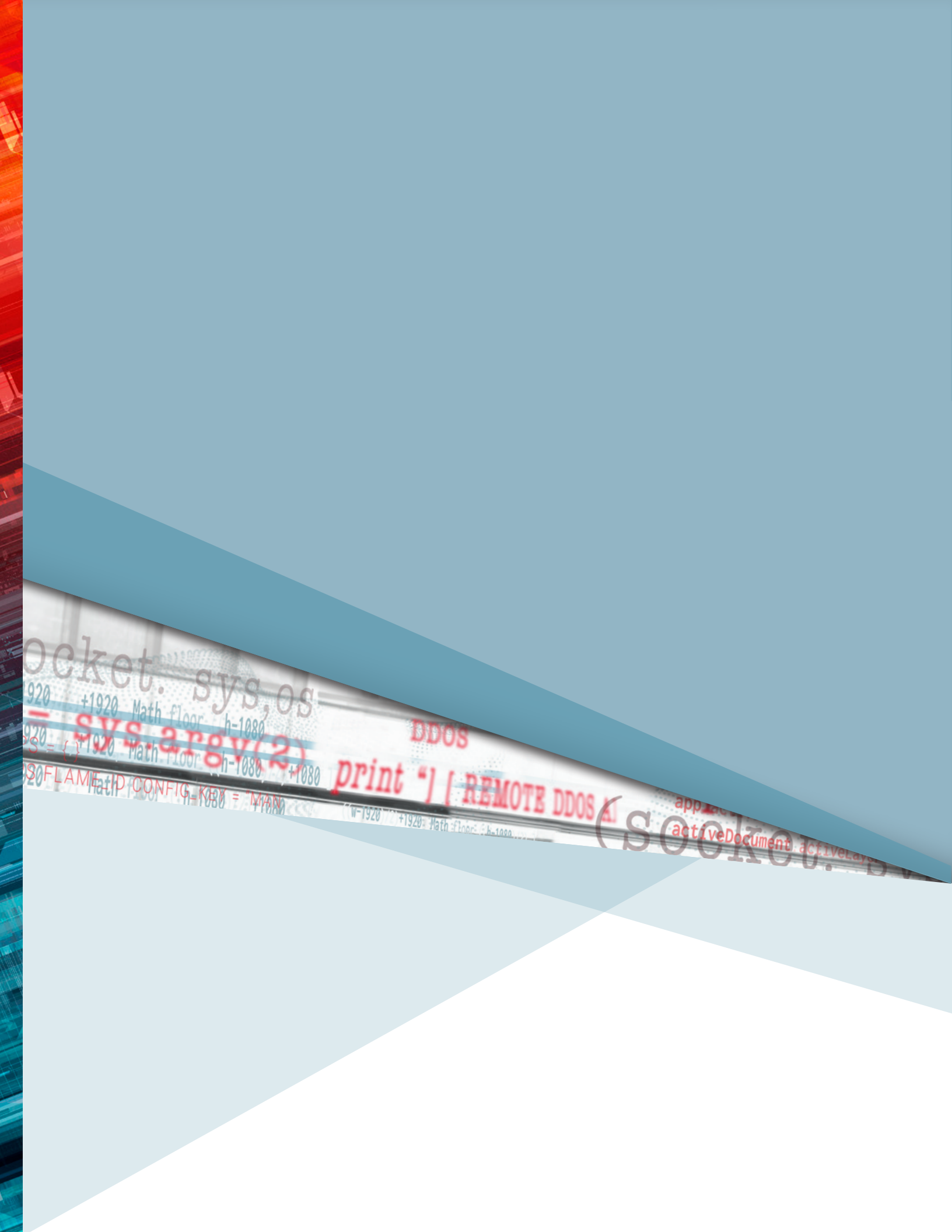


THE TRUST FACTOR

Cybersecurity's Role in
Sustaining Business Momentum





ocket. sys,os

+1920 Math floor h-1080
= sys.argv(2)

DDOS

print "] [REMOTE DDOS AI

920- { } 1920 Math floor n-1080 +1080
920-FLAME Math CONFIG-key = MAN

applic
activeDocument activeLay
(Socket. DA

Table of Contents

Executive Summary	04
Methodology & Sources	06
Dissecting the 2018 Threat Landscape	08
Long-Term Business Impacts of Cyberattacks	18
▶ The Real Costs of Cyberattacks	19
▶ Perceptions of Preparedness	24
▶ Readiness for the Future	29
Analysis of Emerging Risks	32
▶ HTTPS: The Myth of Secure Encrypted Traffic Exposed	32
▶ Time to Take Charge: Ensuring Data Privacy in Public Clouds	35
▶ Adapting Application Security to the New World of Bots	40
▶ Q&A: Looking Past the Hype to Discover the Real Potential of AI	44
Radware Research: Deep Dives	48
▶ What's New in Network and Application Security	48
▶ IoT Expands the Botnet Universe	49
▶ The Rise of Cryptomining	54
Cybersecurity Predictions — 2019	56
Respondent Profile	60
Credits	62

Executive Summary

In 2018, the stakes for cyberattacks were higher than ever. Attention-grabbing data security incidents continued to make news, including the largest distributed denial-of-service (DDoS) attack ever recorded at 1.7Tbps.¹ In the European Union (EU), the General Data Protection Regulation (GDPR) went into effect on May 25, 2018, imposing strict new rules on how personally identifiable information (PII) is collected, processed and controlled. In addition, cryptominers infiltrated networks looking for a quick score.

We've entered a "post-trust" era when organizations and individuals are increasingly wary of accepting promises of security at face value. Every time consumers interact with a brand, they make a judgment about whether they trust a company enough to share their PII. Successful cyberattacks break the trust that companies have worked hard to establish between their brands and customers. Ramifications are no longer the sole responsibility of security professionals; C-suite executives are accountable as well.

To provide insights into the complex challenges faced by organizations as they fight to protect their brands, Radware produces an annual Global Application & Network Security Report. This eighth annual version of the report combines Radware's organic research, real attack data and analyses of developing trends and technologies with the findings from a global industry survey.

The report highlights the business and technology impacts of cybersecurity, including:

- ▶ Lessons learned from recent attacks
- ▶ The true costs of cyberattacks, both quantitative and qualitative
- ▶ An overview of the network and application threat landscape
- ▶ Insights into vulnerabilities of emerging technologies
- ▶ Predictions for 2019

KEY FINDINGS

Balancing the Cost vs. Risk Calculation

Protecting against cyberattacks requires a significant investment that falls on the operating expenses side of the balance sheet. By nature, organizations are always looking for ways to conserve funds. But how much is enough when you factor in the risk of cyberattacks penetrating defenses and impacting businesses?

Consider these revealing insights from Radware's 2018 global industry survey:

- ▶ In just one year, the initial costs attributable to cyberattacks increased 52% to \$1.1 million
- ▶ Organizations that modeled overall costs of cyberattacks to their firms estimated the amount at nearly double versus companies that did not model costs
- ▶ Two in five companies reported negative customer experiences and reputation loss following a successful attack
- ▶ Ninety-three percent of respondents experienced a cyberattack in the past 12 months; only seven percent claimed not to have experienced an attack
- ▶ Cyberattacks were a weekly occurrence for one-third of organizations
- ▶ The primary impact of cyberattacks was service disruption, reported by almost half of respondents. Attacks resulting in a complete or partial service disruption grew by 15% and hurt productivity
- ▶ Cyber-ransom continued to be the leading motivation of hackers and was the reason for 51% of the attacks

¹<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/>

Emerging Attack Vectors

Attackers employ efficient techniques to cause denial of service, such as bursts, amplification, encryption or internet of things (IoT) botnets, and target the application layer to cause more harm.

- ▶ Application-layer attacks caused the most damage. Two-thirds of respondents experienced application attacks. One-third foresee application vulnerabilities being a big concern in 2019, especially in cloud environments. More than half made changes and updated applications monthly, while the rest made updates more frequently, driving the need for automated security.
- ▶ Cyberassaults resulting in a complete outage or service disruption grew by 15%, and one in six organizations reported having suffered a 1Tbps attack.
- ▶ Hackers found new tactics to bring down networks and data centers: HTTPS Floods grew 20%, DNS and Burst attacks both grew 15% and bot attacks grew 10%.
- ▶ A third of companies reported suffering attacks for which they could not identify the motive.

Preparing for What's Next

Businesses indicate that they understand the seriousness of the changing threat landscape and are taking steps to protect their digital assets, but the severity of security threats weighs heavy.

- ▶ Nearly half felt ill-prepared to defend against all types of cyberattacks, despite having security solutions in place.
- ▶ Eighty-six percent of businesses explored machine-learning and artificial intelligence (AI) solutions in the past 12 months. Almost half said that quicker response times to cyberattacks were the motivation. Radware saw a 44% growth in those conducting business over blockchains.
- ▶ Companies continued to diversify network operations across multiple cloud providers. Two in five organizations use hybrid cybersecurity solutions that combine on-premise and cloud-based protection.
- ▶ Forty-nine percent of organizations in EMEA said that they were not well prepared for GDPR.

The Only Option Is Success

The cost of cyberattacks is simply too great to not succeed in mitigating every threat, every time. Customer trust is obliterated in moments, and the impact is significant on brand reputation and costs to win back business. The GDPR and other government regulations have the capacity to bankrupt businesses that do not comply.

It is critical for organizations to incorporate cybersecurity into their long-term growth plans. Securing digital assets can no longer be delegated solely to the IT department. Rather, security planning needs to be infused into new product and service offerings, security, development plans and new business initiatives. The CEO and executive team need to lead the way in setting the tone and investing in securing their customers' experience.



C-Suite Perspective

CEOs Are the New Trust Officers

Cybersecurity is becoming a very personal topic for executives trusted to lead companies at the highest level. To build and maintain solid relationships with customers, CEOs must take on an additional role as “chief trust officer.” When the years of curating a brand strategy can be obliterated with one cyberattack, assigning security strategy to the chief information security officer (CISO) is no longer enough. There is too much at stake.

Consider the fates of CEOs at companies with high-profile breaches such as Equifax, Yahoo, Moller-Maersk and Anthem Healthcare. All of the work that the organizations put into building their brands' value evaporated the moment customers lost trust as a result of the attacks. Before long, the CEOs of most of these companies were “pursuing other interests.”

To ensure cybersecurity is an integral part of the companies' business models, CEOs need to verify efforts and fund protective measures. CEOs who delegate security strategy without oversight do so at their own peril.



Methodology & Sources

The *2018–2019 Global Application & Network Security Report* combines statistical research and frontline experience to identify cybersecurity trends that are important to organizations as they determine long-term growth strategies.

Global Industry Survey

The quantitative data source is a cross-industry survey conducted by Radware. This year's survey included 790 individual respondents representing a wide variety of organizations around the world. The study was built on prior years' research, collecting vendor-neutral information about issues that organizations faced in preparation and combat of cyberattacks.

In this year's survey, 28% of respondents had revenue of \$1 billion or more, while 31% had revenue of less than \$250 million. Responding organizations had an average of about 4,300 employees and represented at least 15 industries. The largest number of respondents worked at service providers/carriers (26%), banking and financial services (17%), high tech products and services (10%), government and civil service (8%), and professional services and consulting (7%). The survey provided global coverage — with 33% of respondents from Asia-Pacific, 31% from North America (U.S. and Canada), and 18% from both EMEA and Central/Latin America (including Mexico). Forty-two percent of respondents' organizations conducted business worldwide.

Radware Threat Research Center

Security experts from the Radware Threat Research Center provide insights on the current and evolving threat landscape.



Emergency Response Team (ERT)

The team is composed of dedicated security consultants providing 24x7 security services. In the event of cyberattacks, ERT members serve as the first line of defense. They have successfully dealt with some of the industry's most notable cyber episodes and other attacks. This report shares their insights from frontline experiences, providing deeper forensic analysis than surveys or academic research alone.



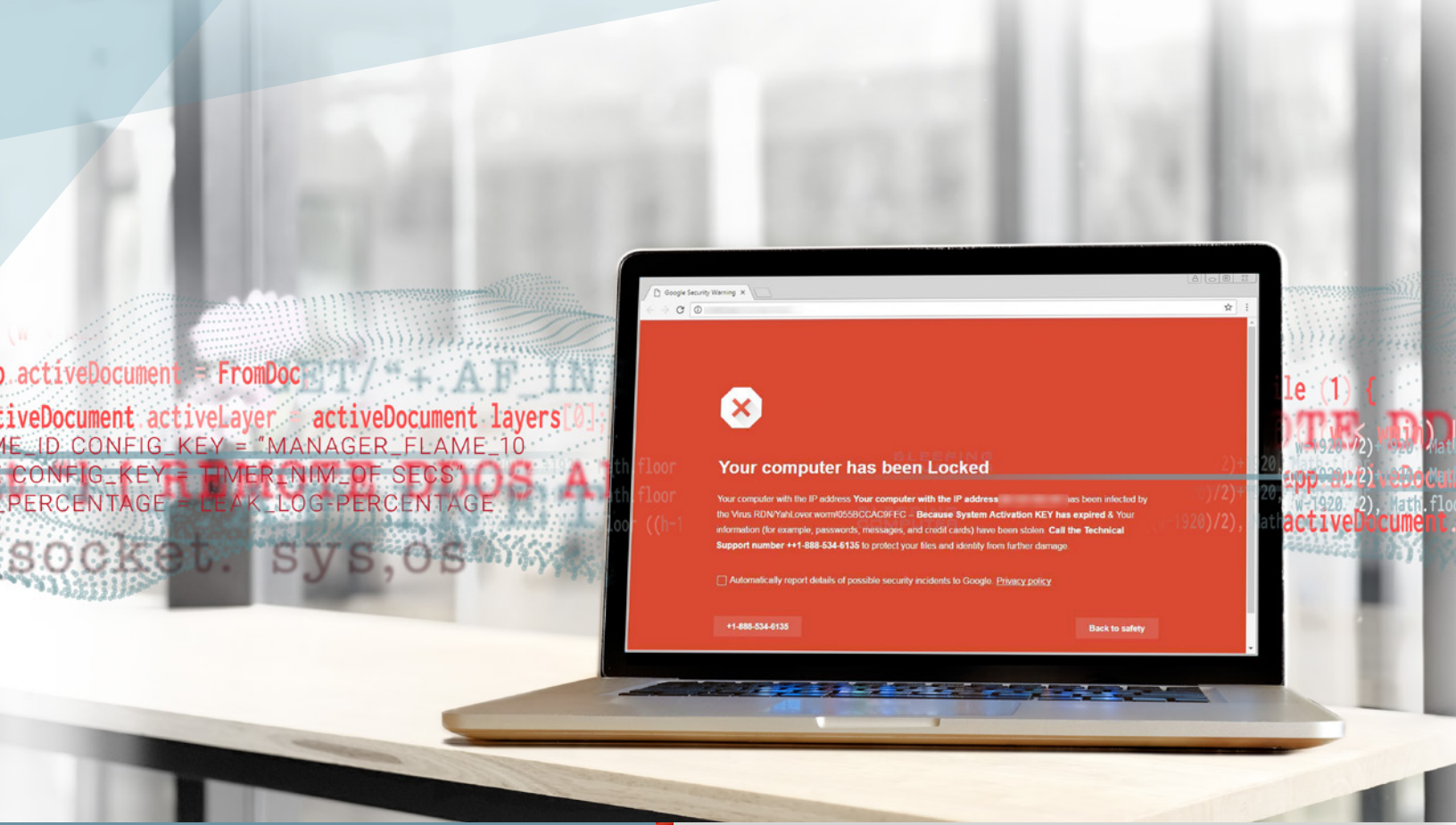
Malware Analysts

Radware's team of malware analysts includes skilled threat researchers and reverse engineers who monitor hundreds of new malware samples every week and issue security advisories based on their findings. Radware's malware analysts examine the samples in research labs to evaluate the malware's evasion, propagation and infection techniques. This team powers Radware's Cloud Malware Protection Service and has collaborated with leading technology organizations to stop malware distribution.



Global Deception Network

Radware's Global Deception Network is a global network of honeypots and detection agents that trap network and application attack campaigns as they emerge. Every hour, the agents communicate with thousands of IPs performing suspicious or malicious activity, such as DDoS and web application attacks, scanners, IoT botnets and more. Radware's advanced algorithms learn threat patterns and intentions, qualify them and feed them in real time to Radware's security solutions for preemptive protection. This report features the top threats caught in Radware's Global Deception Network during 2018.



Dissecting the 2018 Threat Landscape

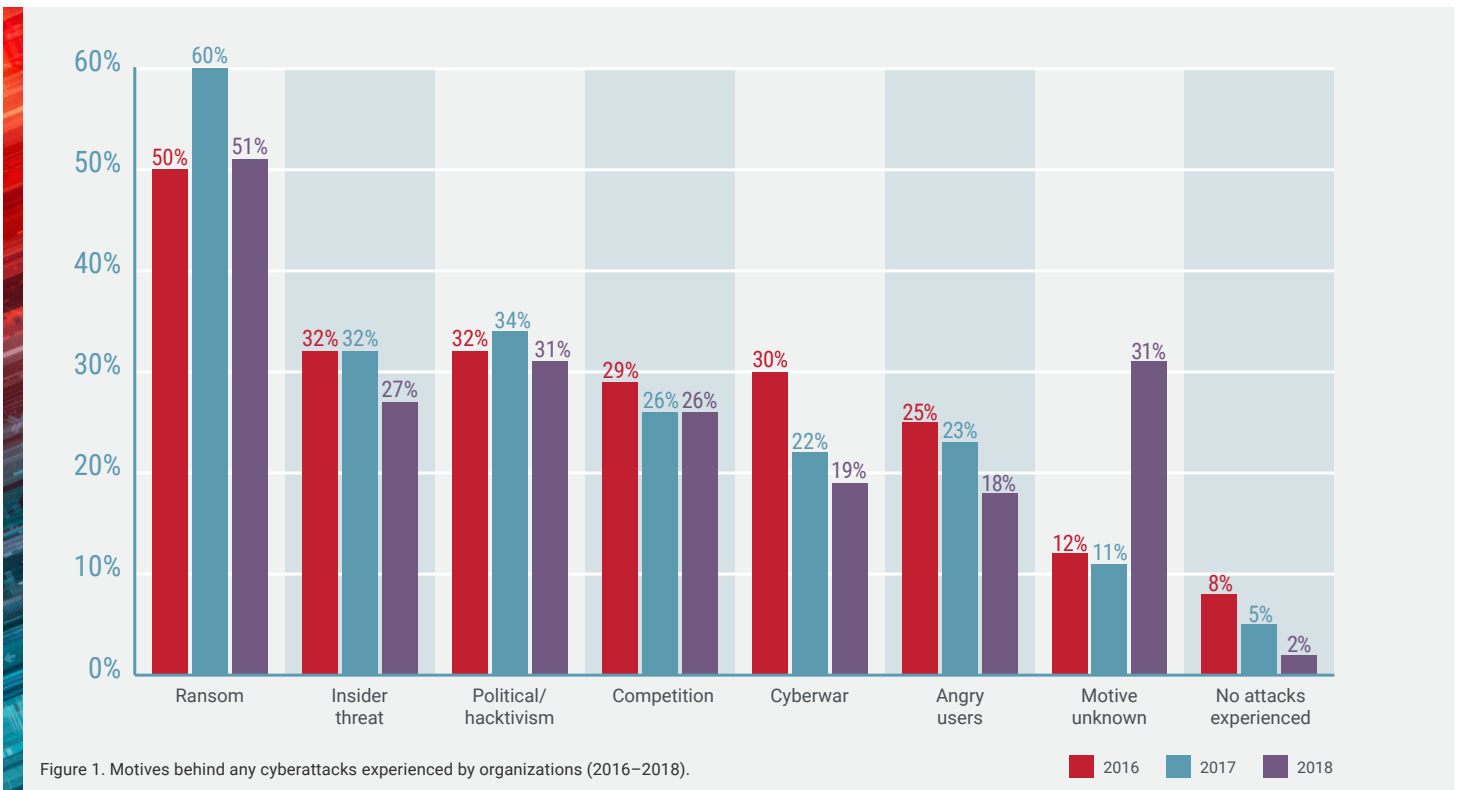
Cyberattacks continued to make headlines in 2018 as organizations faced constant evolving threats. Radware's global industry survey revealed what businesses were up against as they fought to secure their networks and protect the customer experience.

Digital transformation is a double-edged sword. As corporations seek ways to increase productivity and efficiency, advances in network technologies can add agility to business operations. At the same time, cyberattackers are keeping watch, discovering new vulnerabilities to threaten network assets. The Radware global industry survey uncovered the frequency, types and consequences of cyberattacks in 2018, along with hacker motivations.

Ninety-three percent of respondents experienced a cyberattack in the past 12 months. Only seven percent claimed not to have experienced an attack. It is not a matter of if but when an organization will be attacked. The detection and mitigation of cyberattacks needs to be built into every step of the business life cycle.

Why Are Businesses Attacked?

A puzzling piece of data emerged from this year's survey. While the motivations for attacks remained fairly consistent year over year, the responses for "motive unknown" almost tripled in 2018 (see Figure 1). Radware believes it is becoming harder for organizations to distinguish malicious traffic from legitimate traffic as a result of growing incidences and evasive disguise tactics. In some cases, such as cyberwarfare, threat actors are purposeful about hiding their motives.



Notable differences in motives for attacks emerged in different regions of the globe (see Figure 2). For example, financial ransom was 10 points higher in EMEA than the worldwide average.

Have Experienced a Cyberattack in Past Year	Total	REGION			
		USA/Canada	APAC	EMEA	CALA
Financial/ransom	51%	52%	48%	61%	43%
Political/hacktivism/social	31%	27%	30%	32%	37%
Insider threat	27%	28%	29%	22%	30%
Competition/espionage	26%	26%	28%	29%	20%
Cyberwar/geopolitical conflict related	18%	22%	17%	21%	12%
Angry users	18%	20%	12%	19%	23%
Motive unknown/other	31%	36%	30%	32%	24%
Have not experienced any cyberattacks	2%	2%	2%	4%	1%

Figure 2. Motives for cyberattacks on organizations vary by region.

