost. Until the border gateway protocol route announcement is propagated, a site will continue to receive attack traffic which could result in network link saturation or server/application failure. If an ISP protects only at the network edge, traffic must be manually redirected from the organization's premises back to the edge, further increasing latency. Moreover, protection is typically limited to what the ISP can see as traffic first enters the network.

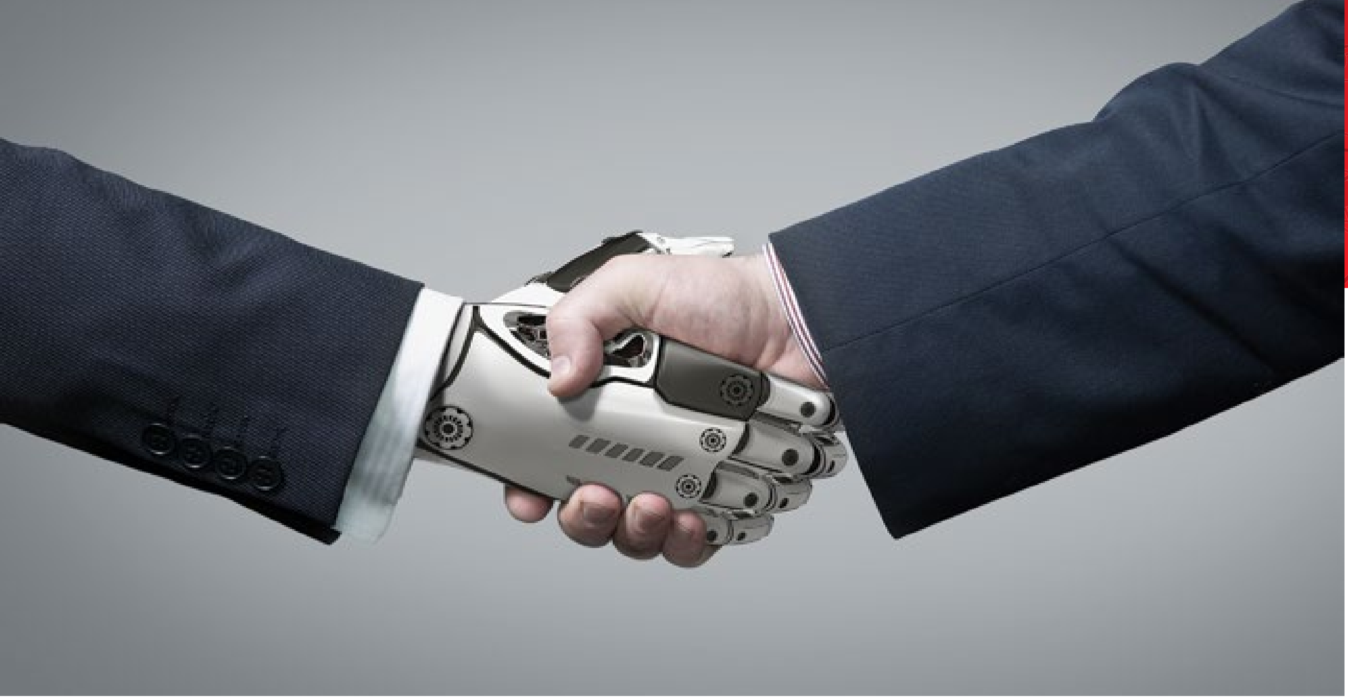
While ISPs that have scrubbing facilities within their core are able to provide in-line, always-on protection, the level of protection offered is typically limited by the bandwidth of its internal network links. The ideal solution is to choose an ISP that has augmented its in-line protection with scrubbing at the network edge, allowing them to detect and mitigate threats wherever it's most efficient to do so—and with significantly less latency than using third-party cloud-based services.

Another consideration is the geographic location of the cloud-based scrubbing facilities, as governments and financial institutions often have requirements to keep traffic within a particular country or region.

How Bell Approaches the DDoS Problem

The best way to defend against DDoS attacks is through a multi-layered solution that offers in-line, always-on protection. If an ISP can offer this capability within its network, it will have the ability to protect its customers from malicious traffic before it can reach its businesses.