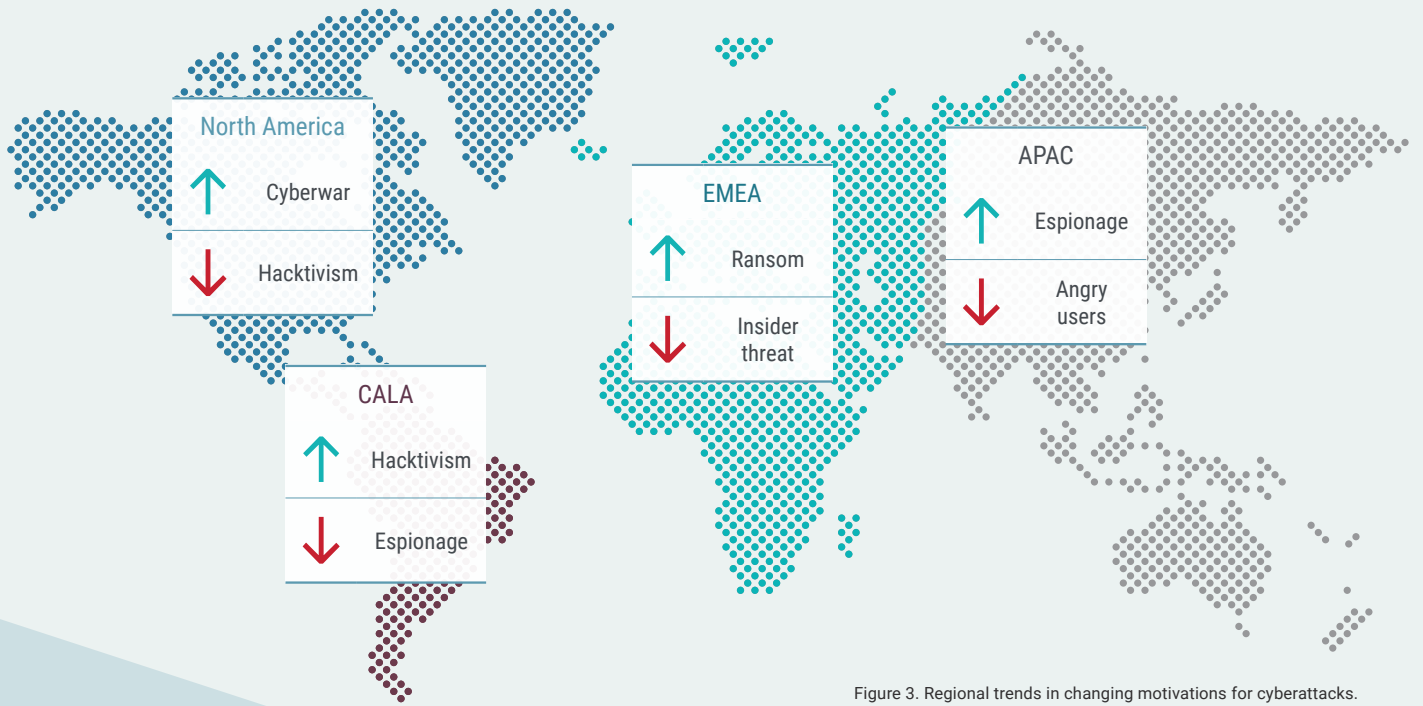


Figure 3. Regional trends in changing motivations for cyberattacks.

How Often Are Businesses Attacked?

One in five respondents reported being attacked daily, a 62% increase over 2017 (see Figure 4). One in five respondents also did not know how often or if they were attacked, which is concerning. The significant reduction in firms reporting attacks once or twice a year, or never, from 2017 indicates they are likely being attacked more frequently.

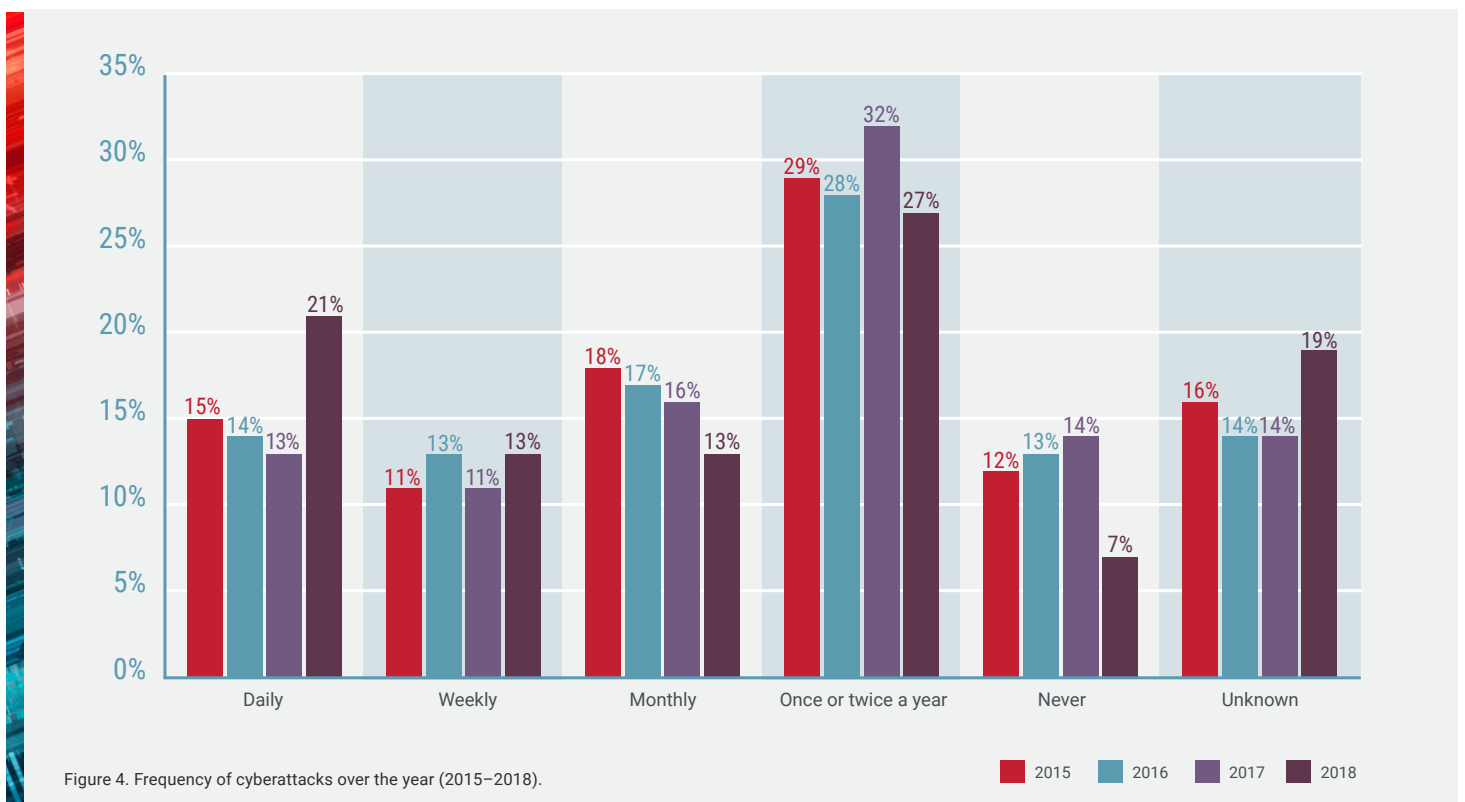


Figure 4. Frequency of cyberattacks over the year (2015-2018).

2015 2016 2017 2018

When broken out by vertical markets, government entities were hit most frequently, on a daily or weekly basis, followed by healthcare and retail (see Figure 5). One-quarter of service providers were attacked daily, likely by hackers hoping to cause service disruptions to internet infrastructure.

Significantly, 20% of all respondents had no idea how often they were targeted. Forty percent of education respondents believed they were rarely attacked.

	Total	Financial Services	Service Prov. & Telecom	Education	Government	Healthcare*	Retail*	High Tech
Daily/weekly	34%	34%	33%	25%	45%	39%	35%	29%
Daily	21%	19%	25%	15%	27%	21%	22%	15%
Weekly	13%	15%	8%	11%	19%	18%	13%	14%
Monthly	13%	12%	13%	16%	9%	15%	17%	14%
Once or twice a year	27%	27%	26%	38%	25%	21%	39%	28%
Never	7%	8%	7%	2%	6%	6%	9%	9%
Unknown	19%	18%	21%	18%	14%	18%	0%	20%

Figure 5. Frequency of cyberattacks in the previous 12 months by vertical markets.
 *Note: Percentages are based on a smaller sample size.

What Kinds of Attacks Are Businesses Experiencing?

Survey results revealed a significant increase in malware/bot attacks and steady growth in socially engineered threats and DDoS. The significant drop in ransom threats is in line with the shift Radware sees as attackers are now more focused on cryptomining. Forty-four percent reported being a victim of either ransom or cryptomining; 14% suffered both.

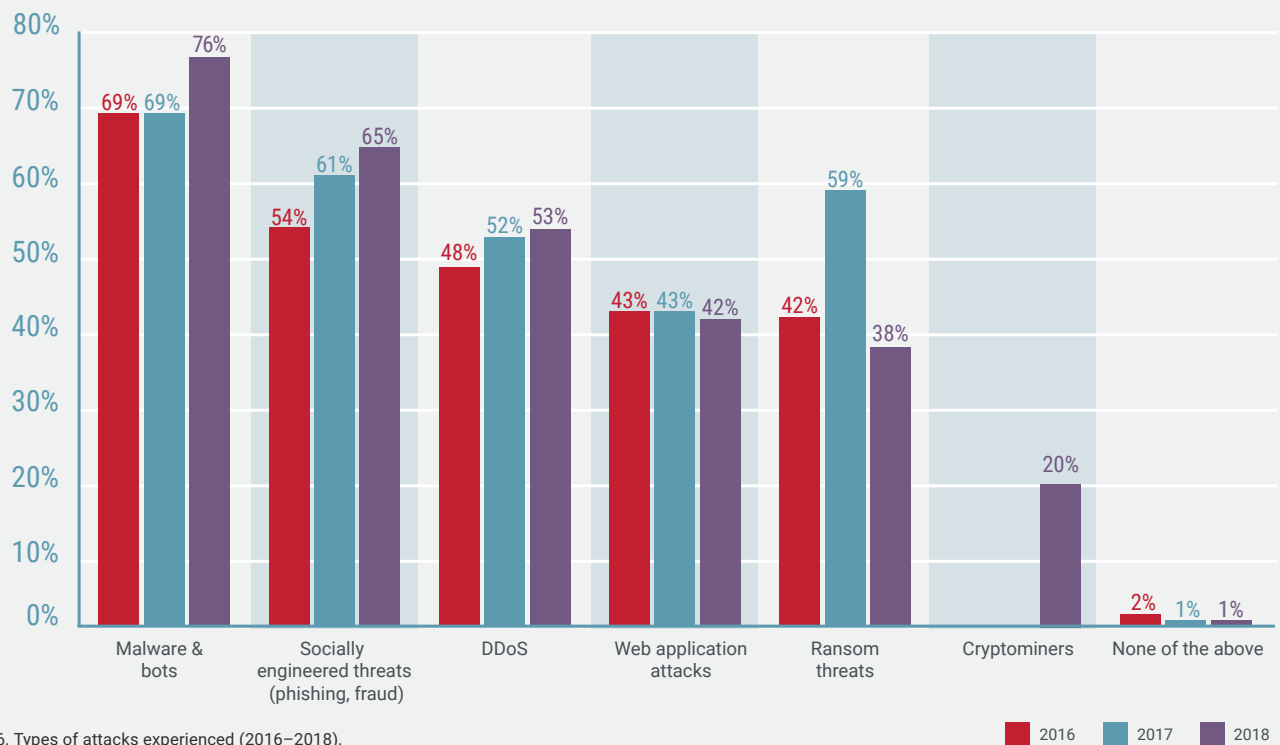
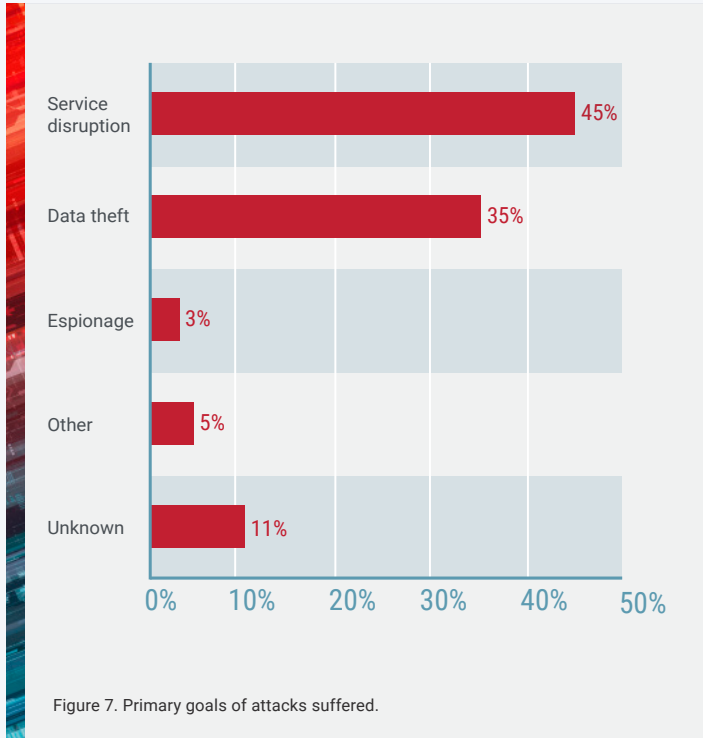


Figure 6. Types of attacks experienced (2016–2018).



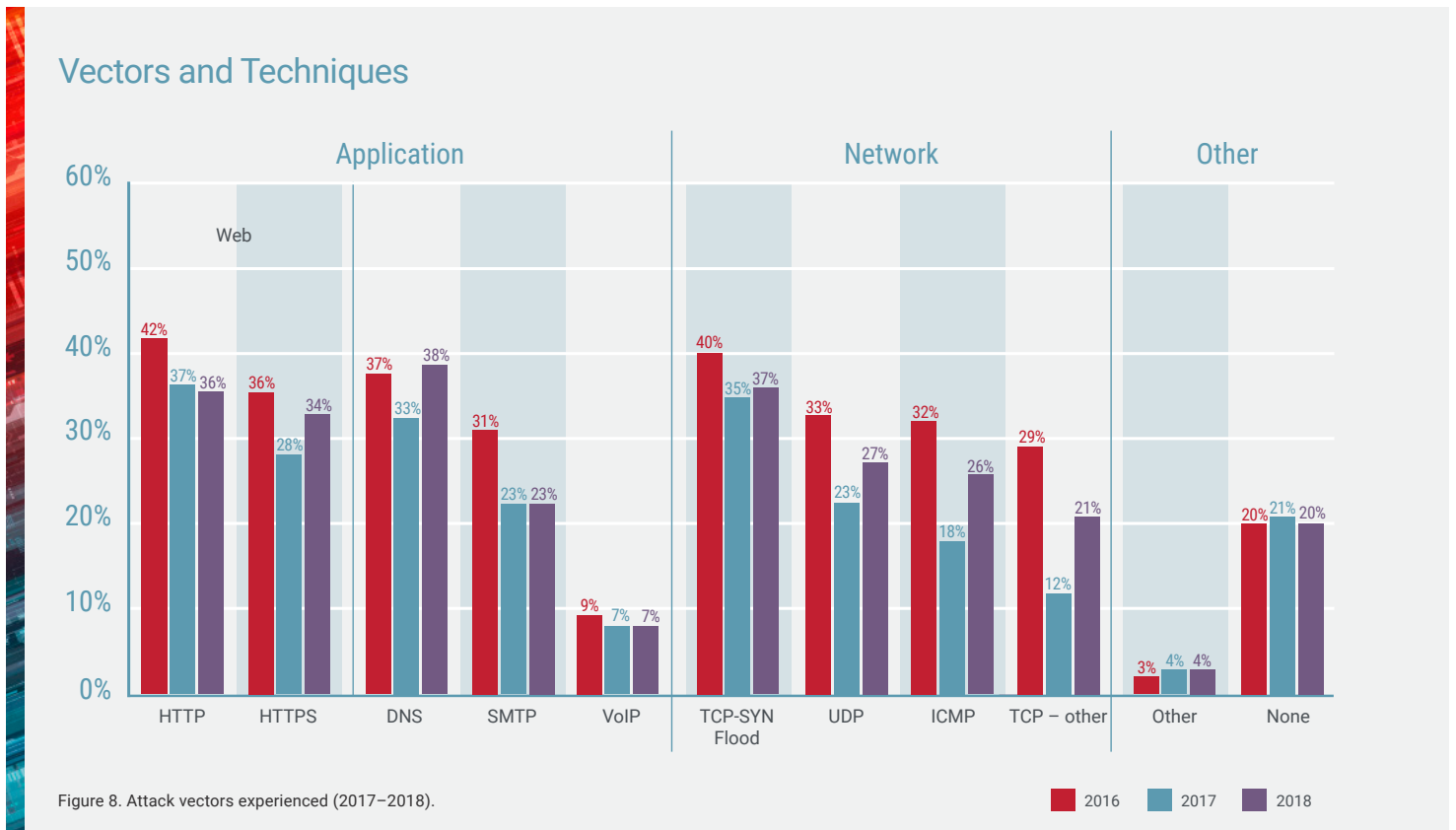
What Is the Ultimate Goal of These Attacks?

In the two most popular types of attacks, organizations are either harmed by service disruptions or the theft of data. Radware sees a trend with more attackers focusing on causing harm as the main goal of their attacks. They want to negatively impact an organization’s customer experience by disrupting network services or the data center.

Vectors and Techniques

Hackers employ a variety of vectors and techniques to launch application or network attacks (see Figure 8).

Denial-of-service attacks can come in two forms: volumetric (DDoS) and nonvolumetric, aimed at exhausting the resources of the target server of application. Typically – but not always – DDoS attacks cause traffic floods that congest the capacity of the targeted network or server and prevent legitimate users from accessing them. While traditionally these floods were generated at the network level (Layers 3–4 of the OSI model – UDP/TCP Floods), in 2017, the application layer emerged as the preferred vector. In 2018, the application layer is still a target, but network-layer DDoS attacks are back on the rise, growing 12% year over year.

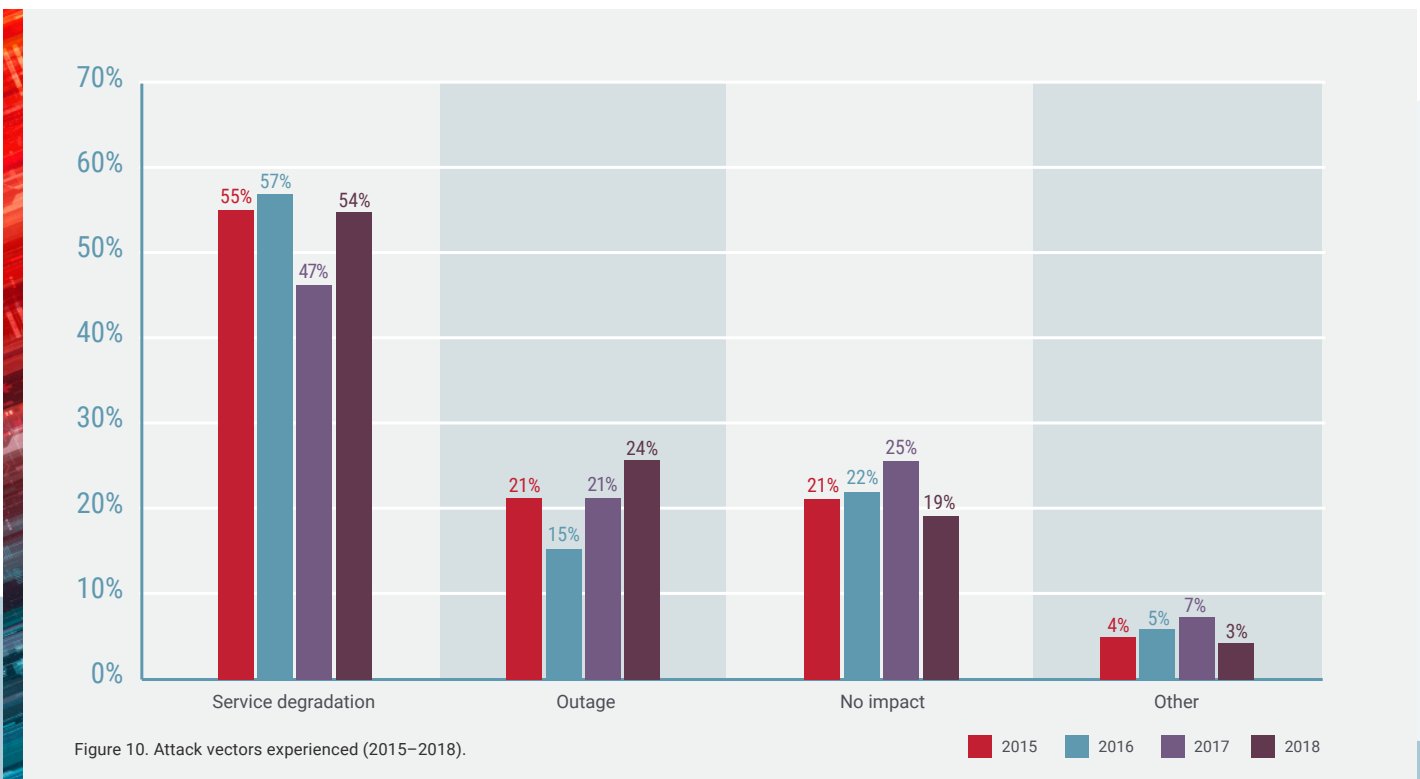
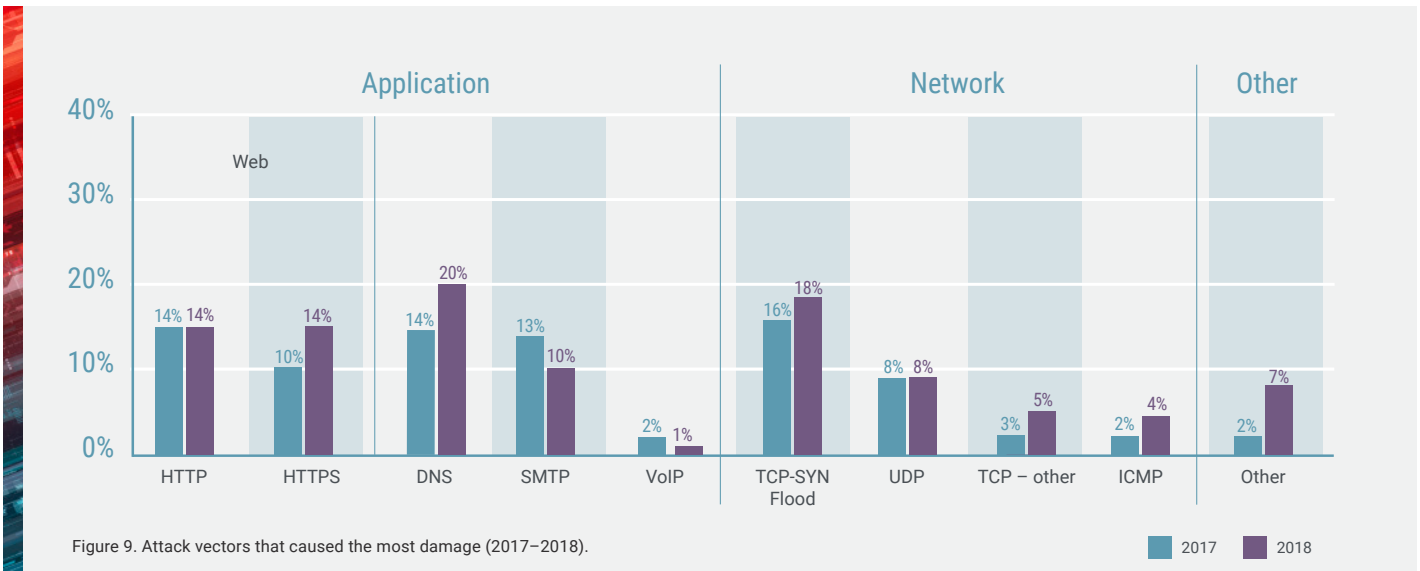


The application-layer attack dominance was driven by a growth in the incidence of HTTPS Floods and DNS attacks, rising by 20% and 15% respectively. In network layers, Radware sees 44% growth in ICMP Floods and 75% growth in other forms of TCP attacks. One in 13 organizations suffered attacks over VoIP.

Is there a way to estimate the impact of each type of DDoS attack? According to survey results, application-layer attacks caused more damage, and the top three harmful vectors were web attacks, DNS attacks and SYN Floods (see Figure 9).

Consequences

In 2018, 78% of attacks resulted in service degradation or a complete outage, compared to 68% in 2017 (see Figure 10). This 15% growth shows that attacks are becoming more powerful because tools used by adversaries are more efficient in compromising security defenses.

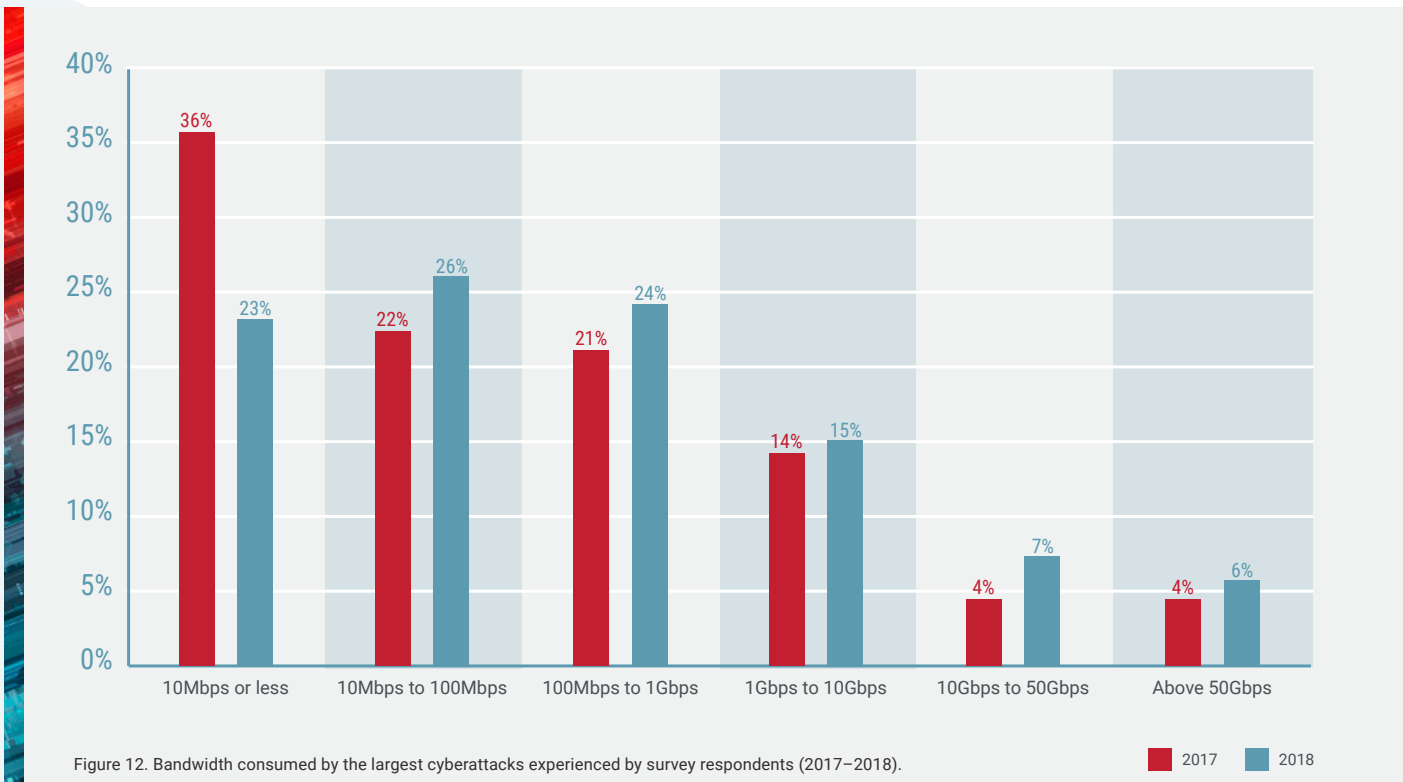
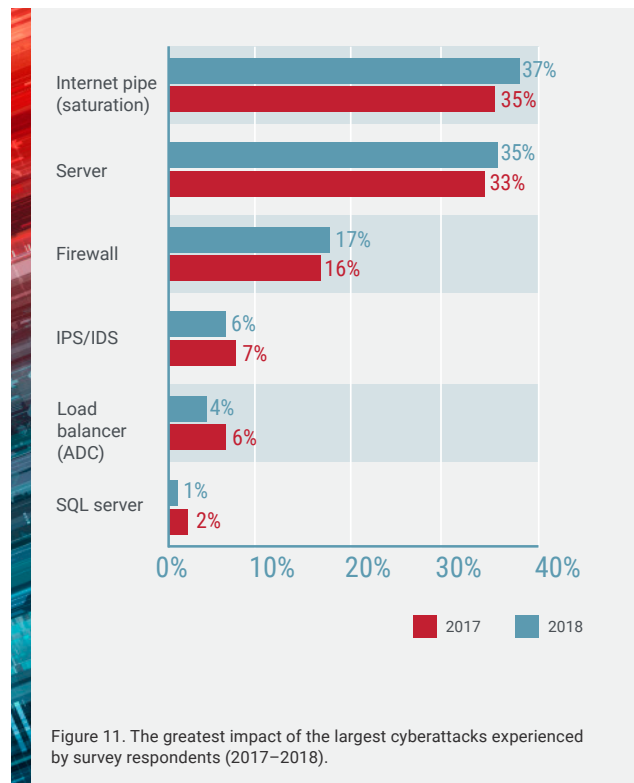


Impact on Components

The greatest impact of cyberattacks is clogging the internet pipe, followed by crashing servers if attacks are not mitigated at the perimeter or firewall. Firewalls are third on the list, as they – together with IPSs and ADCs – are stateful devices that, by design, cannot withstand a DDoS attack since their connection tables are quickly filled. There is a clear need for an always-on DDoS mitigation solution – either a hybrid (integrating on-premise protection with cloud-based scrubbing) or an always-on cloud service to mitigate the attack traffic and maintain availability of these network components (see Figure 11).

Characteristics of DDoS Attacks

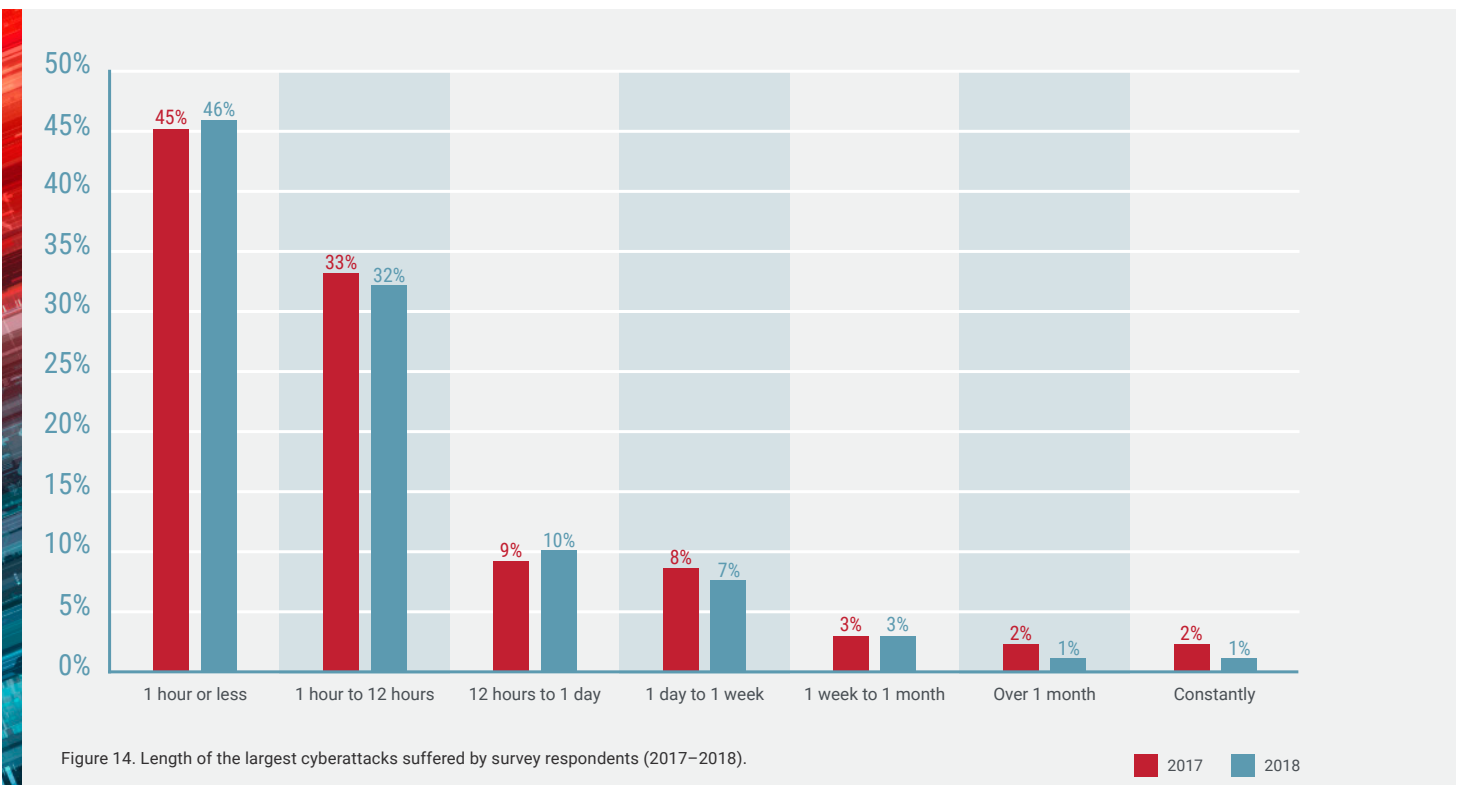
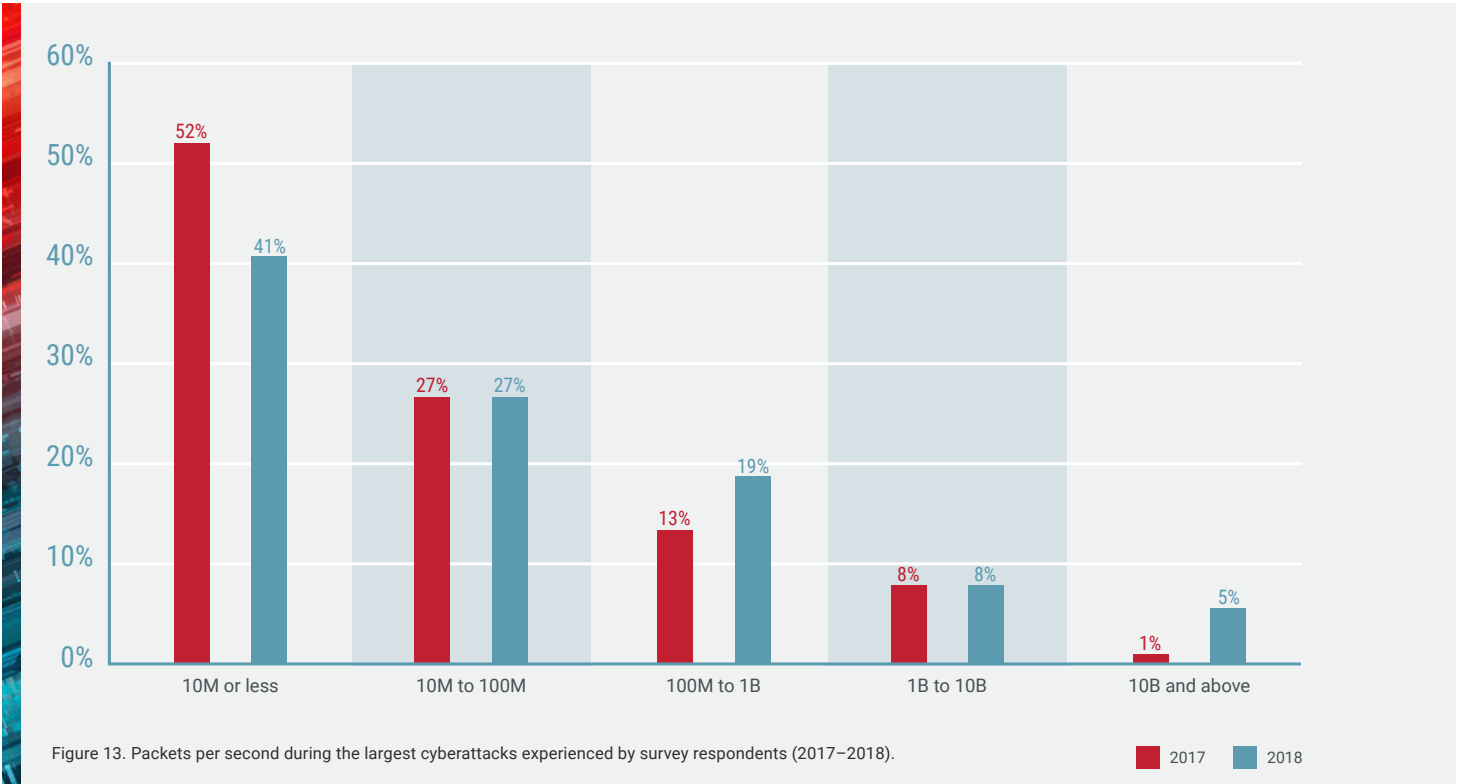
Radware sees a decrease in small-scale attacks and a shift toward larger volumes across the board. The use of extra-large attacks (above 10Gbps) that can saturate most of the internet pipes globally have almost doubled in 2018 (see Figure 12).



In terms of intensity, there is a similar trend in packets per second (PPS). High-paced attacks are increasing over low-paced ones (see Figure 13). The change requires a shift in defense strategy because looking at capacity alone is no longer a sufficient test. Companies also need to consider and test packet intensity.

Duration

Radware also noticed that almost half of the denial-of-service attacks lasted less than one hour (see Figure 14). Sometimes they hit in recurring bursts. More than 20% of the DDoS attack campaigns lasted more than 12 hours, exhausting the target network and security teams.



DNS Attacks

Forty-nine percent of respondents said that they had suffered attacks against their DNS servers compared to 41% in 2017, an increase of 20% (see Figure 16). Drivers included easy access to powerful attack tools over the darknet and the growing popularity of IoT botnets that often included DNS attack vectors.

Of those who did suffer DNS attacks, 40% did not mitigate them well and were impacted by the attack. This finding emphasizes the gap in traditional protections that cannot effectively mitigate today's sophisticated DNS attack vectors. Attacks against DNS services come in various shapes and sizes. The prevalence of attacks experienced by respondents were ranked (see Figure 15). The most notable growth (45%) was in cache poisoning attacks.

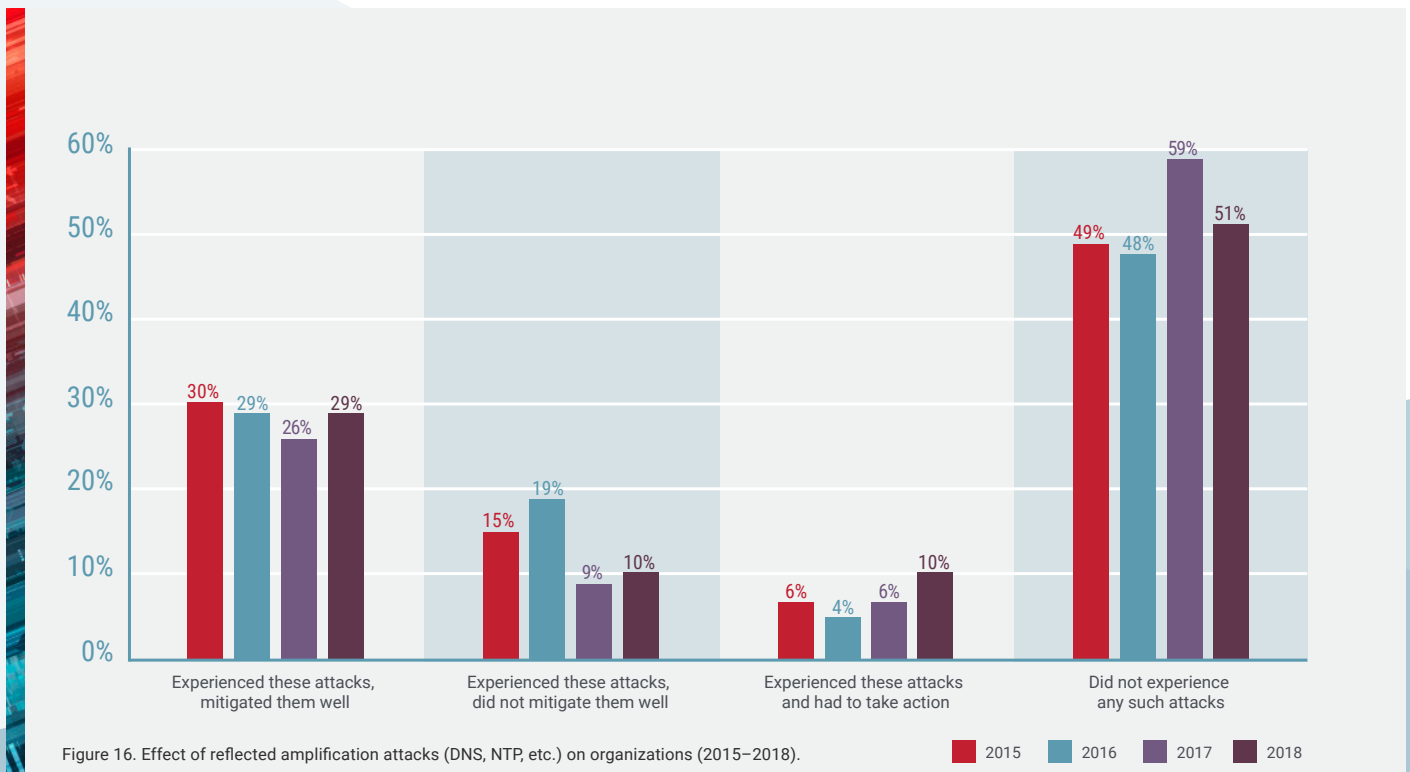
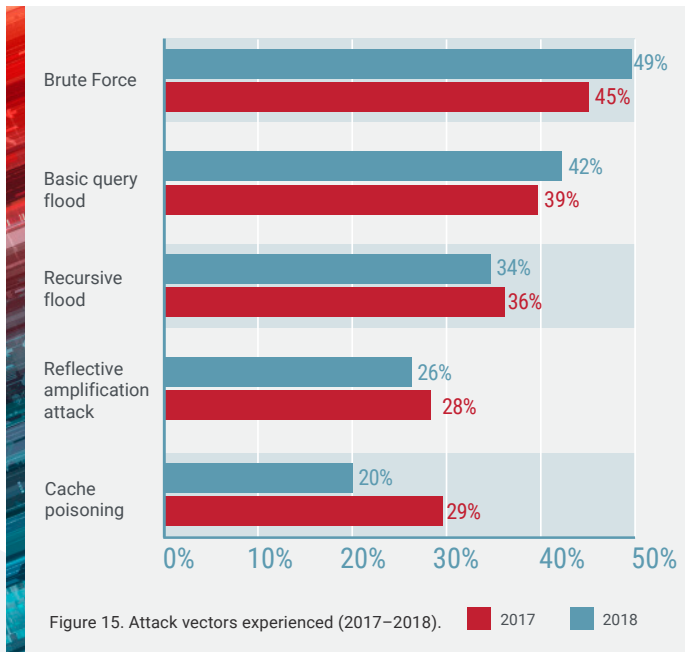
Emerging DDoS Tactics

IoT Botnets

Similar to 2017, one in six respondents indicated that they were hit by a DDoS attack originating from an IoT botnet. Also like 2017, Radware suspects many of the others did not know or could not tell where an attack originated. Based on the growing presence and variety of such botnets, Radware expects to see an increase in IoT botnet attack incidences.

SSL-Based Attacks

There was a 13% increase in organizations experiencing encrypted attacks. These attacks required high-capacity resources to mitigate and tended to be effective against most traditional defenses. Detecting and mitigating attacks in encrypted traffic was a challenge for organizations on different levels. A third of respondents reported



that they could not tell if they experienced such an attack in 2018, demonstrating a visibility challenge of which hackers are quick to take advantage. SSL-based attacks were most prevalent in North America (16% above the global average) and EMEA (10% above the global average).

Attacks Above 1Tbps

This monstrous bar of 1Tbps was crossed for the first time in late 2016, but 2018 saw new records in denial-of-service attack volumes. Attackers generated attacks peaking at 1.3Tbps and 1.7Tbps in the spring of 2018. These two attacks specifically took advantage of a vulnerability in Memcached. Seven percent admitted to suffering Memcached attacks, and another 10% said that they suffered attacks above 1Tbps other than Memcached.

Burst Attacks

In recent years, DDoS attackers have adopted more Burst attacks, generating attacks in high waves of enormous volumes, but for short periods. They come back at random intervals and cause havoc among surprised, helpless security teams. The shorter the attacks, the harder it is for organizations to fight them. Last year, 42% reported suffering Burst attacks. In 2018, the number grew to 49%. We also see the shift toward shorter bursts rather than longer ones.

Half of organizations suffered Burst attacks in 2018.

Nonvolumetric Denial of Service

Large volumes are not the only way to disrupt the operation of servers and applications. Many tools are available (Torshammer, LOIC, Slowloris) that make targets open and hold connections by sending data bit by bit at a very slow pace until they eventually crash. Other forms of attacks — particularly against applications — bring resources to overload. Respondents to Radware's *The State of Web Application Security* report² experienced a variety of nonvolumetric denial-of-service attacks in 2018 (see Figure 18). IoT botnets help scale these targeted attacks. With more IoT botnets, it is easier to create low-volume attacks from multiple IoT devices that together create a very impactful attack on the target.

Application-Layer Attacks

Radware's *The State of Web Application Security* report³ revealed the most common application attacks in the previous 12 months (see Figure 19).

The Big Picture

The global industry survey results mirror industry trends around the increase in frequency and changing techniques used to launch cyberattacks. As security professionals benchmark the companies' experiences against the data covered here, a bigger picture is likely to emerge about the need to deploy security solutions that not only adapt to changing attack vectors to mitigate evolving threats, but also maintain service availability at the same time.