Bell Network DDoS Security protects against network, server and application layer attacks, all from within the network core. Its network-based service can be further augmented by managed on-premise deployments, providing more granular defense by enacting additional application-layer protection profiles, botnet detection for outbound traffic and protection from encrypted attacks. With the percentage of encrypted Internet traffic continuing to rise, de-encryption/re-encryption technology is also becoming an increasingly important component of DDoS protection.



11 The Case for Automation

Defenses are succumbing to a dizzying array of attacks and attack techniques. In the face of these realities, it is time to say goodbye to the expectation that humans can deploy detection technologies and choreograph responses, including mitigation, in real time. It is time to fight automation with automation. Here is why.

The pace of attacks is changing. Radware's latest survey showed an increase in attacks that last one hour or less, with more than half of the three biggest attacks falling into that category. This represents a significant increase over the 27% who said the same in 2014. The implication: even long attack campaigns are based on short bursts of traffic—short cycles of attacks repeated over the length of the campaign.

> Say goodbye to the expectation that humans can deploy detection technologies and choreograph responses, including mitigation, in real time. It is time to fight automation with automation.

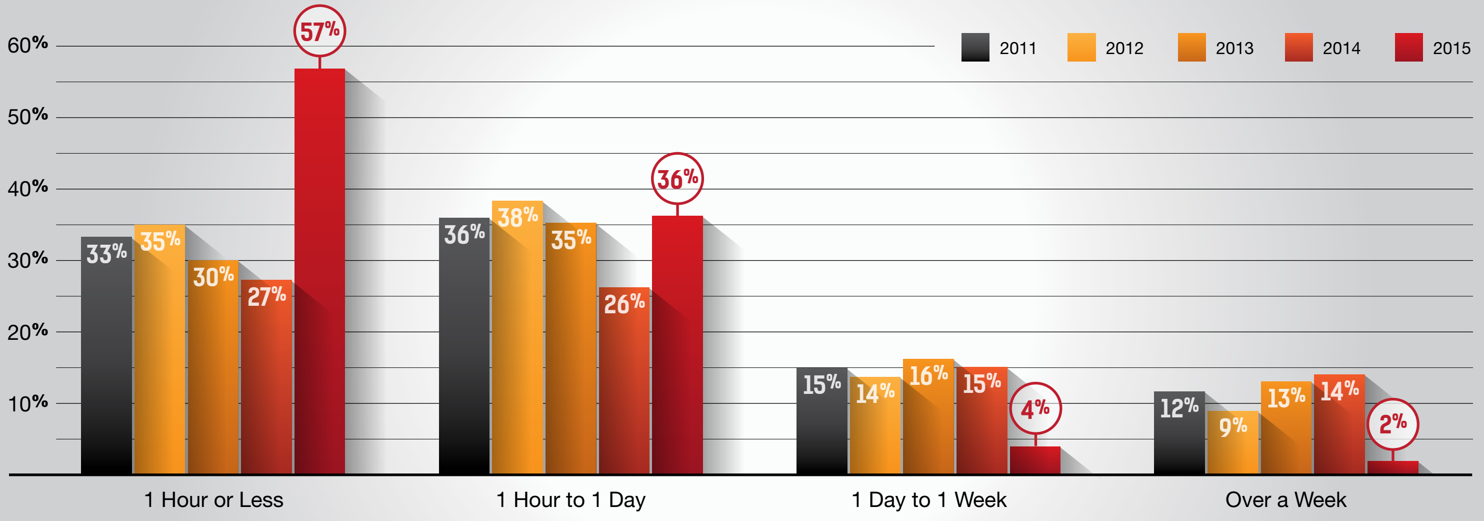


Figure 34: Duration of Cyber-Attacks

This year's survey also found that 91% of respondents are using multiple solutions, with just 6% relying on only one solution against cyber-attacks. This finding does not change by company size, revenue or scope of the business—underscoring that most organizations still rely on multiple and separate solutions to protect their infrastructure and applications.

Which solutions does your organization use against cyber-attacks?

Significantly, existing solutions require a heavy degree of manual intervention to properly configure and protect an organization. Almost three-fifths of survey respondents indicated a medium degree of manual tuning required by its current solution. Some configurations are manual while others are automatic. That points to a big, and dangerous, gap given the increase in fully automated cyber-attacks.