SSL-based attacks by region

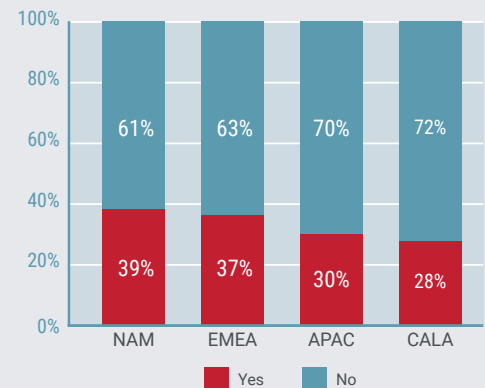


Figure 17. SSL-based attacks grew by 10% in 2018, striking more frequently in North America than in APAC and CALA.

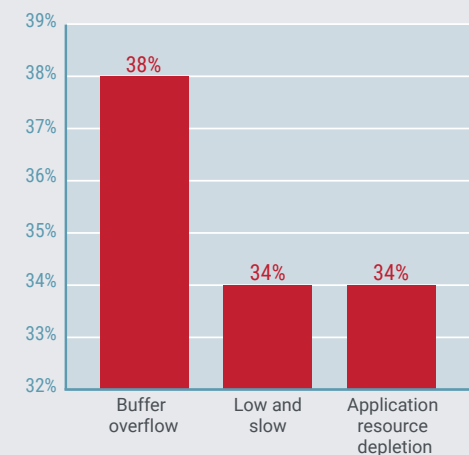


Figure 18. Nonvolumetric denial-of-service attacks in 2018.

Encrypted web attacks (SSL/TLS based)	50%
Data security breaches	46%
Web scraping	39%
HTTP/Layer 7 DDoS	34%
API manipulations	34%
SQL injection	34%
Cross-site scripting	32%
Credential stuffing/credential cracking	24%
None of these/no attacks experienced	11%

Figure 19. Encrypted web attacks were the most commonly reported form of application-layer attacks in 2018.

²<https://www.radware.com/webapplicationsecurityreport/>
³<https://www.radware.com/webapplicationsecurityreport/>



Long-Term Business Impacts of Cyberattacks

The relationships between businesses and customers are based on one simple concept: trust. Organizations invest a lot of time and money curating their brands to assure customers that their products/services are essential, customer service is vital, and transactions are secure.

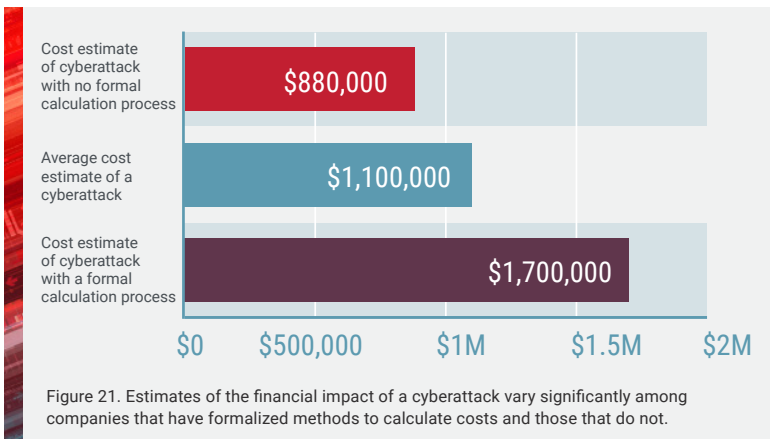
Customers put their trust in companies to deliver on promises of security. Think about how quickly most people tick the boxes on required privacy agreements, likely without reading them. They want to believe the companies they choose to associate with have their best interests at heart and expect them to implement the necessary safeguards. The quickest way to lose customers is to betray that confidence, especially when it comes to their personal information.

Hackers understand that, too. They quickly adapt tools and techniques to disrupt that delicate balance. Executives from every business unit need to understand how cybersecurity affects the overall success of their businesses.

In our digital world, businesses feel added pressure to maintain this social contract as the prevalence and severity of cyberattacks increase. Respondents to Radware’s global industry survey were definitely feeling the pain. Ninety-three percent of the organizations worldwide indicated that they suffered some kind of negative impact to their relationships with customers as a result of cyberattacks (see Figure 20).

Negative customer experience	43%
Brand reputation loss	37%
Customer loss	23%

Figure 20. Successful cyberattacks are damaging to customer relationships.



The Real Costs of Cyberattacks

What are the real costs of a cyberattack? Besides the breaking of customers’ trust, according to Radware’s global industry survey, the financial cost of a single successful cyberattack was on average \$1.1 million, a staggering 52% increase from the estimation in the previous year’s survey.

According to Accenture’s *Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience* report⁶, 13% of cyberattacks are successful. Simple math tells us that, if a company suffers 10 successful attacks in a year, it could potentially experience additional operating costs of \$11 million to mitigate the threats.

Similar to last year’s survey results, about three-fourths of companies did not currently have a formalized calculation to determine the financial impact of a cyberattack, revealing no improvement in defining this metric. The 28% that did have a way to calculate related costs reported an average cost of \$1.7 million, nearly double the estimate of firms that did not have a formal method to determine costs.

The impact of cyberattacks is gaining notice. Radware sees a 50% growth in organizations that estimate the cost of an attack is greater than \$1 million and an overall shift away from lower estimations (see Figure 22).

Comparing 2017 to 2018*

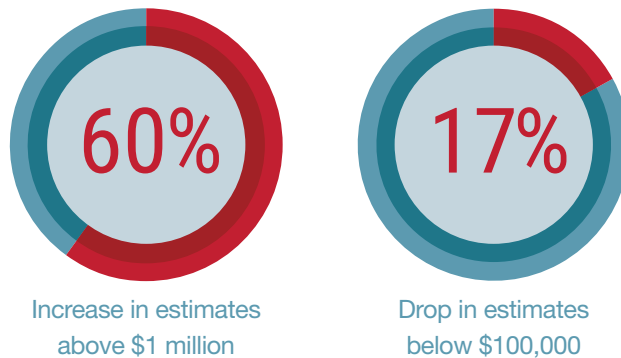


Figure 22. Companies’ estimates of costs related to cyberattacks are on the rise. *Companies surveyed in both years were of similar size and revenues.

According to Radware’s global industry survey, 45% of cyberattacks aim to cause service disruptions. Service interruptions result in negative customer experiences that can damage customer loyalty, resulting in churn. Customer attrition rates can increase by as much as 30% following a cyberattack.⁴ Churn also results in increased spending for marketing to acquire new customers or regain lost ones.

Enterprises worldwide point at a negative customer experience as the primary impact of cyberattacks, with one in four reporting having experienced customer churn following an attack, according to Radware’s global industry survey.

Data breaches have real and long-lasting business impacts. Quantifiable monetary losses can be directly tied to the aftermath of cyberattacks in lost revenue, unexpected budget expenditures and drops in stock values. Protracted repercussions are most likely to emerge as a result of negative customer experiences, damage to brand reputation and loss of customers.

In Radware’s 2018 *Consumer Sentiments: Personal Data and the Impact on Customer Loyalty*⁵, the vast majority (68%) of consumers said that, when a company suffers a data breach, they must be convinced that the security issue has been addressed and any damage has been rectified before continuing to do business with the brand. Even worse for the organization’s bottom line, one in 10 consumers will walk away entirely from the brand.

Because the stakes are so high, Radware wanted to know how businesses are handling the added pressure. The global industry survey explored the impact of cyberattacks on businesses from three angles:

- ▶ The Real Costs of Cyberattacks
- ▶ Perceptions of Preparedness
- ▶ Readiness for the Future

⁴Journal of Accountancy, July 25, 2016, “The hidden costs of a data breach.” Retrieved from <https://www.journalofaccountancy.com/news/2016/jul/hidden-costs-of-data-breach-201614870.html>

⁵Radware, 2018, *Consumer Sentiments: Personal Data and the Impact on Customer Loyalty*. Retrieved from <https://www.radware.com/cybersecurity-consumers/>

⁶Accenture, 2018, *Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience* report. Retrieved from <https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index>



The size of an organization also affects the estimated cost of an attack (see Figure 23).




Size of Business	Estimated Cost of Attack
 SMBs <1,000 employees	\$450,000
 ENTERPRISES 1,000 to 10,000 employees	\$1.1 million
 LARGE CORPORATIONS >10,000 employees	\$2.1 million

Figure 23. Cost-of-attack estimates by company size.

Larger global companies that employ more than 10,000 people and have greater than \$1 billion in total revenue are more likely to estimate higher costs as a result of cyberattacks.

When the responses are broken out by vertical, the education market estimates the lowest costs as a result of cyberattacks, which is consistent over the past three years (see Figure 24).

Mean Estimation (in millions)

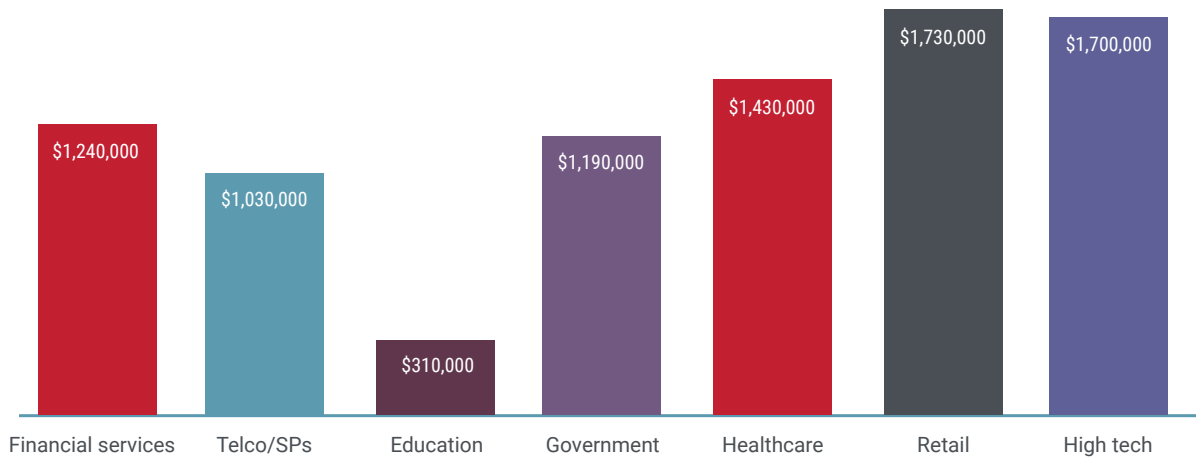


Figure 24. Estimated cost related to cyberattacks by vertical market.

Missing Variables from the Cost Equation

In many ways, attackers are assaulting companies' operating expenses (opex). Cyberattacks are a viable threat to opex, and the impact is severe. The estimated cost of a cyberattack at \$1.1 million should be enough to pique the attention of every business executive. But the figure might be low because it likely does not incorporate three variables.

- 1 **Direct costs** — Other expenses attributable to a cyberattack such as the costs for extended labor, investigations, audits and software patches that often require development.
- 2 **Indirect costs** — Other overhead costs such as crisis management, technical consultants, regulatory fines, customer compensation, legal expenses, liability and stock price drops.
- 3 **Prevention** — Other costs associated with the protection of data centers and applications, the hardening of endpoints, the management of cloud workloads, and the development and testing of emergency response and disaster recovery plans.

Companies of every size suffer when cyberattacks are successful. For small- and medium-size businesses, the impact can be a deadly hit, which is of great concern because these sized companies report that they are less prepared (see Figure 25).

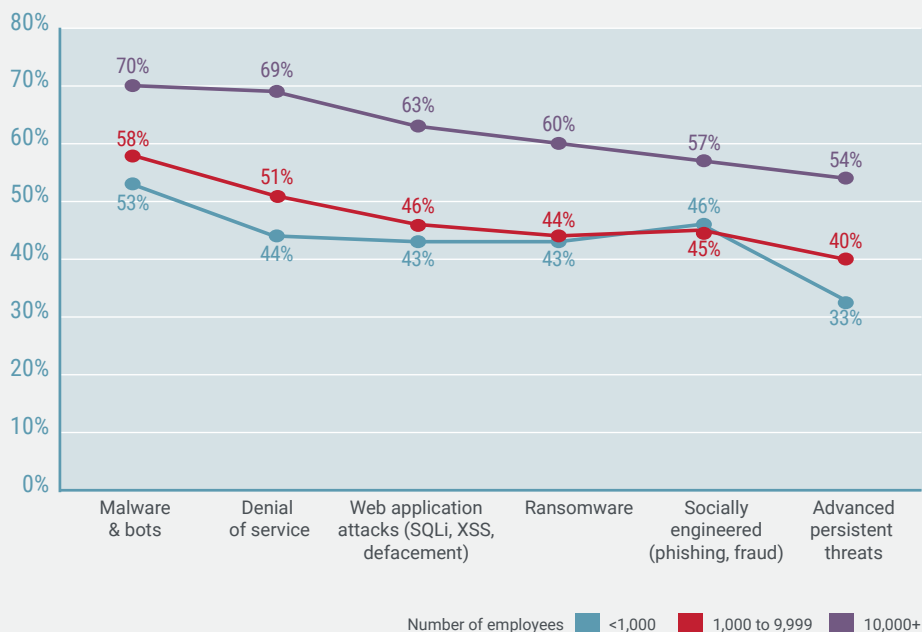
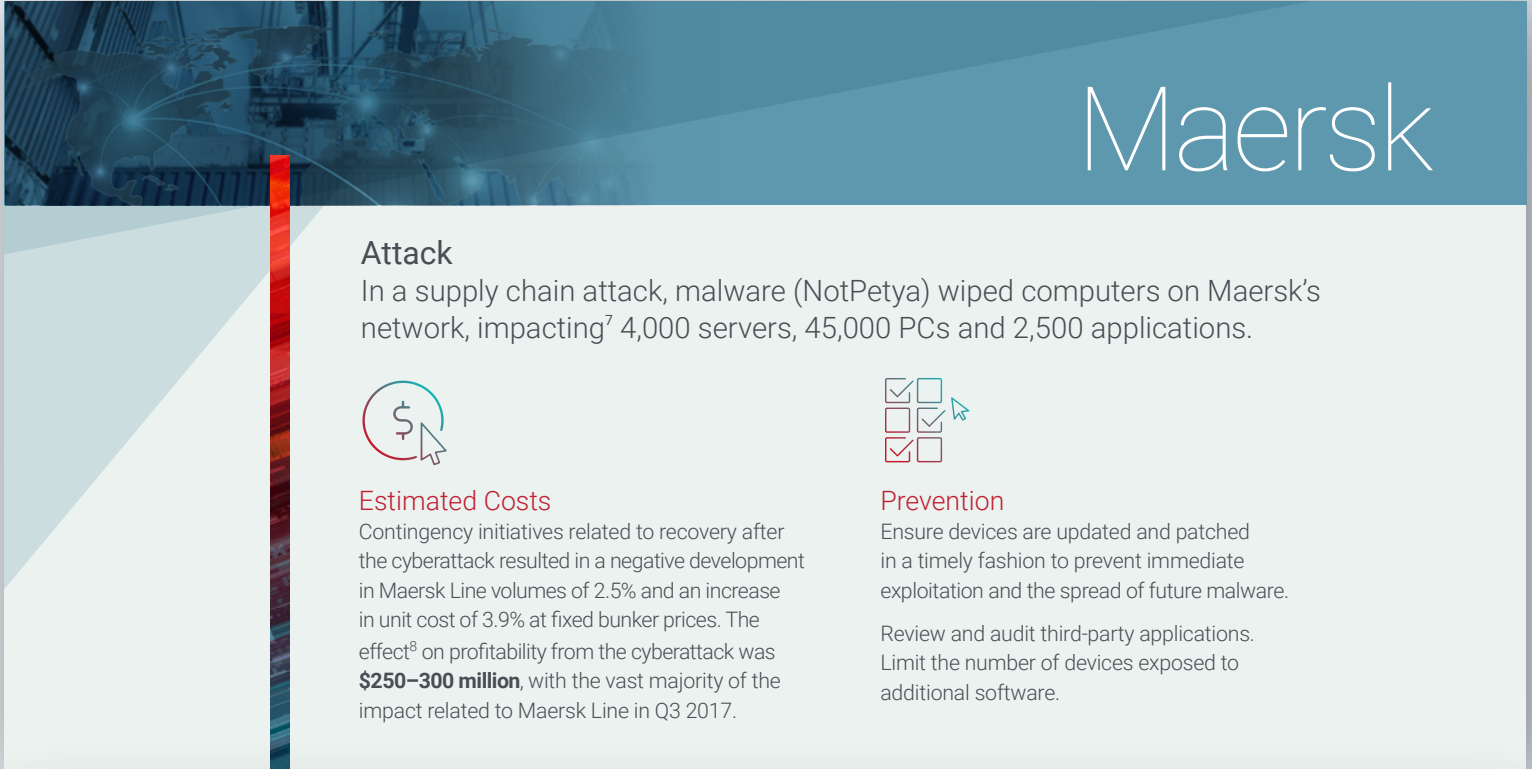


Figure 25. Reported preparedness for cyberattacks by organization size.




The Costs Are Real


Expenditures related to cyberattacks are often realized over the course of several years. What's more is that many of the massive data breaches highlighted in Figure 26 could have been avoided with careful security hygiene and diligence to publicly reported system exploits.



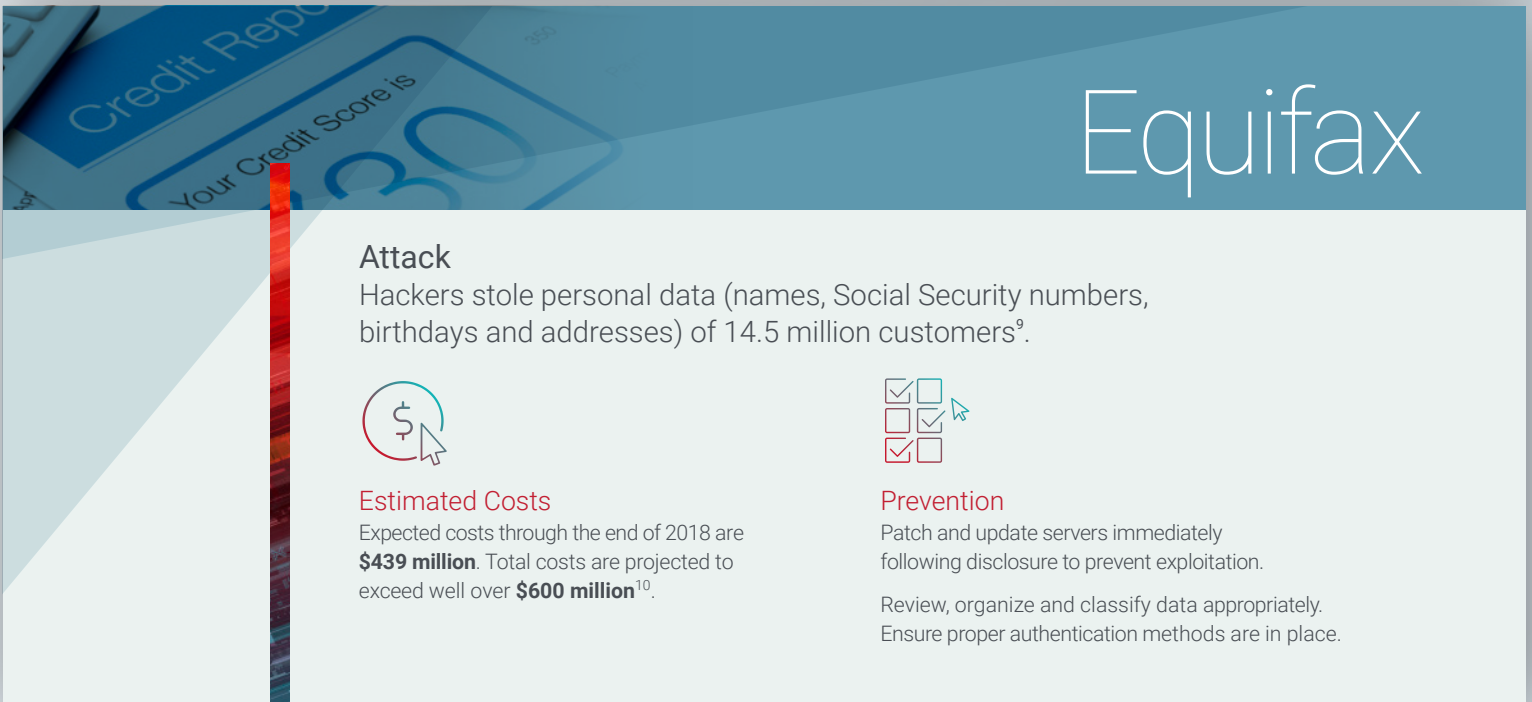
Maersk

Attack
In a supply chain attack, malware (NotPetya) wiped computers on Maersk's network, impacting⁷ 4,000 servers, 45,000 PCs and 2,500 applications.

 **Estimated Costs**
Contingency initiatives related to recovery after the cyberattack resulted in a negative development in Maersk Line volumes of 2.5% and an increase in unit cost of 3.9% at fixed bunker prices. The effect⁸ on profitability from the cyberattack was **\$250–300 million**, with the vast majority of the impact related to Maersk Line in Q3 2017.


 **Prevention**
Ensure devices are updated and patched in a timely fashion to prevent immediate exploitation and the spread of future malware.


Review and audit third-party applications. Limit the number of devices exposed to additional software.



Equifax

Attack
Hackers stole personal data (names, Social Security numbers, birthdays and addresses) of 14.5 million customers⁹.

 **Estimated Costs**
Expected costs through the end of 2018 are **\$439 million**. Total costs are projected to exceed well over **\$600 million**¹⁰.

 **Prevention**
Patch and update servers immediately following disclosure to prevent exploitation.

Review, organize and classify data appropriately. Ensure proper authentication methods are in place.

⁷<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

⁸<https://www.maersk.com/news/2018/06/29/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year>

⁹<https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf>

¹⁰<https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257>



Yahoo!

Attack

A state-sponsored actor stole Yahoo's proprietary source code and used it to access¹¹ user accounts.



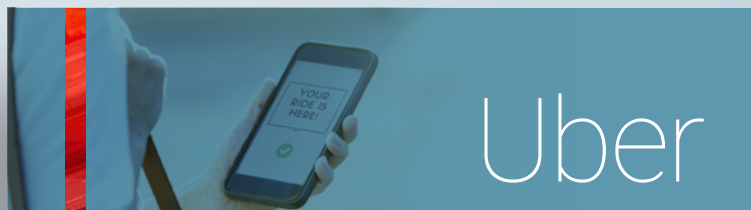
Estimated Costs

Costs¹² included **\$1.3 billion** in market capitalization and **\$165+ million** in fines. The company was sold to Verizon for \$350 million less than the initial offer.



Prevention

Protect your company's source code by preventing or limiting internal and external access to repositories hosting sensitive data.



Uber

Attack

Hackers¹³ obtained login credentials from a compromised private repository on GitHub to steal unencrypted data stored on Uber's Amazon Web Services account.