Currently Using	Total
Any Solution	96%
Multiple Solutions in Place	91%
(NET) Single Solution	6%
Firewall	3%
DoS Expert Services	1%
ISP-Based or Clean Link Service	*
On-Demand Cloud Based Service	*
Always-On Cloud Based Service	*
Other	*

* less than 1%

Fall of Human Cyber Defenses. Rise of the Cyberbotted Defense

No one would assert that the design, caretaking or break-fix of information security will be fully automated. However, Radware believes that many of current security professionals' activities will go the way of automation. When focused on superior value delivery, bots will take over a range of functions—including network and application security, compliance, cyber-attack mitigation, incident response, disaster recovery, and identity and access management.

> Many security professionals' activities will go the way of automation. Bots will take over a range of functions—including network and application security, compliance, cyber-attack mitigation, incident response, disaster recovery, and identity and access management.

Why and how could this happen? First is the fact that compelling economics—without the influence of unnatural controls, such as laws, religious values or societal ethics—will always trump perfection and human objections. In other words, if it is cheaper and perhaps more effective, an organization's preference will be to handle a process via automation. Why would a robot be better than a human? It's simple: people cost money and are ubiquitously insecure.

Let us consider the costs of people in bot terms of overt and covert costs—overt in terms of dollars and cents, covert in terms of how security professional can contribute to insecurity.

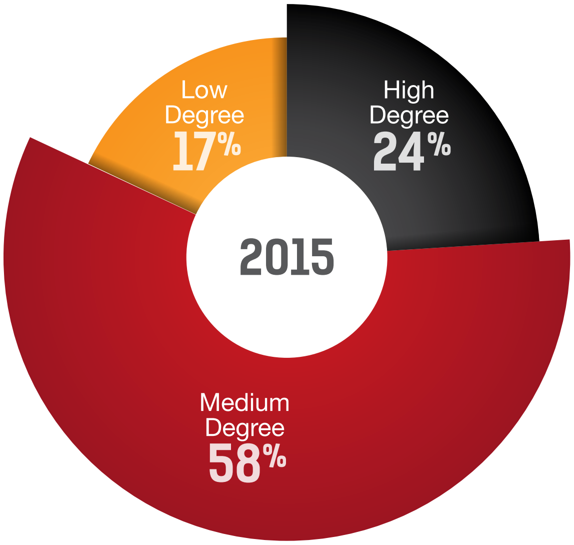


Figure 35: Degree of Manual Tuning or Configuration Required

High Cost of Humans	
Overt	**Covert**
Salaries	Accidents, including socially engineered
Healthcare	Carelessness, including misconfigurations and misdiagnosis of security problems
Benefits	Unavailability of people for sleep, vacations and time off

Robot Returns

- Decreased insurance costs
- Decreased liabilities
- Lower risks
- Fewer violations of security and corporate policy violations

Information security problems have been largely defined by nefarious bots usurping the controls of modest and imperfect security departments. When it comes to detection quality and mitigation speed, humans are simply unable to match highly crafted automated bots. Malicious bots have proven effective—exacting steep tolls on careers, finances and, even the existence of companies themselves.

As costs and concerns reach a crescendo, business executives are met with innovative technologies designed to automate security management. As a result, these automated "white-hat" bots will slowly ebb the tide of hiring security professionals. Over time, bots will prove themselves more effective and more cost effective, eventually replacing security headcount.

In the end, bots will replace security professionals in performing the very processes that originally defined the need for those professionals. Before dismissing the possibility as futuristic or paranoid, consider other industries where bots are becoming vital parts of the workforce:

- **Writing** – many blogs are automated
- **Stock and equity trading** – people no longer make trades at the NYSE or CBOE because they are simply too slow, inaccurate, emotional and unpredictable
- **Legal research** – bots are increasingly mandatory when conducting legal research
- **Drug interactions** – bots are the only way to fully understand potential impacts of multiple medicines

In the realm of information security, what areas are ripest for quick replacement by bots? Startups are coming to market with automated solutions to the following security problems:

- **Compliance**. Spreadsheets and attestations are poised to give way to portals and self-reporting.
- **Security Vulnerability Testing**. Does anyone believe that vulnerability assessments still need to be personalized or that these activities couldn't be automated for higher frequency of testing—and better results?
- **Incident Response**. Latency of human interaction is among the loopholes that today's fast-moving attacks exploit. Automating incident response will close that loophole, diminishing attack effectiveness.
- **Governance**. In time, corporate policies will be fed into tools that monitor the work environment for violations in a continuous and automated fashion.
- **Security Operations**. This area is already under assault. We see decreasing value associated with hiring people to watch detection technology and provide escalations. Soon, these roles will become integrated into automation and orchestration software programs that can quickly react to attacks. Consider the Netflix Simian army or Amazon's use of AWS for examples of how this will work going forward.

In light of these changes, security "wrench-turners" will soon discover that its wrenches have become pixelated. The future is not completely bleak for the security profession, however. Individuals who understand how to implement automation—and excel at orchestrating and managing white-hat bots—will become increasingly in demand. To succeed, initiate or continue the migration to an agile and high-quality detection and mitigation environment that supports customization and self-healing.

12

Summary: Seven Predictions for 2016

Cyber-attacks have become commonplace. In many ways, the only "news" is that they continue to grow in frequency and variety. When dealing with the day-to-day, it can be difficult to tally the mounting toll associated with this awful state of affairs—and even more challenging to predict what surprises could lie ahead. Based on industry trends, legal framework changes, expert insights and technological evolution, Radware makes seven predictions for 2016.

Prediction #1:

APDoS as SOP

Advanced persistent DoS (APDoS) will become hacktivists' preferred technique—and the cause of a significant portion of business outages. APDoS attacks involve massive DDoS attacks, from assaults on the network layer to focused application layer floods. Those attacks are followed by repeated SQLI and XSS attacks, which occur at varying intervals.

Perpetrators of APDoS attacks can simultaneously use as few as two or as many as five attack vectors, involving up to several tens of millions of requests per second. All the while, large SYN floods attack not only the direct target but also the service provider as it implements managed DDoS mitigation. APDoS attacks can persist for weeks at a time—challenging the resources of even the most sophisticated security infrastructures.

APDoS is essentially a potpourri of attack types and thus requires diverse technology to stop everything from network floods and HTTP application-level DDoS to encrypted threats. The ProtonMail case highlighted earlier in this report illustrates the problem vis-à-vis SMTP attacks (a relatively new vector) and secure-SMTP, such as TLS over SMTP. Yet, many companies that have procured DDoS solutions have not thought about the threat from a broader spectrum, such as SMTP or FTP, or from secure variants of those.

When facing a hacktivist campaign, APDoS has become the rule. Attackers in this scenario often switch tactically between several targets to create a diversion to evade defensive DDoS countermeasures while eventually directing the main thrust of the attack on a single victim. When threat actors have continuous access to several, powerful network resources, they are capable of sustaining a prolonged campaign generating enormous levels of un-amplified DDoS traffic.

Prediction #2:

Continued Rise of RDoS

Ransomware and RansomDoS (RDoS) schemes will continue to affect everything from traditional enterprises to cloud companies. It is reminiscent of the old joke: Why do robbers burglarize banks? Because that is where the money is! Cloud companies, beware; we predict you will experience significant RDoS in 2016.

Cloud companies, beware!

We predict you will experience significant RansomDoS (RDoS) in 2016.

Prediction #3:

Privacy as a Right (Not Just a Regulation)

Around the world, privacy's legal comeuppance is upon us. Some countries already recognize privacy as a human right and provide for constitutional covenants to protect its citizens. It's no longer a matter of whether or not data can be secured in pursuit of privacy, but rather if privacy is endemic to the human condition. If privacy is a human right, what must we do to protect and cherish it?

In the meantime, security professionals and businesses entrusted with data will continue to bear the cost and operational responsibility of safeguarding it. They are in the position where they must steward data as best they can, which to some will be an insurmountable challenge. Around the world, early on-boarders lead the way, with this trend picking up toward the second half of 2016.

Prediction #4:

More Laws Governing Sensitive Data

Many countries took notice when the US Government's PRISM program was revealed to the public. Contention exists between normally allied governments when it comes to the handling and use of data and this has given rise throughout the world to special laws governing the use, processing and domiciling of certain data. Some examples include the Canadian government's decree on processing sensitive Canadian data within Canada following U.S. passage of the Patriot Act. Other examples can be found in Brazil, Japan and China—and more will follow in 2016, further complicating the privacy and security officer's responsibility to technically secure data.

Prediction #5:

Arrival of Permanent Denial-of-Service (PDoS) Attacks, Albeit Very Slowly

PDoS, also known loosely as phlashing is an attack that damages a system so badly that replacement or reinstallation of hardware is required. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of the system. It is a contrast to its well-known cousin, the DDoS attack, which overloads systems with requests meant to saturate resources through unintended usage.

PDoS can accomplish its damage via remote or physical administration on the management interfaces of the victim's hardware, such as routers, printers or other networking hardware. In the case of firmware attacks, the attacker may use vulnerabilities to replace a device's basic software with a modified, corrupt or defective firmware image—a process that, when done legitimately, is known as flashing. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced. Other PDoS attacks succeed by overloading battery or power systems.

Prediction #6:

Growing Encryption to and from Cloud Applications

A few years ago, effective technology to secure communication to and from cloud providers and user communities of companies simply did not exist. 2016 will usher in a great capability to encrypt this data en masse. It's a trend that's necessary but also wrought with folly and will ultimately prove a short-term solution to an overall large problem.

Prediction #7:

The Internet of Zombies

Security on Internet of Things (IoT) devices is abysmal—and such data will be breached at a higher rate than any other technical regime. Technical adoption is the paramount concern, and security is clearly an afterthought. These devices represent a cottage industry for privacy violators and 2016 will highlight the risks to this rich data source—transforming the Internet of Things into a dangerous Internet of Zombies.

13 Respondent Profile

In September and October of 2015, Radware conducted a survey of the security community and collected 311 responses. The survey was sent to a wide variety of organizations globally and was designed to collect objective, vendor-neutral information about issues organizations faced while planning for and combating cyber-attacks. All responder profile information is listed below. Please note that not all answers add up to 100%, as some responders may have skipped the question.

Which of the following best describes you and your role at work?

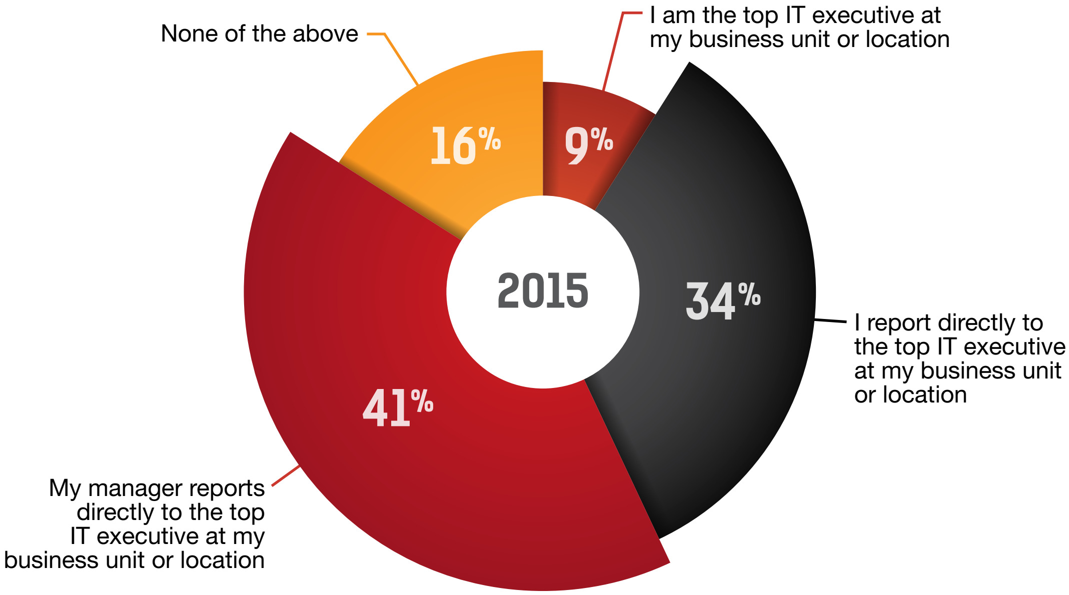


Figure 36: Role Within Organization

Which one of the following best describes your title within your organization?