Estimated Costs

Legal settlements¹⁴ cost **\$148 million**, which does not include the hard costs on mitigating an attack or other business impacts.



Prevention

When available, use two-factor authentication (2FA) for protecting source codes or other digital assets hosted across multiple cloud networks.



Anthem

Attack

A phishing campaign targeting employees was reportedly¹⁵ caused by an attacker acting on behalf of a foreign nation.



Estimated Costs

Costs included **\$131 million** in settlements¹⁶ — including the largest settlement¹⁷ reached by the U.S. Department of Health & Human Services Office for Civil Rights for a Health Insurance Portability and Accountability Act (HIPAA) breach. That amount excludes the attack mitigation costs.



Prevention

Ensure that employees have received adequate training on how to spot social engineering attacks.

Access controls to prevent unauthorized access to the internal system and patients' data.

¹¹<https://help.yahoo.com/kb/SLN27925.html>

¹²<https://www.businessinsider.com/yahoo-16-million-dollars-q1-hacking-incidents-2017-5>

¹³<https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack>

¹⁴https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf

¹⁵<https://healthsecurity.com/news/anthem-data-breach-reportedly-caused-by-foreign-nation-attack>

¹⁶<https://healthsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement>

¹⁷<https://www.modernhealthcare.com/article/20181016/NEWS/181019927>

Figure 26. Impact of cyberattacks on companies.

Management boards and directorates should understand the impact of cyberattacks on their businesses. They should also prioritize how much liability they can absorb and what is considered a major risk to the business continuity. Technology and business executives are mostly in sync about how cyberattacks affect their businesses (see Figure 27).

Ranked First	Technology Executives	Business Executives
Data leakage	31%	42%
Service outage	21%	12%
Reputation loss	21%	21%
Revenue loss	15%	6%
Customer/partner loss	6%	12%
Productivity loss	3%	6%
Job loss	4%	0%

Figure 27. Impact of attacks as rated by technology and business executives.

Perceptions of Preparedness

Even though organizations reported higher estimated financial costs and greater negative impacts on customer relationships, the perceptions that their organizations were prepared remained consistent with survey results from 2017. Across all attack types, about one-half of all respondents reported feeling that their organizations were extremely or very well prepared to protect against security threats. Respondents felt most prepared to handle malware attacks (59%).

At the same time, many expressed a level of uncertainty with regards to their current security posture. Fifty-nine percent had concerns about their ability to handle advanced persistent threats, followed by ransomware (52%), web application attacks and socially engineered attacks (both 51%), (see Figure 28).



	Extremely/ Very Well Prepared	Somewhat/ Not Very/Not Prepared
Malware (worms, viruses)	59%	41%
DDoS	53%	47%
Ransomware	48%	52%
Web application attacks	49%	51%
Socially engineered (phishing, fraud)	49%	51%
Advanced persistent threats	41%	59%

Figure 28. Perceptions of preparedness to safeguard against specific cyberattacks.

Confidence by Region

Perceptions of ability to effectively fight long-lasting attacks across all regions

North American companies are most confident in their abilities to fight attacks lasting more than one day or longer (47%) while CALA is the least confident (24%).

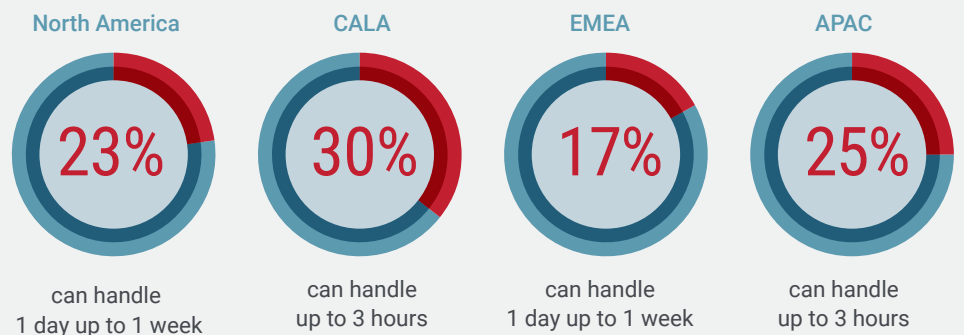


Figure 29. The durability of security teams in different regions.

Extremely/Very Well Prepared	Total	Financial Services	Service Prov. & Telecom	Education	Government	Healthcare*	Retail*	High Tech
Malware and bots (worms, viruses, spam)	59%	63%	61%	53%	58%	55%	57%	65%
Distributed denial of service (DDoS)	53%	54%	63%	33%	52%	55%	61%	63%
Web application attacks (SQLi, XSS, defacement)	49%	56%	50%	31%	47%	52%	43%	64%
Socially engineered threats (phishing, fraud)	49%	53%	50%	31%	44%	58%	57%	53%
Ransomware	48%	51%	50%	29%	50%	39%	57%	55%
Advanced persistent threats	41%	46%	46%	27%	38%	39%	35%	48%

Figure 30. Vertical markets preparedness to safeguard against specific cyberattacks. *Percentages based on a smaller sample size.

Advanced persistent attacks are a reason for concern. Nearly two out of five organizations could not fight long-lasting attack campaigns, with significant variances between regions.

What industry respondents represent affects perceptions of preparedness for specific types of attacks (see Figure 30). The education vertical consistently ranked itself lower than average for its confidence to mitigate all attack types. The high-tech vertical was more prepared to handle web application attacks than other industries.

Nearly half said that they are not ready to deal with DDoS or web application attacks. Retailers, because of the nature of their business and for the sake of the customer experience, are more prepared for DDoS and fraud scams and least ready for advanced persistent threats.

Healthcare, despite infamous hits on the United Kingdom National Health Service, Hollywood Hospital and others, is still intimidated by ransomware. Service providers felt most confident in protecting their infrastructure from DDoS attacks, and financial services felt most confident in protecting against malware.

Network and Application Defense Strategies

In response to the added pressure to secure the customer experience and maintain trust, organizations implement a layered protection strategy. What types of protections are deployed is influenced by where applications and data are housed. Radware continues to see evidence of more organizations adopting a hybrid approach in which network operations are maintained at both the LAN and the cloud (see Figure 31).

The shift to hosting applications and services with cloud service providers is driven by quality of service, availability, speed and lower latency. This approach is more visible among global companies with annual revenue of \$1 billion, with hints at higher adoption rates among service providers. The education market is least likely to use a hybrid approach.

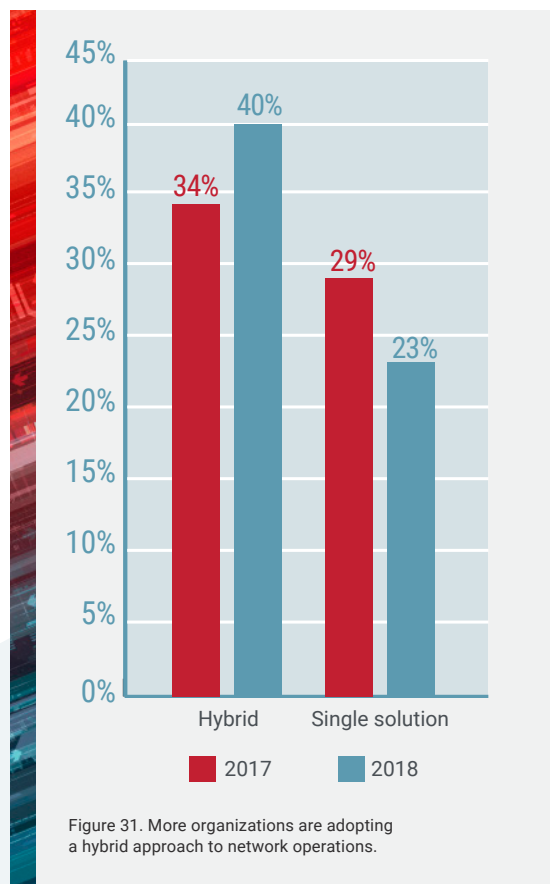
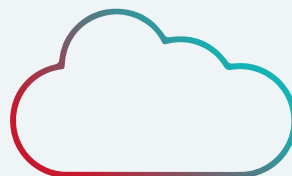


Figure 31. More organizations are adopting a hybrid approach to network operations.



Two-thirds of businesses use a cloud service for DDoS protection.

Overall, three-fourths reported use of DDoS mitigation solutions, whether on-premise, in the cloud or a hybrid. What solutions organizations used to defend against cyberattacks was consistent over the last three years: Half had an on-premise device, two-thirds had some kind of cloud service (by the vendor, the ISP or a CDN), and 40% used both.

Application Protection Strategies/Readiness

Applications are the entry point for hackers in many instances. The combination of easy scanning with publicly available exploit kits and common coding errors makes it the default crack that hackers seek when planning attacks. Yet security practices in many cases fall behind (see Figure 32). For instance, Radware was surprised to learn that one in five organizations still did not use a web application firewall (WAF) to protect its web server and the confidential information it accesses. Moreover, only half ran penetration tests against their networks to find vulnerabilities.

There is consistent growth in a hybrid approach with both on-premise WAF and a cloud WAF service. The challenge is that most vendors do not use the same technology on-premise and in the cloud, which is more of a dual solution instead of a hybrid approach. It makes migration complex and onboarding difficult.

This situation requires different experts to manage both solutions and tediously maintain the same security policy across the different environments. In addition, it leaves the organizations with either a negative or positive security model that does not exchange threat information, resulting in limited protection against known and unknown attacks.

As the threat landscape evolves, WAFs must do more than just protect the applications. They should be able to protect APIs, manage bot traffic and withhold denial-of-service attacks.

Applications today are open to interactions with cloud infrastructure, other apps, automation tools and other systems. The attack surface is growing larger, leading to a greater risk exposure. Some businesses already recognize the trend and deploy additional solutions on top of a WAF for complete application protection (see Figure 33).

Not only are the applications difficult to secure because they are scattered across different platforms and frameworks, but they must also comply with multiple information security policies. Adding even more complexity is that applications constantly change: 44% on a weekly basis, 18% on a daily basis (see Figure 34).

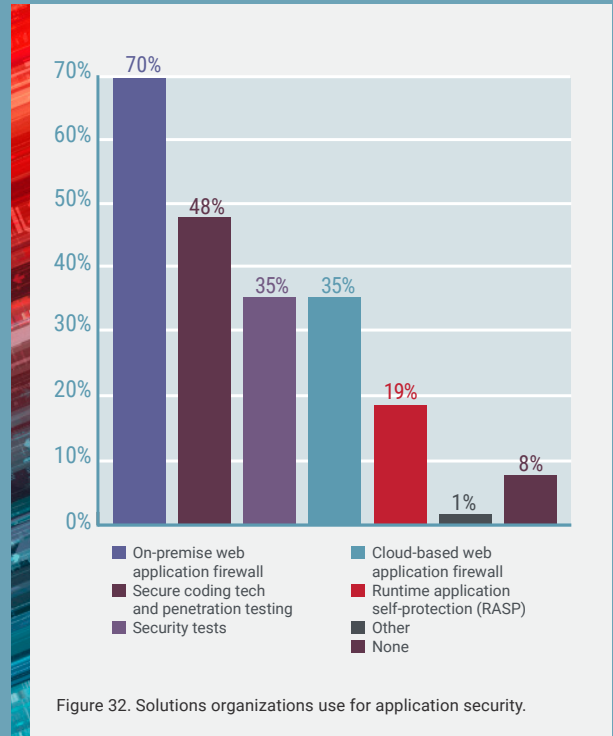


Figure 32. Solutions organizations use for application security.

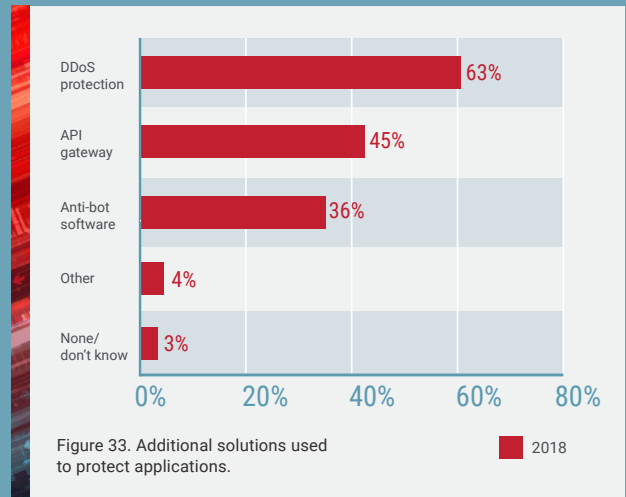


Figure 33. Additional solutions used to protect applications. 2018

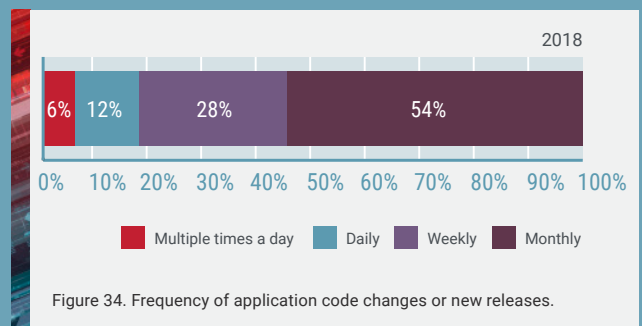
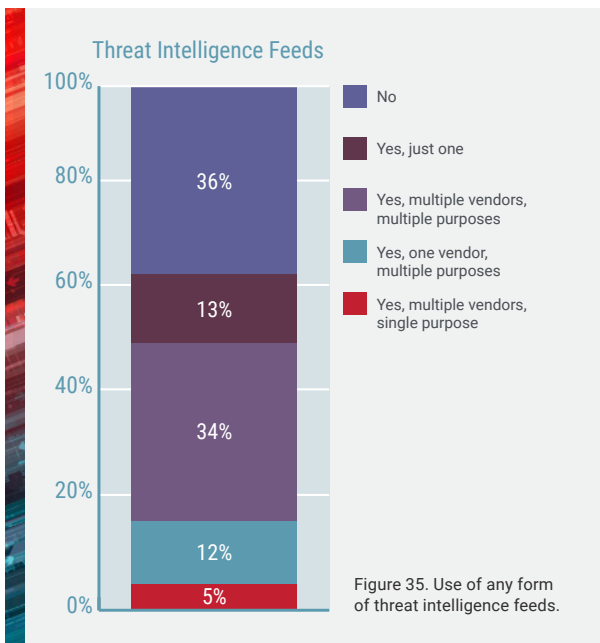


Figure 34. Frequency of application code changes or new releases. 2018



As applications are updated, security policies must adapt accordingly. Policy generation, detection and mitigation can no longer rely on manual labor as these frequent changes impact the operational costs and increase risk exposure. To protect against an expanding variety of attacks, automation of security policies is the best option.

Threat Intelligence

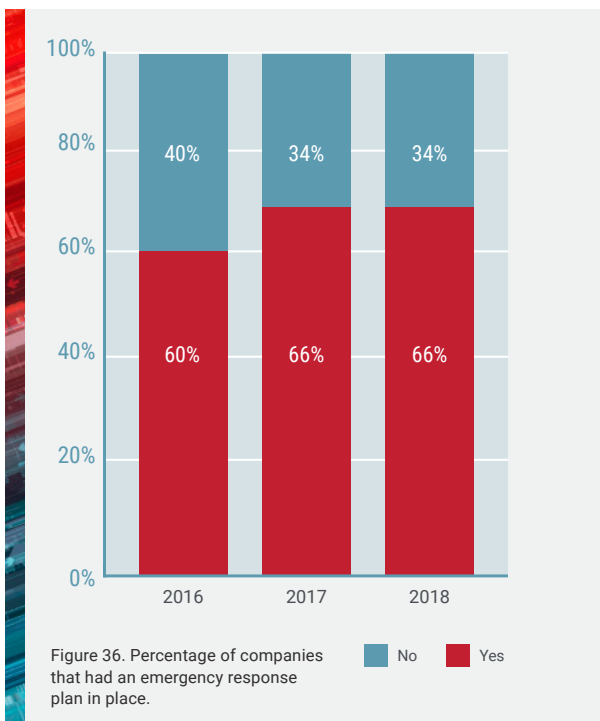
Many security protection vendors offer threat intelligence feeds as part of their portfolios. Because some rely on the same research on the back end to inform the reports, it is often difficult to distinguish one from the other. The frequency of feeds varies with some published weekly and others in real time. Some are based on signatures and vulnerabilities and others on real-life events.

Two-thirds of survey respondents consumed threat intelligence feeds (see Figure 35). These feeds can come from different vendors for a sole purpose or from one source for different purposes (for example, DDoS protection, application security, IPS or spam).

Emergency Response

Even though only seven percent of companies reported not experiencing cyberattacks in the previous 12 months, the number of organizations that lacked an emergency response plan remained stagnant at 34% (see Figure 36).

Healthcare institutions, pharmaceutical, medical insurance, labs and physicians are becoming more popular targets for attackers. The value of medical records on the darknet is higher than that of passwords and credit cards. To prevent attacks that affect the functionality of medical systems, this industry must be able to promptly detect and thwart cyberattacks. At 82%, healthcare leads industries that have an emergency response plan in place.



Compliance

The GDPR in the EU became enforceable on May 25, 2018. Failure to meet the legal obligations of GDPR can result in a fine up to €20 million or up to four percent of the organization’s annual worldwide turnover of the previous financial year, whichever is greater.

Within EMEA, there is a slight difference in how companies in EU and non-EU countries said they were doing with GDPR compliance (see Figure 37).

Many other countries, including the United States and Canada, also levy stiff fines for data breaches as regulators understand that they need to take a stance. One well-timed cyberattack has the potential to be the David to a multinational Goliath, wiping out brand and market value in a short amount of time.

For example, in addition to the hard costs of Yahoo’s data breach, the company was sold under duress and is still getting hit with U.S. fines of \$300 million. Now that the GDPR is active, a similar breach would result in a fine of at least four percent of total revenue from the EU, plus additional fines from other countries, hard costs of mitigating a breach, customer churn, stock price drops and potential C-suite terminations — enough to bankrupt even the largest multinationals.



One GDPR infringement can result in a fine of up to €20 million or 4% of an organization’s total annual worldwide turnover.

Source: European Commission [website](#)



	Very Well	Well	Somewhat Well
European Union countries	18%	40%	33%
Non-EU countries	18%	27%	26%
Rest of the world	16%	23%	26%

Figure 37. Perception of success complying with the GDPR.

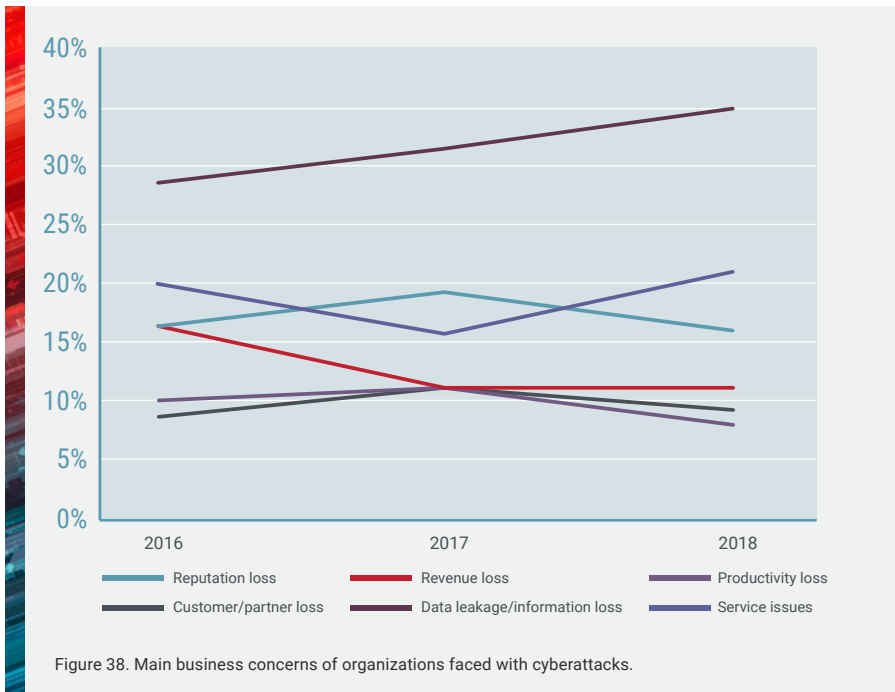


Figure 38. Main business concerns of organizations faced with cyberattacks.

Readiness for the Future

Consumers have high expectations when it comes to safeguarding their personal information. Cybersecurity is an issue that touches all aspects of a business’s operations, not just information technology. Smart brands will embrace security as a key element of the overall customer experience and leverage it as a market differentiator in our post-trust world where the presumption of security is waning.

The impact of cyberattacks on customer retention, response costs and operating expenses weighs heavy on the minds of survey respondents.

In 2018, respondents are concerned about how successful cyberattacks affect relationships with customers.

Productivity losses and service outages ranked highest, even over revenue and reputation (see Figure 38).

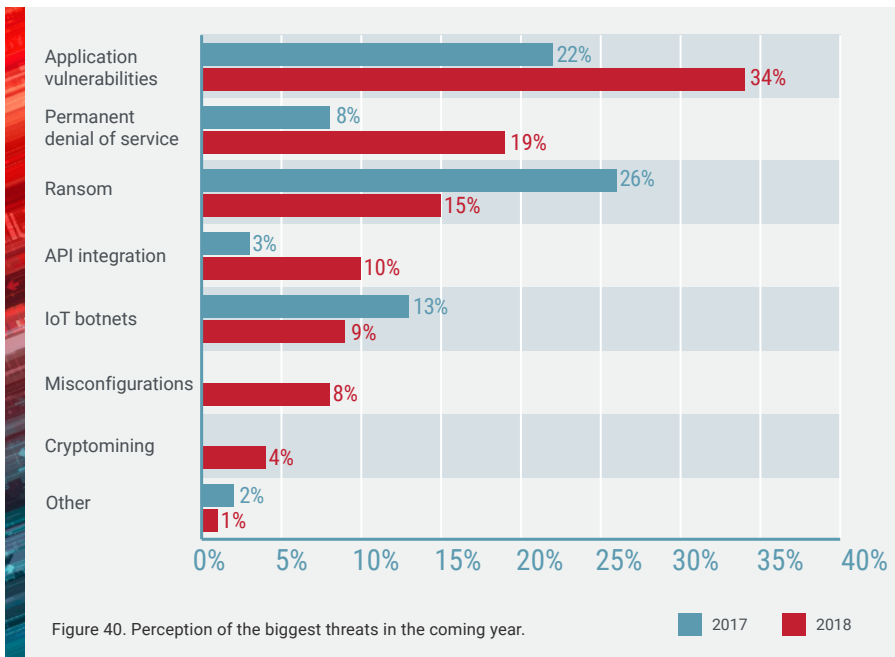


Figure 40. Perception of the biggest threats in the coming year.

Biggest Threats in 2019

Application vulnerabilities (34%) and permanent denial of service (19%) were the two biggest threats respondents are concerned about in 2019, up quite a bit from last year’s report (see Figure 40). The threat of ransom attacks dropped to 15%, down from 26%.

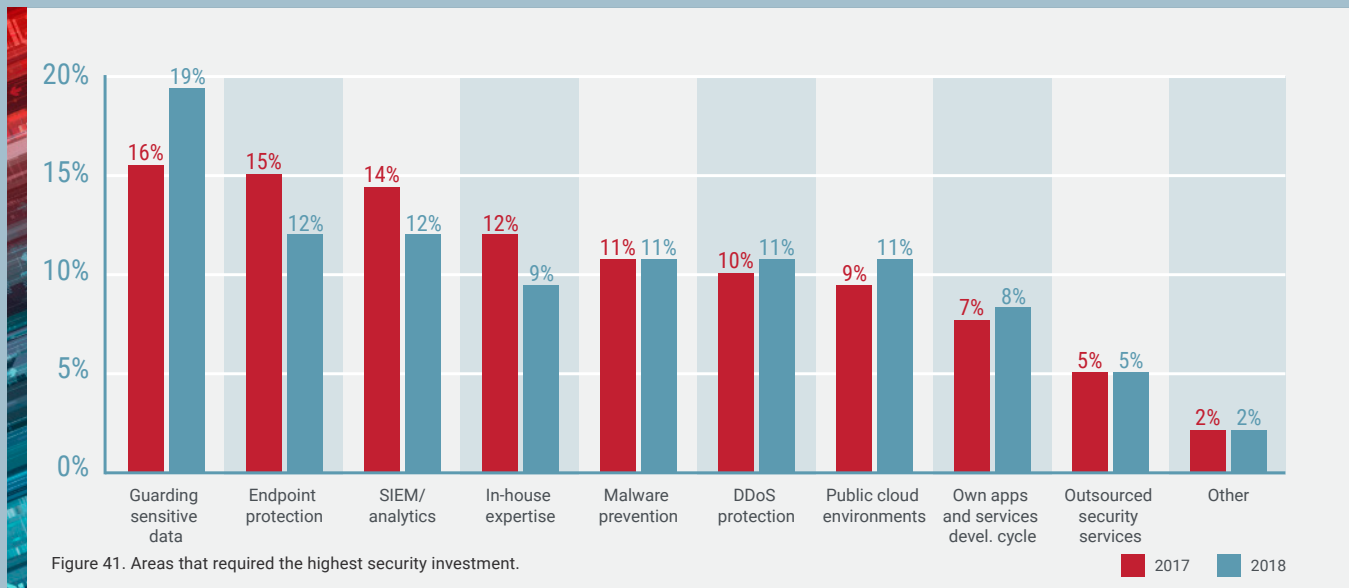
North America	Data leakage
EMEA	Reputation loss
APAC	Service outage
Latin America	Service outage

Figure 39. Common concerns as a result of cyberattacks by region.



Investment in Information Security

Survey results revealed that organizations were not making dramatic changes to their investment strategies for information security. However, there are shifts in budget allocations from endpoint protection to data security and from security staff training to cloud and DDoS protection (see Figure 41).



Adoption of Machine-Learning/AI Technologies

Meeting SLAs is critical to maintaining positive customer relationships. That is likely why hackers focus on causing service disruptions.

Machine learning and AI were on the radar of many survey respondents because the technologies promised faster and better security (see Figure 42). One-third of respondents also felt that AI solutions would help them reduce costs or gain a competitive advantage.

Blockchain Moving Toward the Mainstream

The adoption of blockchain as a way to conduct business increased 44% when compared to 2017 (see Figure 43). Nearly half of respondents said that they were either conducting or considering business activity via blockchain. About one in five larger companies, as determined by revenue and employee size, was more likely to use blockchain than smaller companies.

Businesses in APAC are most open to exploring blockchain.

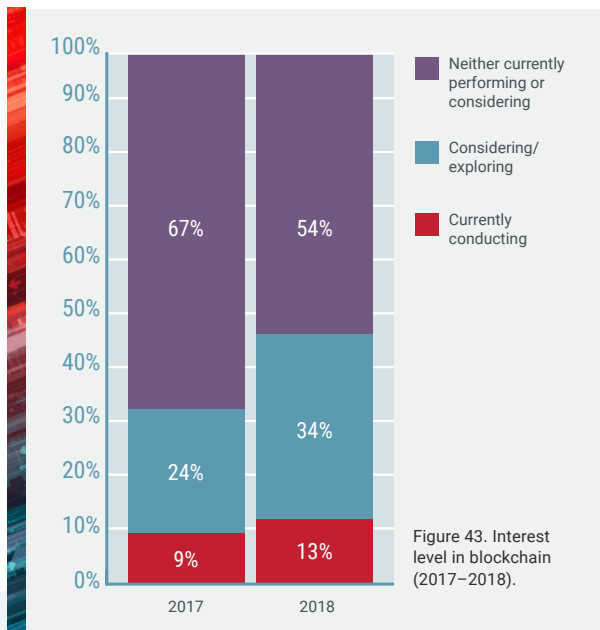
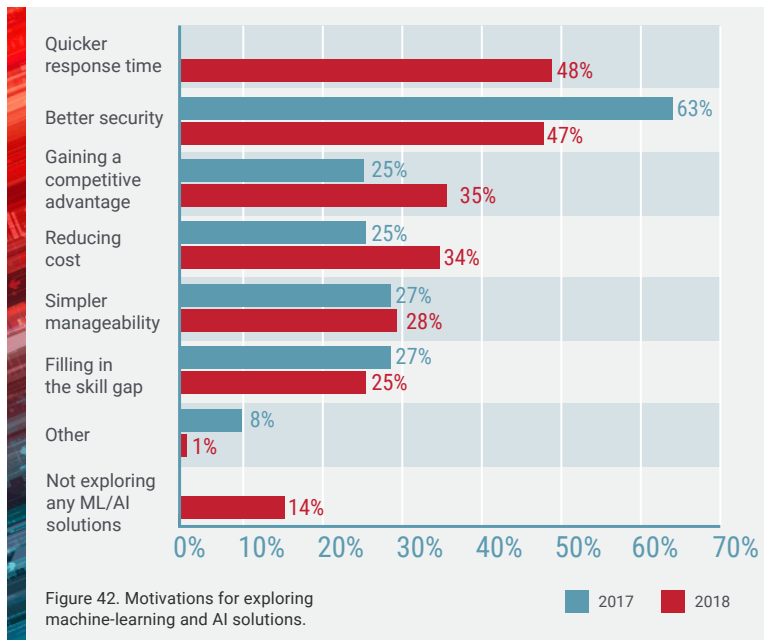
Hiring Hackers

About 30% of respondents were open to hiring hackers as part of their security strategy, consistent over the last three years. Hackers can provide real-world viewpoints and assist with forensics. Companies with revenues greater than \$1 billion are the most open to hiring hackers.

The Trust Factor

In Radware's 2018 C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts¹⁸, 41% of executives said that the threat of customer loss ranks highest as having the most impact on their businesses as a result of a cyberattack.

The pressure is on. Securing the customer experience against cyberattacks is no longer just the responsibility of the IT department. Companies need to implement security strategies as if their very survival depends on them. Information security aspects must be considered in every new business initiative, program or project. It only takes one data breach for customers to lose trust and take their business elsewhere.



¹⁸Radware, 2018 C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts



```
loop h-1080 ]
loop h-1080 +1080
(h-1080 +1080 A
(admin) ((h - hmin) break;
ActiveDocument = FromDoc
eDocument.activeLayer = activeDocument.layers
CONFIG_KEY = "MANAGER_FLAME_0
FIG_KEY = TIMER_NIM_OF_SECS"
ENTAGE = LEAK_LOG-PERCENTAGE
```

Analysis of Emerging Risks

Encrypted traffic. Hybrid cloud strategy. Mobile applications. It seems that every new technology or network development introduces new ways for attackers to try to impact business operations. What can we expect moving forward?

HTTPS: The Myth of Secure Encrypted Traffic Exposed

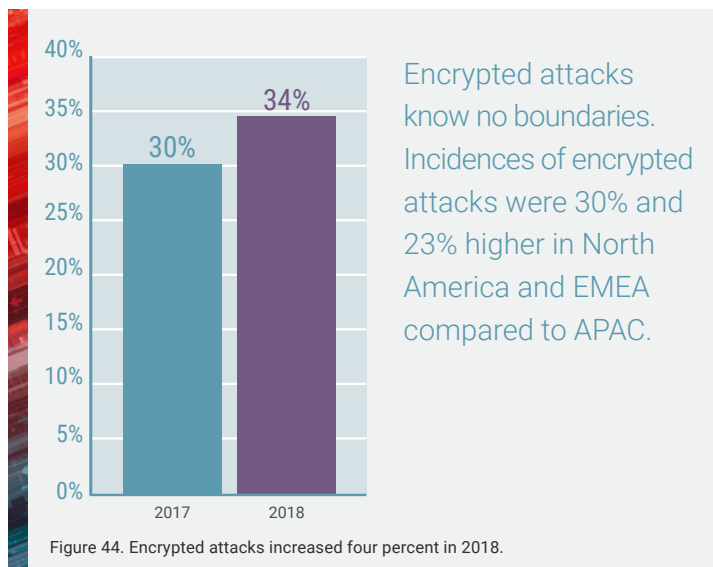
The *S* in *HTTPS* is supposed to mean that encrypted traffic is secure. For attackers, it just means that they have a larger attack surface from which to launch assaults on the applications to exploit the security vulnerabilities. How should organizations respond?

Most web traffic is encrypted to provide better privacy and security. By 2018, over 70% of webpages are loaded over HTTPS.¹⁹ Radware expects this trend to continue until nearly all web traffic is encrypted. The major drivers pushing adoption rates are the availability of free SSL certificates and the perception that clear traffic is insecure.

While encrypting traffic is a vital practice for organizations, cybercriminals are not necessarily deterred by the practice. They are looking for ways to take advantage of encrypted traffic as a platform from which to launch attacks that can be difficult to detect and mitigate, especially at the application layer. As encrypted applications grow more complex, the potential attack surface is larger. Organizations need to incorporate protection of the application layer as part of their overall network security strategies.

Results from the global industry survey revealed a 10% increase in encrypted attacks on organizations by 2018 (see Figure 44).

¹⁹ZDNet, Oct. 23, 2017, "Google: This surge in Chrome HTTPS traffic shows how much safer you now are online." Available at <https://www.zdnet.com/article/google-this-surge-in-chrome-https-traffic-shows-how-much-safer-you-now-are-online/>



Encrypted Application Layers

When planning protection for encrypted applications, it is important to consider all of the layers that are involved in delivering an application. It is not uncommon for application owners to focus on protecting the encrypted application layer while overlooking the lower layers in the stack which might be vulnerable. In many cases, protection selected for the application layer may itself be vulnerable to transport-layer attacks.

To ensure applications are protected, organizations need to analyze the following Open Systems Interconnection (OSI) layers:

Transport — In most encrypted applications, the underlying transport is TCP. TCP attacks come in many forms, so volumes and protection must be resilient to protect applications from attacks on the TCP layer. Some applications now use QUIC, which uses UDP as the underlying layer and adds reflection and amplification risks to the mix.

Session — The SSL itself is vulnerable. Once an SSL/TLS session is created, the server invests about 15 times more compute power than the client, which makes the session layer particularly vulnerable and attractive to attackers.

Application — Application attacks are the most complex type of attack, and encryption only makes it harder for security solutions to detect and mitigate them. Attackers often select specific areas in applications to generate a high request-to-load ratio, may attack several resources simultaneously to make detection harder, or may mimic legitimate user behavior in various ways to bypass common application security solutions. The size of an attack surface is determined by the application design. For example, in a login attack, botnets perform multiple login attempts from different sources to try to stress the application. The application login is always encrypted and requires resources on the application side such as a database, authentication gateway or identity service invocation. The attack does not require a high volume of traffic to affect the application, making it very hard to detect.

Environmental Aspects

Organizations also need to consider the overall environment and application structure because it greatly affects the selection of the ideal security design based on a vulnerability assessment.

Content Delivery Network — Applications using a content delivery network (CDN) generate a challenge for security controls which are deployed at the origin. Technologies that use the source IP for analyzing client application behavior only see the source IP of the CDN. There is a risk that the solutions will either overmitigate and disrupt legitimate users or become ineffective. High rates of false positives prove that protection based on source IP addresses is pointless. Instead, when using a CDN, the selected security technology should have the right measures to analyze attacks that originate behind it, including device fingerprinting or extraction of the original source from the application headers.

Application Programming Interface — Application programming interface (API) usage is common in all applications. According to Radware's *The State of Web Application Security* report, a third of attacks against APIs intends to yield a denial-of-service state. The security challenge here comes from the legitimate client side. Many solutions rely on various active user validation techniques to distinguish legitimate users from attackers. These techniques require that a real browser reside at the client. In the case of an API, many times a legitimate browser is not at the client side, so the behavior and legitimate response to various validation challenges is different.

Mobile Applications — Like APIs, the client side is not a browser for a mobile application and cannot be expected to behave and respond like one. Mobile applications pose a challenge because they rely on different operating systems and use different browsers. Many security solutions were created based on former standards and common tools and have not yet fully adapted. The fact that mobile apps process a high amount of encrypted traffic increases the capacity and security challenges.

Directionality — Many security solutions only inspect inbound traffic to protect against availability threats. Directionality of traffic has significant implications on the protection efficiency because attacks usually target the egress path of the application. In such cases, there might not be an observed change in the incoming traffic profile, but the application might still become unavailable. An effective security solution must process both directions of traffic to protect against sophisticated application attacks.

Regulatory Limitations

Major selection criterion for security solutions is regulatory compliance. In the case of encrypted attacks, compliance requirements examine whether traffic is decrypted, what parts of traffic are decrypted and where the decryption happens. The governing paradigm has always been that the more intrusive the solution, the more effective the security, but that is not necessarily the case here. Solutions show different levels of effectiveness for the same intrusiveness.

Encryption Protocols

The encryption protocol in use has implications toward how security can be applied and what types of vulnerabilities it represents. Specifically, TLS 1.3 generates enhanced security from the data privacy perspective but is expected to generate challenges to security solutions which rely on eavesdropping on the encrypted connection. Users planning to upgrade to TLS 1.3 should consider the future resiliency of their solutions.

Attack Patterns

Determining attack patterns is the most important undertaking that organizations must master. Because there are so many layers that are vulnerable, attackers can easily change their tactics midattack. The motivation is normally twofold: first, inflicting maximum impact with minimal cost; second, making detection and mitigation difficult.

Distribution — The level of attack distribution is very important to the attacker. It impacts the variety of vectors that can be used and makes the job harder for the security controls. Most importantly, the more distributed the attack, the less traffic each attacking source has to generate. That way, behavior can better resemble legitimate users. Gaining control of a large botnet used to be difficult to do and extremely costly. With the growth in the IoT and corresponding IoT botnets, it is common to come across botnets consisting of hundreds of thousands of bots.

Overall Attack Rates — The overall attack traffic rate varies from one vector to another. Normally, the lower the layer, the higher the rate. At the application layer, attackers are able to generate low-rate attacks, which still generate significant impact. Security solutions should be able to handle both high- and low-rate attacks, without compromising user experience and SLA.

Rate per Attacker — Many security solutions in the availability space rely on the rate per source to detect attackers. This method is not always effective as highly distributed attacks proliferate.

Connection Rates — Available attack tools today can be divided into two major classes based on their connection behavior. The first class includes tools that open a single connection and generate many. The second includes tools that generate many connections with only a single request or very few requests on each connection. Security tools that can analyze connection behavior are more effective in discerning legitimate users from attackers.

Session Rates — SSL/TLS session behavior has various distinct behavioral characteristics in legitimate users and browsers. The major target is to optimize performance and user experience. Attack traffic does not usually fully adhere to those norms, so its SSL session behavior is different. The ability to analyze encryption session behavior contributes to protecting both the encryption layer and the underlying application layer.

Application Rates — Because the application is the most complex part to attack, attackers have the most degree of freedom when it comes to application behavior. Attack patterns vary greatly from one attack to another in terms of how they appear on application behavior analyses. At the same time, the rate of change in the application itself is very high, such that it cannot be followed manually (see Figure 45). Security tools that can automatically analyze a large variety of application aspects and, at the same time, adapt to changes quickly are expected to be more effective in protecting from encrypted application attacks.

About one-quarter of all application types changed on a daily basis, making it difficult for network security protocols to keep pace.

Source: 2018 Radware State of Application Security Study

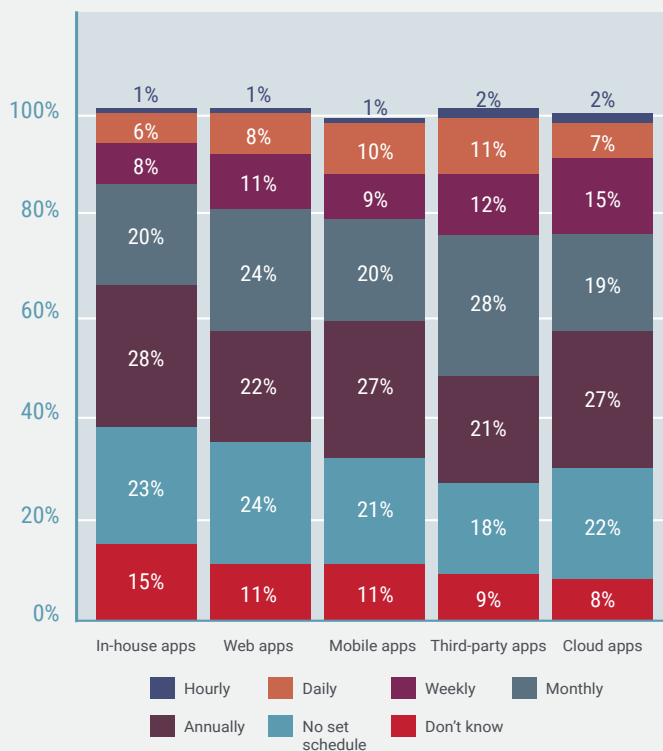


Figure 45. Frequency of application changes.

End-to-End Protection

Protection from encrypted availability attacks is becoming a mandatory requirement for organizations. At the same time, it is one of the more complex tasks to thoroughly perform without leaving blind spots. When considering a protection strategy, it is important to take into account various aspects of the risk and to make sure that, with all good intentions, the side door is not left open.

Time to Take Charge: Ensuring Data Privacy in Public Clouds

In 2018, Radware saw a continuation of the trend for enterprises to host more applications and data in the public cloud with Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform and a variety of other service providers (see Figure 46). The transition is a strategic move by companies to transform infrastructure operations, improve the customer experience and reduce costs. Radware expects to see an accelerated shift to utilizing infrastructure as a service in 2019.

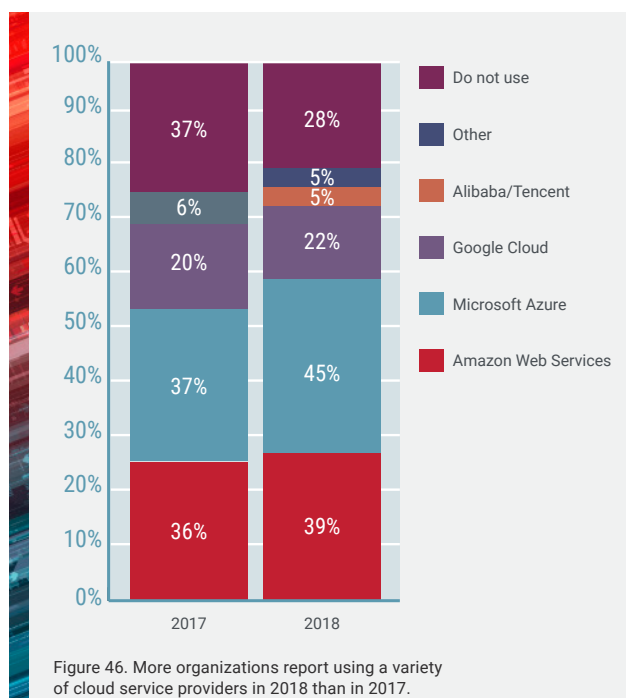


Figure 46. More organizations report using a variety of cloud service providers in 2018 than in 2017.

Most enterprises spread data and applications across multiple cloud providers, typically referred to as a multicloud approach. While it is in the best interest of public cloud providers to offer network security as part of their service offerings, every public cloud provider utilizes different hardware and software security policies, methods and mechanisms, creating a challenge for the enterprise to maintain the exact same policy and configuration across all infrastructures. Public cloud providers typically meet basic security standards in an effort to standardize how they monitor and mitigate threats across their entire customer base. Seventy percent of organizations reported using public cloud providers with varied approaches to security management (see Figure 47).

Moreover, enterprises typically prefer neutral security vendors instead of overrelying on public cloud vendors to protect their workloads. As the multicloud approach expands, it is important to centralize all security aspects.

Using Public Cloud Providers	2018
Yes	70%
Yes, customized	29%
Yes, but I handle some aspects	22%
Yes, their default setting	19%
Our IT handles selection, implementation and configuration	23%
I rely on a local cloud provider for security management	5%
Other	2%

Figure 47. Reliance on public cloud infrastructure providers to secure cloud applications.

When Your Inside Is Out, Your Outside Is In

Moving workloads to publicly hosted environments leads to new threats, previously unknown in the world of premise-based computing. Computing resources hosted inside an organization's perimeter are more easily controlled. Administrators have immediate physical access, and the workload's surface exposure to insider threats is limited.

When those same resources are moved to the public cloud, they are no longer under the direct control of the organization. Administrators no longer have physical access to their workloads. Even the most sensitive configurations must be done from afar via remote connections. Putting internal resources in the outside world results in a far larger attack surface with long, undefined boundaries of the security perimeter.

In other words, when your inside is out, then your outside is in.

External threats that could previously be easily contained can now strike directly at the heart of an organization's workloads. Hackers can have identical access to workloads as do the administrators managing them. In effect, the whole world is now an insider threat.

In such circumstances, restricting the permissions to access an organization's workloads and hardening its security configuration are key aspects of workload security.

Promiscuous Permissions Leave You Exposed

Cloud environments make it very easy to grant access permissions and very difficult to keep track of who has them. With customer demands constantly increasing and development teams put under pressure to quickly roll out new enhancements, many organizations spin up new resources and grant excessive permissions on a routine basis. This is particularly true in many DevOps environments where speed and agility are highly valued and security concerns are often secondary.

Over time, the gap between the permissions that users have and the permissions that they actually need (and use) becomes a significant crack in the organization's security posture. Promiscuous permissions leave workloads vulnerable to data theft and resource exploitation should any of the users who have access permissions to them become compromised. As a result, misconfiguration of access permissions (that is, giving permissions to too many people and/or granting permissions that are overly generous) becomes the most urgent security threat that organizations need to address in public cloud environments.

The Glaring Issue of Misconfiguration

Public cloud providers offer identity access management tools for enterprises to control access to applications, services and databases based on permission policies. It is the responsibility of enterprises to deploy security policies that determine what entities are allowed to connect with other entities or resources in the network. These policies are usually a set of static definitions and rules that control what entities are valid to, for example, run an API or access data.