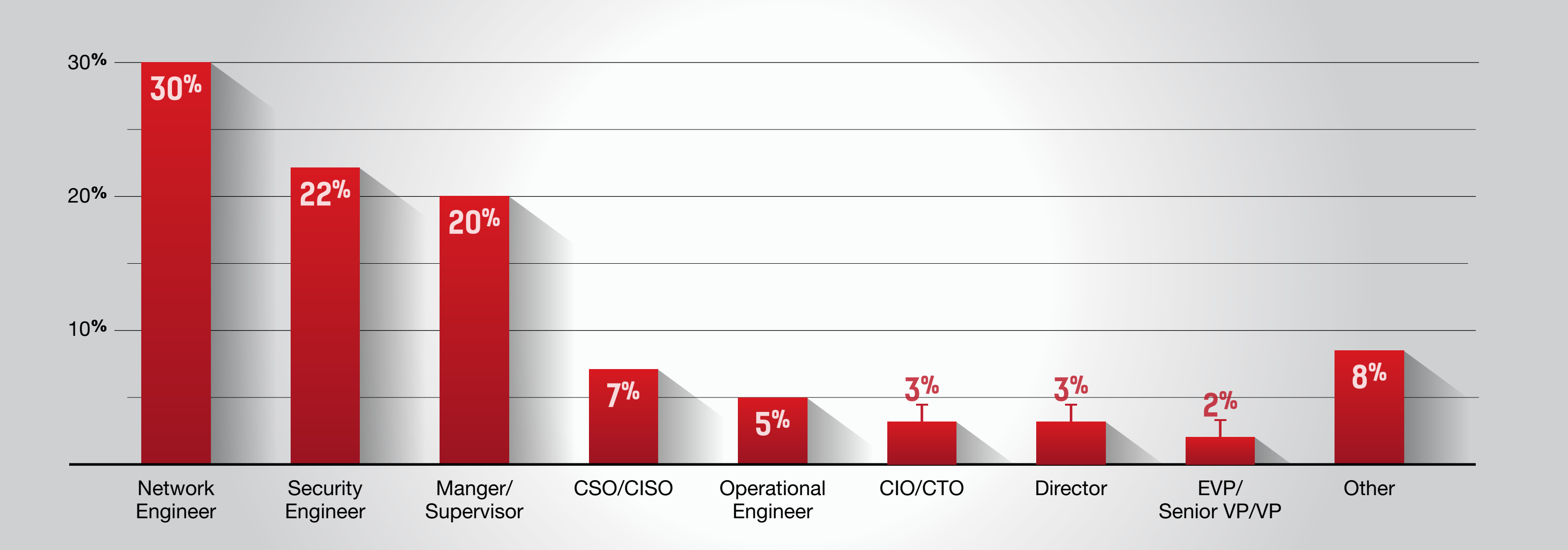


Figure 37: Title Within Organization

In total, how many employees are currently working in your organization?

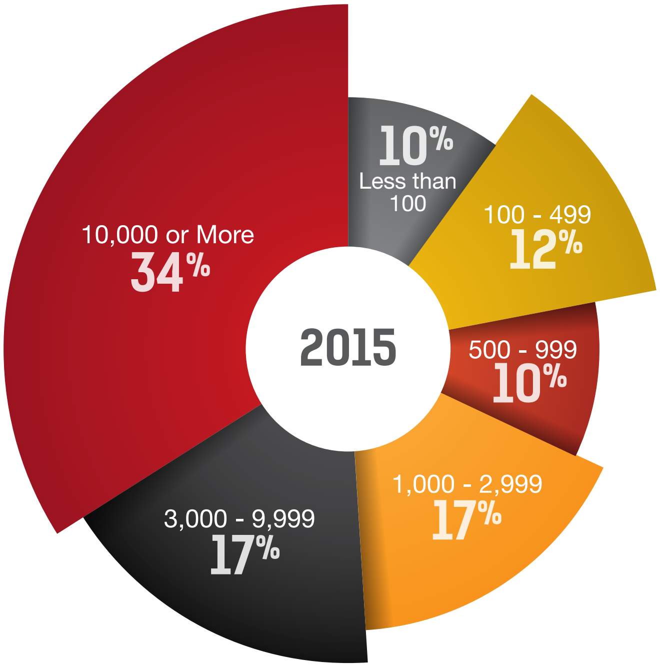


Figure 38: Number of employees in the organization

What is the scope of your organization's business?

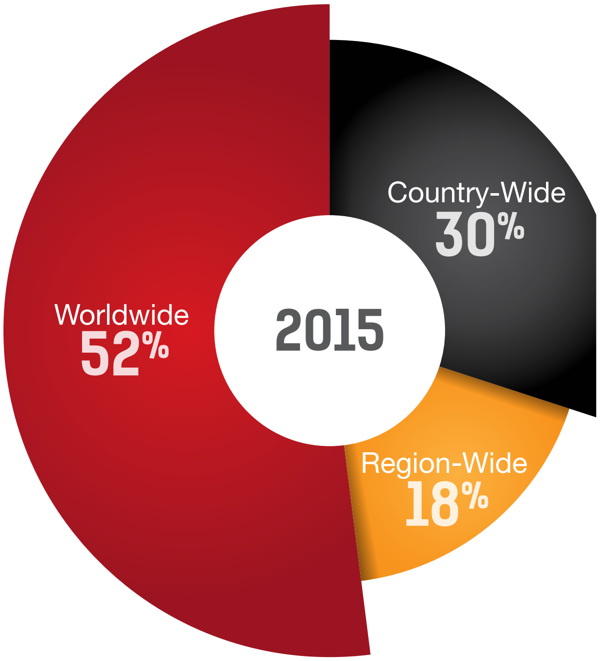


Figure 39: Geographic scope of business

Which of the following best describes your company's industry?