One of the biggest threats to the public cloud is misconfiguration. If permission policies are not managed properly by an enterprise will the tools offered by the public cloud provider, excessive permissions will expand the attack surface, thereby enabling hackers to exploit one entry to gain access to the entire network.

Moreover, common misconfiguration scenarios result from a DevOps engineer who uses predefined permission templates, called *managed permission policies*, in which the granted standardized policy may contain wider permissions than needed. The result is excessive permissions that are never used. Misconfigurations can cause accidental exposure of data, services or machines to the internet, as well as leave doors wide open for attackers.

For example (see Figure 48), an attacker can steal data by using the security credentials of a DevOps engineer gathered in a phishing attack. The attacker leverages the privileged role to take a snapshot of elastic block storage (EBS) to steal data, then shares the EBS snapshot and data on an account in another public network without installing anything. The attacker is able to leverage a role with excessive permissions to create a new machine at the beginning of the attack and then infiltrate deeper into the network to share AMI and RDS snapshots (Amazon Machine Images and Relational Database Service, respectively), and then unshare resources.

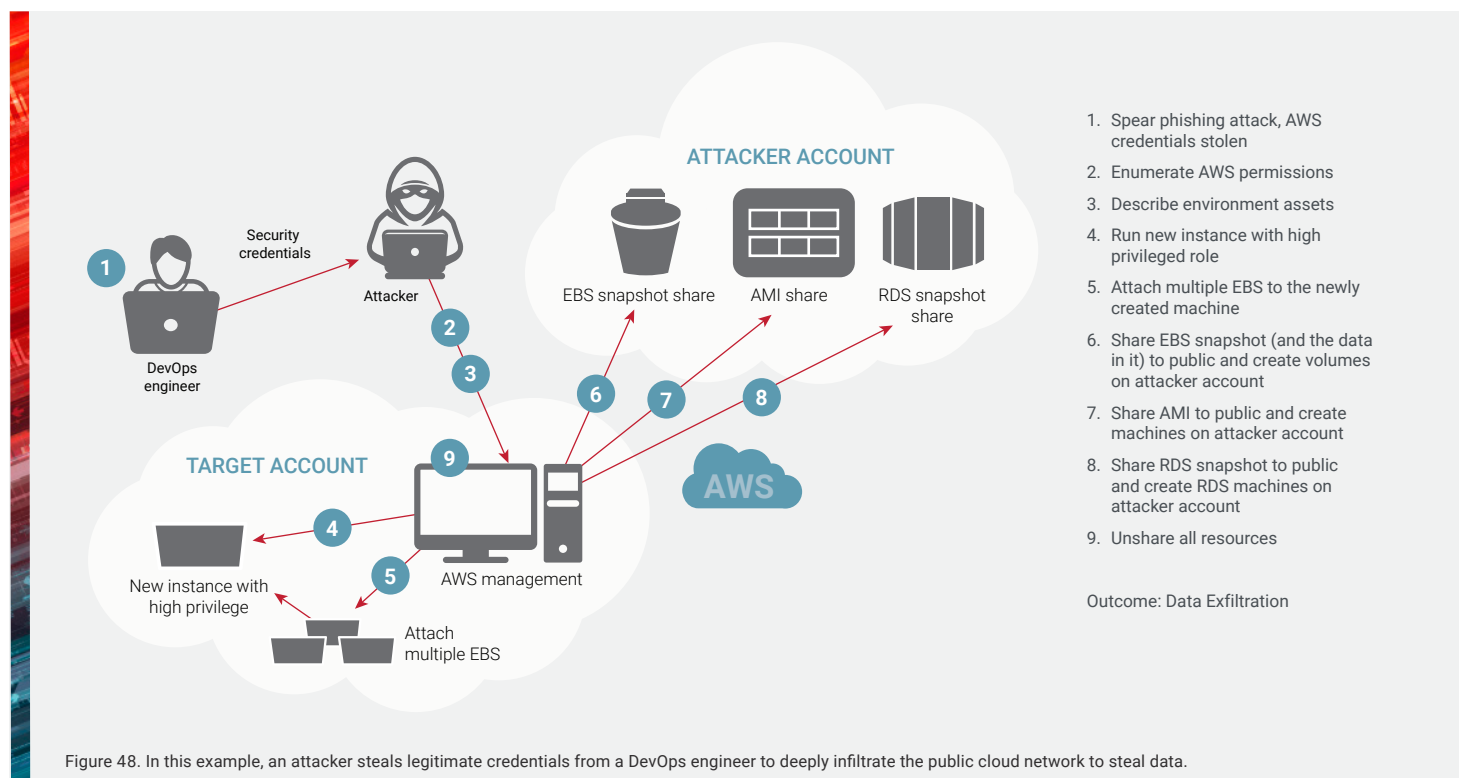
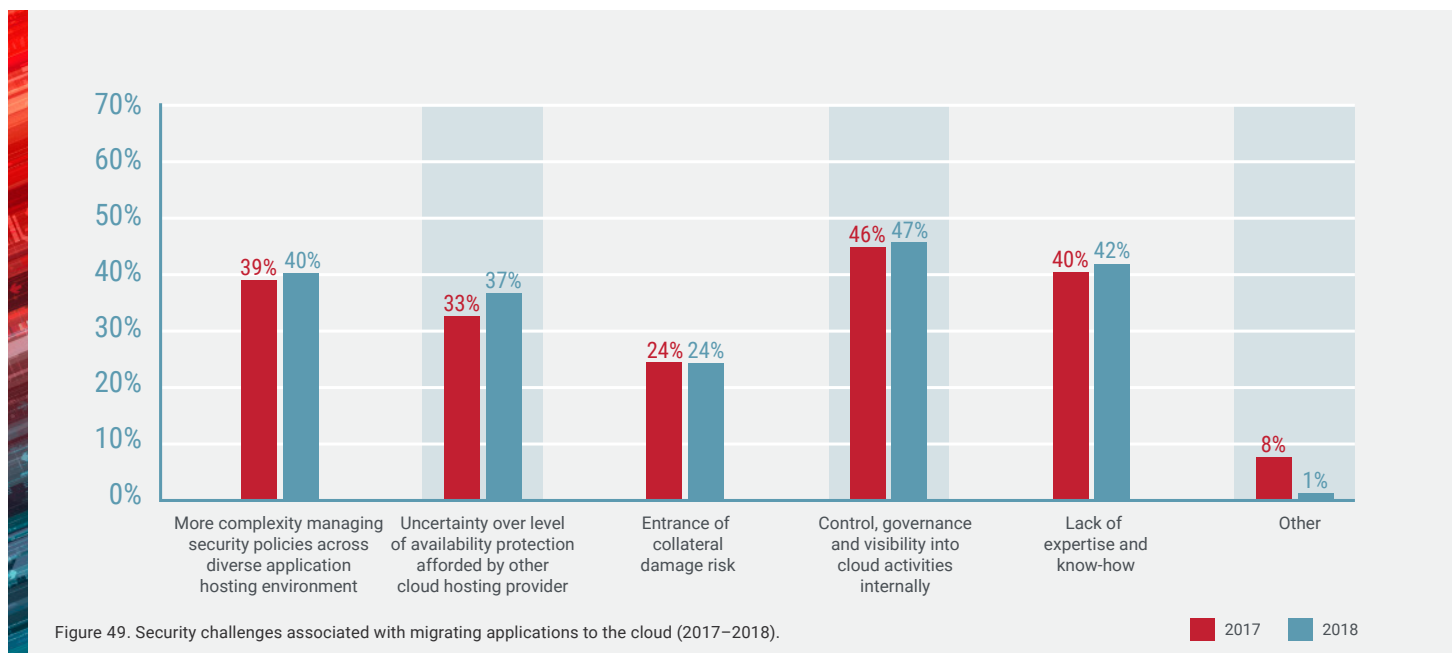


Figure 48. In this example, an attacker steals legitimate credentials from a DevOps engineer to deeply infiltrate the public cloud network to steal data.



Year over year in Radware's global industry survey, the most frequently mentioned security challenges encountered with migrating applications to the cloud are governance issues followed by skill shortage and complexity of managing security policies (see Figure 49). All contribute to the high rate of excessive permissions.

Cause and Effect

The main causes of misconfigurations vary. In many cases, enterprises simply lack visibility into the cloud environment and resources and do not understand what they are responsible for to determine, maintain and update permissions. Or, because applications and services are very dynamic with frequent (many times daily or weekly) changes, permissions are misconfigured because the enterprise DevSecOps is not keeping pace. Sadly, shortage in human capital and expertise also has an impact. Recruiting, training and retaining security professionals is a constant challenge in today's market. It gets even worse when the enterprise has a multicloud approach in which the operation teams need to understand and control multiple, diverse environments. As a result, many enterprises go to cloud service providers expecting to offload these concerns. However, the liability to protect sensitive data while managing the customer experience does not go away.

The negative impact of misconfigurations to the trust enterprises have with their customers can be high:

- ▶ Unauthorized access to systems
- ▶ Exposure of sensitive data to the public
- ▶ Unauthorized access to data and resources
- ▶ Violation of compliance standards
- ▶ Service disruption
- ▶ Erosion of confidence

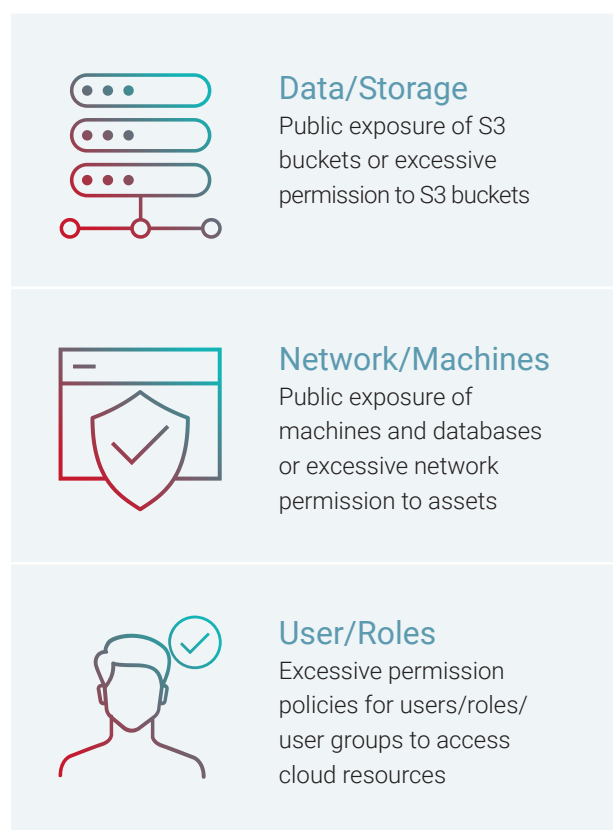
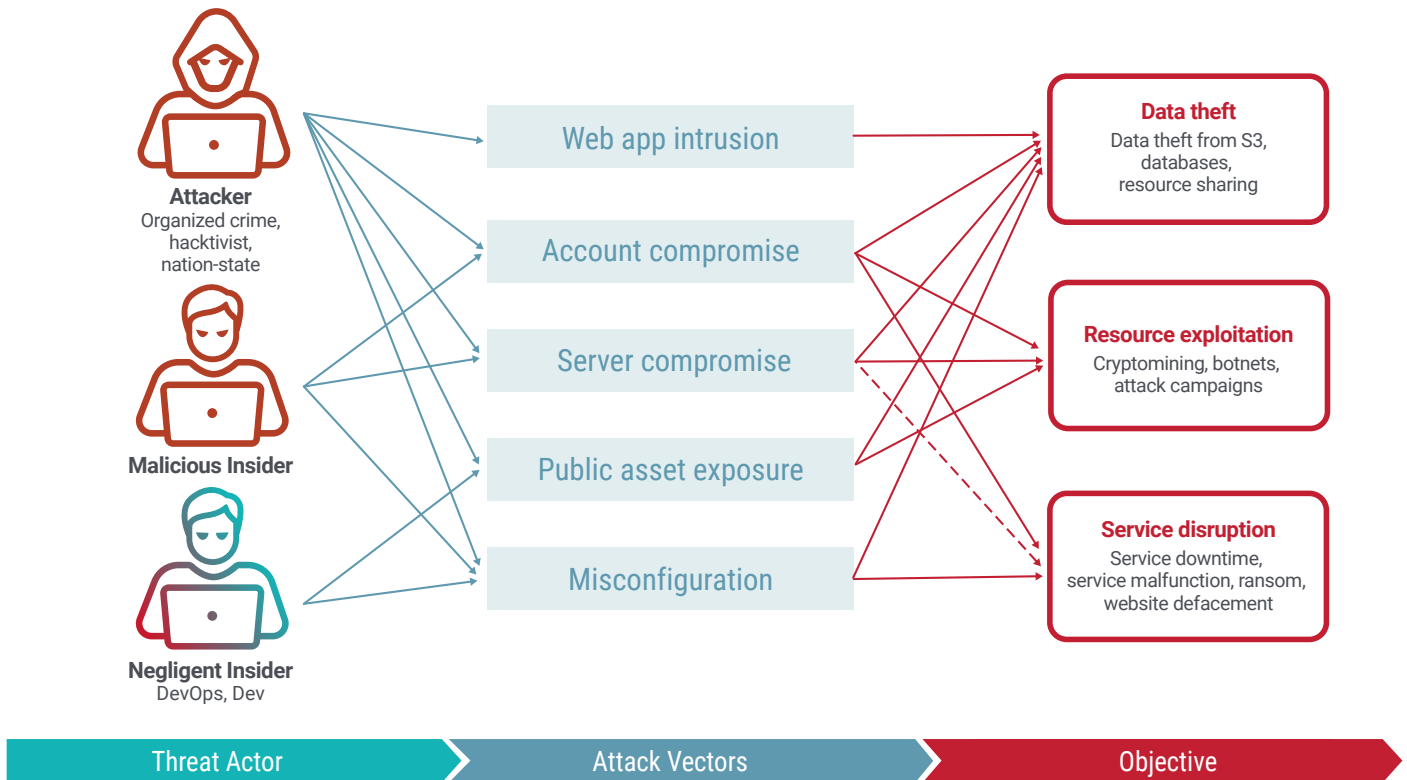


Figure 50. Misconfigurations are apparent in several areas in the cloud.

Attacking the Cloud

For attackers, misconfigurations in the public cloud can be exploited for a number of reasons. Radware created a public cloud threat map (see Figure 51) that identifies types of attackers, what attack vectors they use and their motivations for launching attacks.



Threat Actor: Attackers such as cybercriminals, hackers and nation-state-sponsored attackers have malicious intent. Malicious insiders are legitimate users who exploit their legitimate privileges to cause harm. Negligent users are legitimate users such as Dev/DevOps engineers who make configuration mistakes, or essentially any corporate employee with access that practices low security hygiene. The latter has the higher risk potential among the threat actor personas.

In the cloud environment, the **Negligent Insider** controls the environment from the **outside world**. When your inside is out, then your outside is in. With this situation, excessive permissions essentially become promiscuous permissions.

The Radware global industry survey revealed that 75% of organizations run information security-related employee education programs to reduce the risk of negligent users.

Attack Vectors: Threat actors utilize multiple attack vectors to launch attacks depending on the ultimate objectives.

Objective: Radware's 2018–2019 *Global Application & Network Security Report* revealed that the purpose of more than a third of cyberattacks was data theft. Sensitive PII resided in S3/databases/repositories, and resources are shared between accounts. Other attacks were meant to exploit cloud resources for endless compute power, commonly to perform cryptocurrency/cryptojacking activity.

Figure 51. The Radware public cloud threat map.

Typical attack scenarios include several kill chain steps, such as reconnaissance, lateral movement, privilege escalation, data acquisition, persistence and data exfiltration. These steps might be fully or partially utilized by an attacker over dozens of days until the ultimate objective is achieved and the attacker reaches the valuable data.

Web application intrusion (25%) and misconfiguration (21%) were the biggest threats to a company's cloud environment (see Figure 52). DDoS attacks and credential theft were more of a concern in EMEA and APAC. Credential theft has been a major factor in recent data leaks.

Removing the Mis from Misconfigurations

To prevent attacks, enterprises must harden configurations to address promiscuous permissions by applying continuous hardening checks to limit the attack surface as much as possible. The goals are to avoid public exposure of data from the cloud and reduce overly permissive access to resources by making sure communication between entities within a cloud, as well as access to assets and APIs, are only allowed for valid reasons.

For example, the private data of six million Verizon users was exposed when maintenance work changed a configuration and made an S3 bucket public.

Only smart configuration hardening that applies the approach of "least privilege" enables enterprises to meet those goals. The process requires applying behavior analytics methods over time, including regular reviews of permissions and a continuous analysis of usual behavior of each entity, just to ensure users only have access to what they need, nothing more. By reducing the attack surface, enterprises make it harder for hackers to move laterally in the cloud.

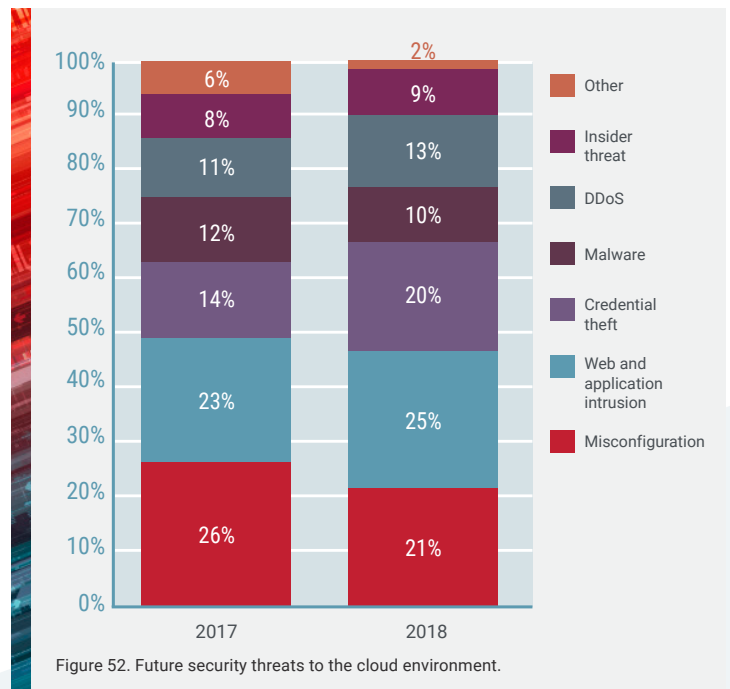
The process is complex and is often best managed with the assistance of an outside security partner with deep expertise and a system that combines a lot of algorithms that measure activity across the network to detect anomalies and determine if malicious intent is probable. Often attackers will perform keychain attacks over several days or months.

Taking Responsibility

It is tempting for enterprises to assume that cloud providers are completely responsible for network and application security to ensure the privacy of data. In practice, cloud providers provide tools that enterprises can use to secure hosted assets. While cloud providers must be vigilant in how they protect their data centers, responsibility for securing access to apps, services, data repositories and databases falls on the enterprises.

Hardened network and meticulous application security can be a competitive advantage for companies to build trust with their customers and business partners. Now is a critical time for enterprises to understand their role in protecting public cloud workloads as they transition more applications and data away from on-premise networks.

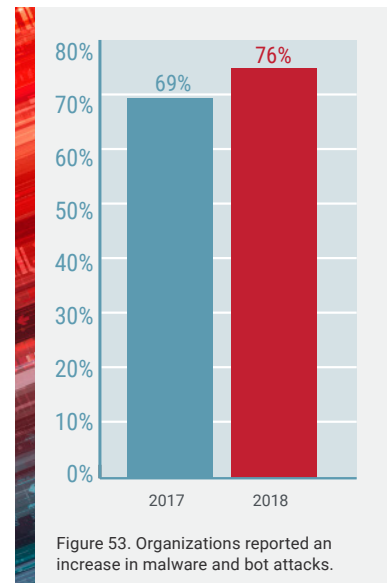
The responsibility to protect the public cloud is a relatively new task for most enterprises. But, everything in the cloud is external and accessible if it is not properly protected with the right level of permissions. Going forward, enterprises must quickly incorporate smart configuration hardening into their network security strategies to address this growing threat.



Adapting Application Security to the New World of Bots

In 2018, organizations reported a 10% increase in malware and bot attacks (see Figure 53). Considering the pervasiveness (70%) of these types of attacks reported in 2017, this uptick is likely having a big impact on organizations globally. Compounding the issue is the fact that the majority of bots are actually leveraged for good intentions, not malicious ones. As a result, it is becoming increasingly difficult for organizations to identify the difference between the two, according to Radware's *Web Application Security in a Digitally Connected World*²⁰ report (see Figure 54).

Bots are automated programs that run independently to perform a series of specific tasks, for example, collecting data. Sophisticated bots can handle complicated interactive situations. More advanced programs feature self-learning capabilities that can address automated threats against traditional security models.



4 out of 5

CISOs cannot make a clear distinction between good and bad bots.²¹



Figure 54.

²⁰<https://www.radware.com/webapplicationsecurityreport/>

²¹<https://www.radware.com/pleaseregister.aspx?returnurl=277d9c3a-1cfc-4f80-9f78-3e22e2de0378>

How Do Bots Affect the Business?

Positive Impact: Business Acceleration

Automated software applications can streamline processes and positively impact overall business performance. They replace tedious human tasks and speed up processes that depend on large volumes of information, thus contributing to overall business efficiency and agility.

Good bots include:

- ▶ **Crawlers** – are used by search engines and contribute to SEO and SEM efforts
- ▶ **Chatbots** – automate and extend customer service and first response
- ▶ **Fetchers** – collect data from multiple locations (for instance, live sporting events)
- ▶ **Pricers** – compare pricing information from different services
- ▶ **Traders** – are used in commercial systems to find the best quote or rate for a transaction

Negative Impact: Security Risks

The Open Web Application Security Project (OWASP) lists 21 automated threats to applications that can be grouped together by business impacts:

- ▶ **Scraping and Data Theft** – Bots try to access restricted areas in web applications to get a hold of sensitive data such as access credentials, payment information and intellectual property. One method of collecting such information is called web scraping. A common example for a web-scraping attack is against e-commerce sites where bots quickly hold or even fully clear the inventory.
- ▶ **Performance** – Bots can impact the availability of a website, bringing it to a complete or partial denial-of-service state. The consumption of resources such as bandwidth or server CPU immediately leads to a deterioration in the customer experience, lower conversions and a bad image. Attacks can be large and volumetric (DDoS) or not (low and slow, buffer overflow).
- ▶ **Poisoning Analytics** – When a significant portion of a website's visitors are fictitious, expect biased figures such as fraudulent links. Compounding this issue is the fact that third-party tools designed to monitor website traffic often have difficulty filtering bot traffic.
- ▶ **Fraud and Account Takeover** – With access to leaked databases such as Yahoo and LinkedIn, hackers use bots to run through usernames and passwords to gain access to accounts. Then they can access restricted files, inject scripts or make unauthorized transactions.
- ▶ **Spammers and Malware Downloaders** – Malicious bots constantly target mobile and web applications. Using sophisticated techniques like spoofing their IPs, mimicking user behavior (keystrokes, mouse movements), abusing open-source tools (PhantomJS) and headless browsers, bots bypass CAPTCHA, challenges and other security heuristics (see Figure 55).