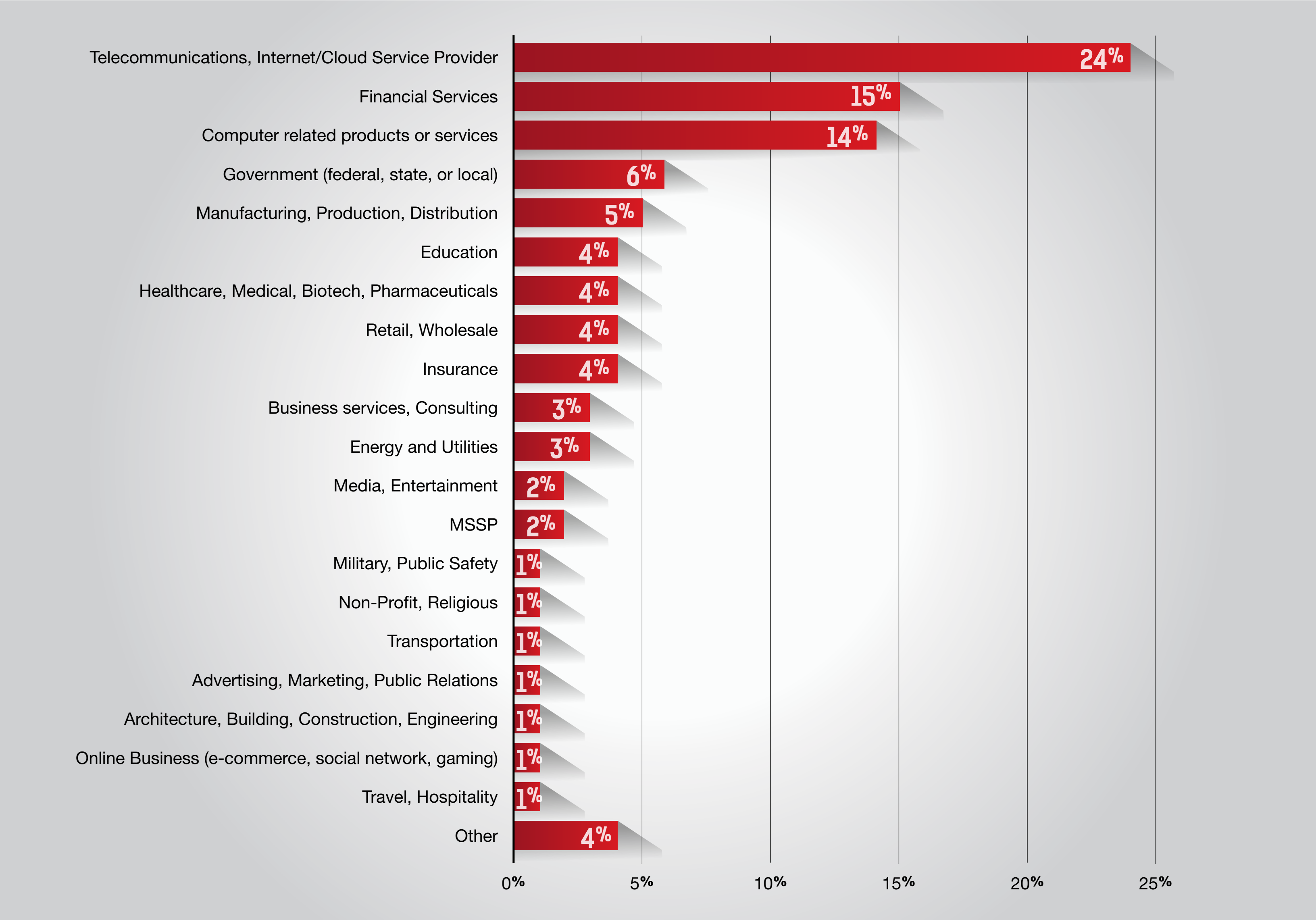


Figure 40: Industry

Regions represented:

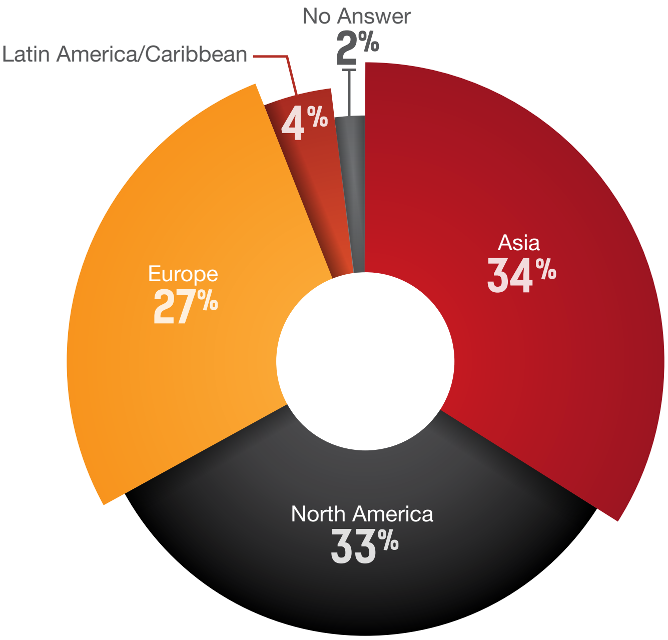


Figure 41: Regions Represented

14 Credits

Authors

Carl Herberger
VP Security Solutions
Radware

Yaniv Hoffman
VP Technical Services
Radware

Michael Groskop
Director, Web Security Products
Radware

Yotam Ben-Ezra
Director, Security Product Management
Radware

Shira Sagiv
Director, Security Product Marketing
Radware

Ben Desjardins
Director, Security Solutions Marketing
Radware

Daniel Smith
ERT Researcher
Radware

Zeev Ravid
Security Research Architect
Radware

David Storch
Cyber Security Portfolio
Atos

Corey Still
Senior Product Manager -
Network and Cyber Security
Bell Business Markets

Advisory Board

Liron Machluf
Director, ERT
Radware

About the Authors

Radware (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency.

Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

About the Radware Emergency Response Team (ERT)

Radware's ERT is a group of dedicated security consultants who are available around the clock. As literal "first responders" to cyber-attacks, Radware's ERT members gained extensive experience by successfully dealing with some of the industry's most notable hacking episodes, providing the knowledge and expertise to mitigate the kind of attack a business's security team may never have handled.

For More Information

Please visit www.radware.com for additional expert resources and information and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats. Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone®

radware

GLOBAL APPLICATION
& NETWORK SECURITY
REPORT

2015–2016

www.radware.com