Methods used by bots to bypass security challenges.



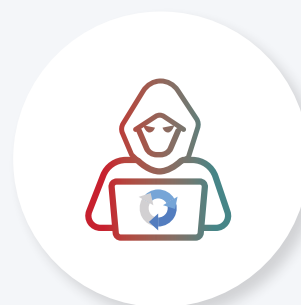
Spoofing their IPs



Mimicking user behavior



Abusing open-source application testing tools (such as PhantomJS)



Bypass CAPTCHA

Figure 55.

Password Cracking by Bots Brings an Airline to DoS

A global airline turned to Radware for emergency support in the spring because it was the target of a persistent campaign against its website. Perpetrators used bots to generate a low-rate DoS attack, hiding their identities behind anonymous proxies and Tor proxies. Attackers targeted login pages with a high number of POST requests with invalid credentials in order to exhaust the server and cause denial of service (see Figure 56).

```

{"username":"23352353","password":"1900","rd":false}HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin:
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Type: application/json;charset=UTF-8
Date: Fri, 11 May 2018 19:33:24 GMT
Expires: 0
Pragma: no-cache
Set-Cookie: AuSALBwK7p8Y2y1iv7gkstoIT9e1u8IMy20N5J0S2zvo/
9YVAUQWJv0ytJ2DJVE5OX98EQSpj26AXLYEEf789YZa8axEPTcJKIPR13av8CwC9rPk4vchFRxznTH00P0KGAuxS8yB0H/
OkuFIdt1P84t+20mAP6GkEHFehha3ntpSelLC6LIDY0x4eA==; Expires=Fri, 18 May 2018 19:33:22 GMT; Path=/
Content-Length: 113
Connection: keep-alive

{"path":", "message":"Invalid user
credentials.", "code":14, "time":"2018-05-11T19:33:24.571Z"}
    
```

Figure 56. Example of an attack on a website using invalid credentials.

The attack lasted a week, at times exceeding 8,000 Brute Force attempts daily (see Figure 57). The bots first scanned the website looking for vulnerable pages. They relied on a wide IP proxy pool (IPs coming from 27 countries) and performed extremely low request counts so as not to trigger DDoS alerts.

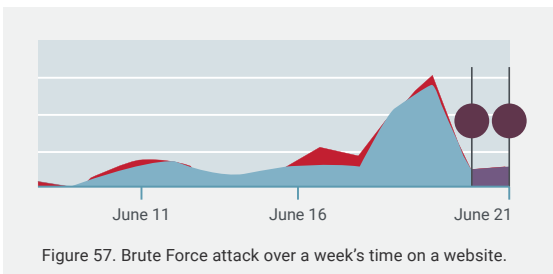


Figure 57. Brute Force attack over a week's time on a website.

The attackers used various combinations of characters trying to get through login and access the data stored at the web server (see Figure 58).

To identify the origin of the high number of bots, Radware found hostile hosts known for aggressive spam and hosts that service many fake domains that return empty responses. Some belonged to spy proxy service, including a popular online game.

Radware saw attackers frequently change the domain to avoid detection by domain reputation services. The attackers also spoofed their IPs to make mitigation even more complex and improve the success rate of the attack (see Figure 59).

The bot uses consecutive numbers – which are obviously fictitious – of IP addresses that belong to benign machines. This tactic makes an IP-based mitigation approach obsolete and also creates a high rate of false positives.

How Bot Attacks Make IP-Based Protection Obsolete

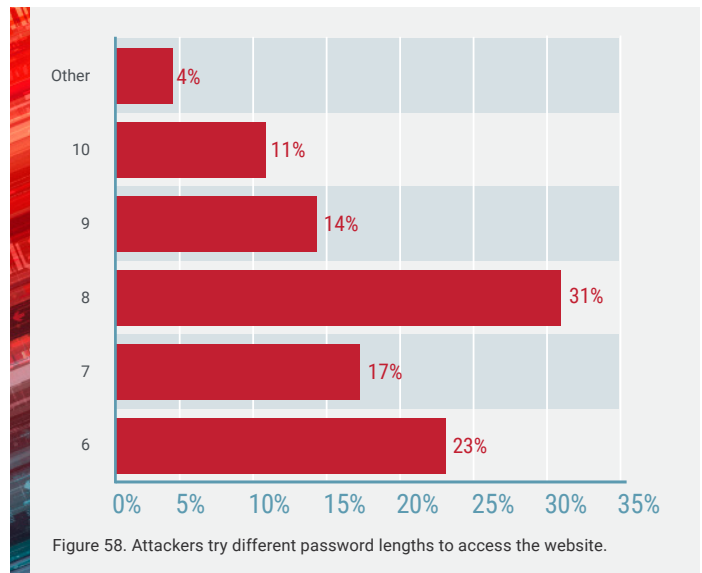
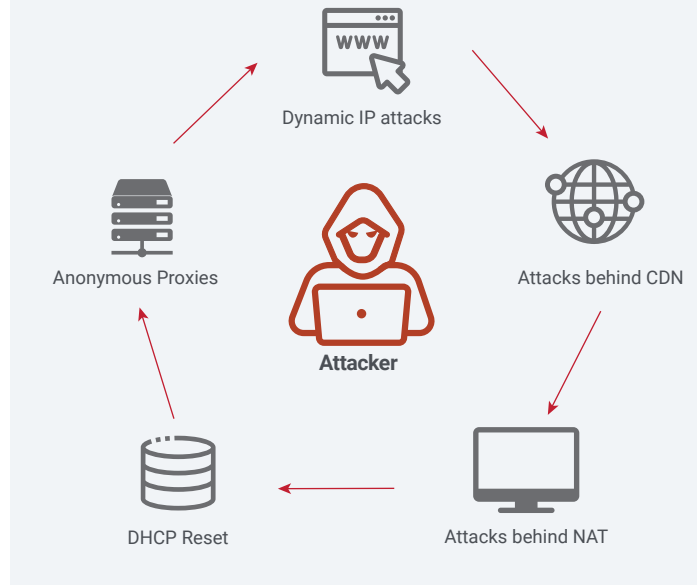


Figure 58. Attackers try different password lengths to access the website.

Generated By	Reported On	GEO	Source IP
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.126
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.168
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.170
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.171
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.172
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.173
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.174
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.175
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.176
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.177
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.178
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.179
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.180
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.181
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.182
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.183
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.15.184
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.16.104
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.16.105
Attacks - Activity Tracking	Web Applications - (S)	Ukraine	213.155.16.106

Figure 59. Example of a spoofed IP attack.

Blocking Automated Threats

Gawky bot attacks against websites are easy to block by IP and reputation-based signatures and rules. However, because of the increase in sophistication and frequency of attacks, it is important to be able to uniquely identify the attacking machine. This process is referred to as device fingerprinting. The process should be IP agnostic and yet unique enough to be confident to act upon. At times, resourceful attacking sources may actively try to manipulate the fingerprint extracted from the web tool, so it should also be client-side manipulation proof.



Figure 60. Device fingerprinting helps identify attacking machines.

Web client fingerprint technology introduces significant value in the context of automated attacks, such as web scraping; Brute Force and advanced availability threats, such as HTTP Dynamic Flood; and low and slow attacks, where the correlation across multiple sessions is essential for proper detection and mitigation.

For each fingerprint-based, uniquely identified source, a historical track record is stored with all security violations, activity records and application session flows. Each abnormal behavior is registered and scored. Violation examples include SQL injection, suspicious session flow and high page access rate. Once a threshold is reached, the source with the marked fingerprint will not be allowed to access the secured application.

Taking the Good with the Bad

Ultimately, understanding and managing bots isn't about crafting a strategy driven by a perceived negative attitude toward bots because, as we've explained, bots serve many useful purposes for propelling the business forward. Rather, it's about equipping your organization to act as a digital detective to mitigate malicious traffic without adversely impacting legitimate traffic.

Organizations need to embrace technological advancements that yield better business performance while integrating the necessary security measures to guard their customer data and experience.

Q&A: Looking Past the Hype to Discover the Real Potential of AI

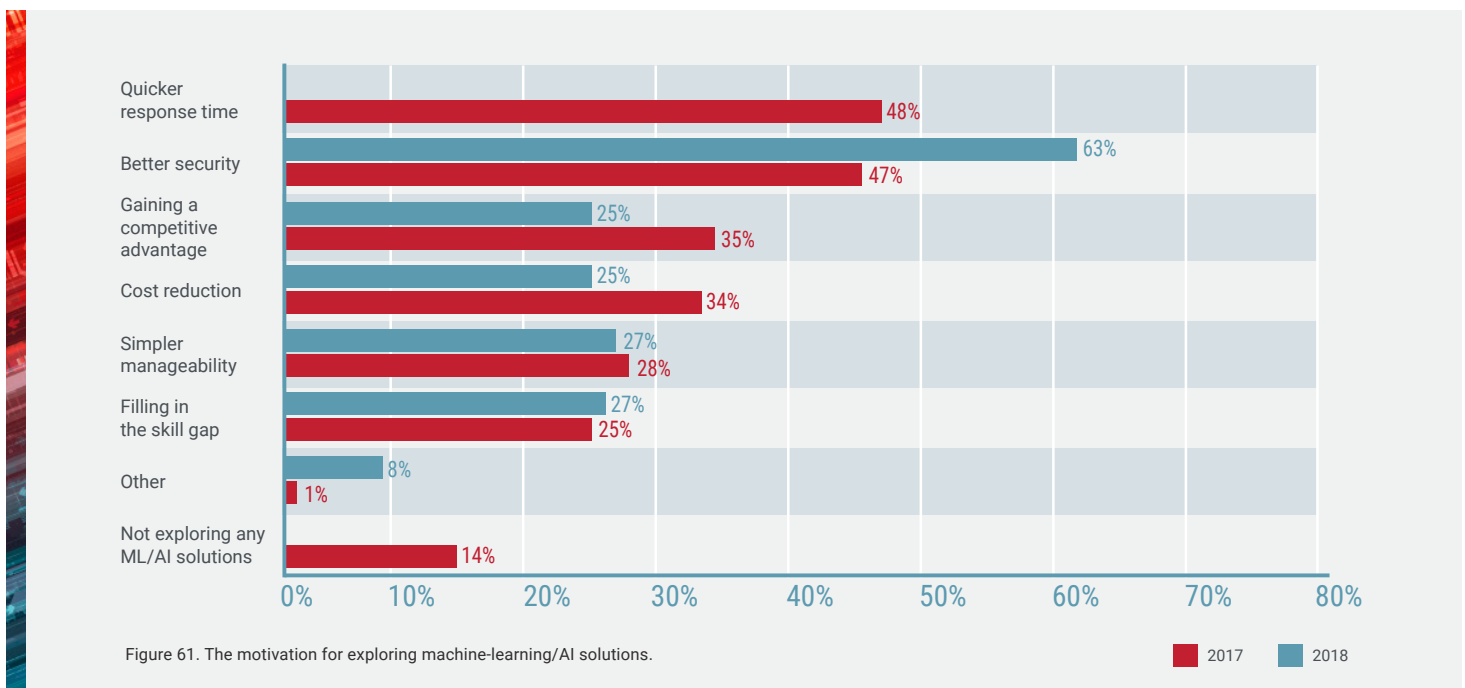
Radware's Security Evangelist Pascal Geenens talks realities and myths regarding AI, reminds us that it is a tool for both security vendors and cyberattackers, and shares his thoughts on how it affects the threat landscape.

The hype around AI has been big in recent years. Every time a new network security technology is introduced, you can be sure terms such as *deep learning*, *machine learning*, *self-learning algorithms*, *cognitive analytics* and *neural networks* are part of the pitch. But the industry's focus on AI as a way to boost protection against threats ignores the larger problem: self-learning attackers.

Security is not the only primary motivation to move toward AI-based solutions. Business efficiency is another principal driver (see Figure 61). The global industry survey revealed that businesses had high expectations when implementing AI solutions and wanted multiple benefits from their investments.

Radware's *IoT Attack Handbook: A Field Guide to Understanding IoT Attacks from the Mirai Botnet to Its Modern Variants*²² is a warning about one of the fastest growing threats in the security landscape: bots that adapt as they seek to cause harm. We continue to see developments in the chess game of machines trying to deceive each other as they try to steal or protect information. The interplay is fascinating from a technology perspective. Mostly what's happening is horrifying because, even though more robust solutions are available, most organizations continue to rely on older technologies and paradigms to defend against these evolving threats.

How can organizations cut through the hype around AI to understand the most important issues they should be addressing? How can they incorporate AI into their security strategies now to take advantage of the technology's ability to detect and mitigate attacks that incorporate the same capabilities? Pascal Geenens, Radware's EMEA security evangelist, weighs in.



²²<https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=2d2d8117-696d-45f5-a706-c54a6407180e>

1. What is the threat landscape, and how disruptive is it likely to be?

In the near term, cybercriminals will mainly use AI to automate attacks and improve evasion capabilities against detection systems and to increase the scale and reach of the threats. Expect to see AI used to automatically breach defenses and generate more sophisticated phishing attacks from information scraped from publicly accessible web sources. The scale of attacks will quickly escalate to volumes that we have never experienced before.

On the evasive side, machine-learning systems such as generative adversarial networks (GANs) can automatically create malware that is harder to detect and block. This technique has already been demonstrated by researchers. The MalGAN research project proposed a GAN to create evasive malware that goes undetected by all modern anti-malware systems, even the systems based on deep learning.²³

In the first phase, AI will be used to improve current attack tools to make them more harmful and difficult to detect. Machine learning and automation can be leveraged to find new vulnerabilities, especially in large public clouds where cloud native systems are being built based on widely reused open-source software frameworks. Platforms running this software will become primary targets for vulnerability scanning.

Given that open-source code is readable and accessible by both criminals and security researchers, this platform may become the next battlefield with an associated “arms race” to discover, abuse or fix vulnerabilities. Deep learning will provide an advantage in discovering new vulnerabilities based on code. While open source is an easier target, even closed-source software will not escape automated attacks based on the learning process of the attack program.

Looking further ahead, I can imagine large cybercrime organizations or nation-states using AI. Where machine learning was previously used mainly for automating attacks, now AI systems such as genetic algorithms and reinforced learning will be used to automatically generate new attack vectors and breach all kinds of systems, whether cloud, IoT or ICS. Then, combine this capability with the automation of the first stage. We will face a fully automated, continuously evolving attack ecosystem that will hack, crack and improve itself over time with no limits in scale or endurance.

Cybercriminals could move from being the actual hackers, performing the real attack and penetrating defenses, to becoming maintainers and developers of the automated AI hacking machine. Machines will do the hacking; humans will focus on improving efficiency of the machines.

2. What vulnerabilities will make targets more attractive to criminals once AI is incorporated in their tools? How will it affect corporate espionage?

Ultimately every organization will be digitally transformed and become a primary target for automated attacks. Which targets are chosen will be solely dependent on the objective of the attack. For ransom and extortion, every organization is a good candidate target. For corporate espionage, it depends how much organizations are willing to pay to secure intellectual property in certain areas. It's fair to say that, by definition, every organization can — and, at some point, will — be a target.

3. What about politically motivated cyberattacks initiated at the national level?

We've already witnessed attacks meant to influence public opinion and the political landscape. Such attacks are likely to grow and become more difficult to identify early in the process and to protect against once attackers leverage deep learning and broader AI technologies. Attackers have already produced automatically generated messages and discussions, as well as “deep fake”²⁴ videos that are created by AI algorithms.

Influencing what topics are important and manipulating opinions are becoming new weapons of choice for nation-states. Social platform providers need to take a stance and remain as clean as possible by dedicating much of their own AI-assisted automated detection systems to stay ahead of cybercriminals and others that create and improve AI-assisted automated systems for fake content creation.

²³<https://arxiv.org/abs/1702.05983>

²⁴<https://www.bloomberg.com/news/videos/2018-09-26/it-s-getting-harder-to-spot-a-deep-fake-video-video>

4. From a defense perspective, what types of AI-based products will be used to combat more technologically savvy cybercriminals?

There's a saying in our industry that "you cannot stop what you cannot detect." Cybersecurity has become automated for the sake of the detection of new, increasingly complex and continuously adapting threats, and deep learning is improving that capability. AI, in the broad sense of the term, will probably come into play in the near-term future rather than immediately. The current state of AI in the defense discussion is confined to the traditional machine learning, and while deep learning shows a lot of promise, it is still too challenged to be used for automated mitigation. More intelligent and self-adaptive systems, the domain of AI, are still further out when it comes to automating our cyberdefenses.

Machine Learning

By definition, an AI system improves and adapts to its environment. In most AI-based security systems, the technology today is mainly based on machine learning. Machine learning consists of a vast collection of algorithms, including deep neural networks. While those algorithms have the capability to improve the quality of their prediction over time, they still perform a single, specific task. The amount of data needed to be effective will depend on whether that system is based on traditional (nondeep learning) machine learning or deep learning.

Traditional machine learning has been used for many years with great success. It is able to detect and block many types of attacks through behavioral tracking and anomaly detection. Although very specific and limited to a specific task, it is very effective and can provide near real-time protection from unknown attacks. In Radware's solutions, it is used to detect behavioral anomalies in traffic patterns as an indicator for denial-of-service attacks.

Deep Learning

Recently, deep-learning technology found its way into information security solutions to detect complex attacks and correlate multiple individual indicators of malicious intent to detect malicious behavior. These systems can detect complex sequences of events in huge amounts of data, events that humans would never be able to notice. On the down side, they are prone to false positives and known to produce unexpected results. Their efficiency is primarily dependent on a huge amount of good, carefully classified data.

Other challenges for deep-learning systems are that they are not transparent, are hard to reproduce and have learning challenges in adversarial contexts.

Deep-learning systems require:

- ▶ Enormous amounts of good data
- ▶ Large amounts of storage and sufficient compute resources for training
- ▶ Supervision in trial and error

Naturally, most deep-learning solutions have their "brain" in the cloud, supervised by data scientists who ensure the efficiency of the model as the amount of data samples increases and the diversity in the learning set changes. Other experts sanitize the results produced by the solution.

As such, deep-learning systems work better as cloud-based threat intelligence services than real-time, on-premise detection and mitigation devices. The output of such systems can be fed back to customer-premises equipment that consumes the threat intelligence feeds.

Another approach, taken by some anti-malware solutions, uses a replica of the cloud-hosted deep-learning model as an on-premise software, and any updates of the weights from training the cloud model are copied onto the on-premise software. That way the solution can make an exact replica of the cloud-trained deep-learning model, which has virtually unlimited resources, to on-premise models which limit resources to achieve local detection and mitigation in near real time. It even takes less data volume to replicate the model compared to transferring signature updates within traditional anti-malware systems.

5. Will the use of AI-based attacks by cybercriminals drive adoption of AI-based mitigation solutions by enterprises, organizations and institutions?

Yes, but not necessarily at the same pace. There are three factors to consider — the attack vector, its speed and its evasion technique:

1. For example, using AI for phishing does not affect the victim in terms of change in attack vector, but it does increase the scale and number of targets, compelling every organization to improve its protection. This protection might include AI-based systems, but not necessarily.
2. On the other hand, as attacks get more automated, organizations will have to automate their security to ensure that they keep on top of the rising number and accelerated speed of attacks.
3. When new evasion techniques based on AI are leveraged by cybercriminals, it will ultimately lead to the use of better detection systems that are based on AI.

6. Are you aware of any AI-derived security threats or defenses that are already in evidence?

Yes, we've already seen both AI-derived security threats and defenses in the ecosystem.

Threats

- ▶ MalGAN — anti-malware evasion²⁵
- ▶ Spear phishing — SNAP_R²⁶
- ▶ I'm not a human — breaking Google's reCAPTCHA with 98% accuracy using deep learning²⁷
- ▶ Deep hack — AI-based hacking tool used to breach websites²⁸

Defenses

- ▶ Organizations that send emails when they detect logins from suspicious locations or unknown devices are leveraging traditional machine learning
- ▶ Anti-malware in the cloud that uses deep-learning systems to train based on massive numbers of malware samples
- ▶ Behavioral detection and automatic signature generation of unknown DDoS attacks
- ▶ Bot/human classification based on activity tracking and correlation in web application firewalls



Summary

AI will become an important, if not the most important, component of future cybersecurity strategies. Organizations will not run or maintain the AI system themselves, but rather will use the results from cloud-based systems. Initially, we will not see on-premise black-box fully autonomous AI systems that provide real-time protection. AI — and deep learning specifically — is a modern cybersecurity strategy that enables experts, not replaces them. However, budgets, testing, deployment and even decisions are supervised by humans who do not keep pace with technology.

²⁵<https://arxiv.org/abs/1702.05983>

²⁶<https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf>

²⁷<https://www.blackhat.com/docs/asia-16/materials/asia-16-Sivakorn-Im-Not-a-Human-Breaking-the-Google-reCAPTCHA-wp.pdf>

²⁸https://www.youtube.com/watch?v=wbRx18VZiYA&list=PLwDEUgS8l_7dh4UCcRkX9uXVKgOtpGh22&t=1668&index=19



Radware Research: Deep Dives

Security experts from Radware provide insights from what they observed in the threat landscape in 2018, assess the impact of the IoT on the increase in botnets, look at the growing popularity of cryptomining and make predictions for what to expect in cybersecurity in 2019.

What's New in Network and Application Security

Radware's Emergency Response Team (ERT) is a group of experienced network and application security engineers who work around-the-clock to provide managed services and under-attack support to thousands of organizations globally. They fight a variety of threats at all levels but specialize in the most sophisticated and hardest to mitigate attacks.

In 2018, this experienced team discovered new tactics and tools used by attackers to overcome defenses to take down networks, data centers and application services. They witnessed a change in the threat landscape with the vast use of botnets as attack agents, an approach that reduces both the cost and operational complexity of launching attacks. The discovery comes with a warning: to effectively mitigate these emerging attacks requires the use of advanced detection and mitigation tools.

The change is characterized by:

1. Several attack tools throughout the same attack, with fast programmatic switches from one attack vector to another — leaving manual policy tuning techniques inefficient, stressing the need for automated, self-learning mitigation systems.
2. Very short Burst attacks that bypass outdated out-of-path offline capture and analysis security operations. Short bursts make it nearly impossible for defenders to take the right capture that will lead to proper analysis and mitigation.
3. Application-layer attacks are increasing in number, with very fast evolution cycles generating new permutations. This type of attack requires a multilayer agile and intelligent defense architecture that can detect zero-day threats and adapt accordingly.

Customer Case Example

For example, over several weeks a customer experienced long-lasting, high volumetric, quickly morphing DDoS attacks aimed at causing severe damage by bringing services down.

Attacks morphed rapidly with the combination of multiple Layers 3 and 4 vectors (such as UDP, SYN, ACK and ICMP Floods), Layer 7 vectors (such as HTTP and HTTPS Floods), attacks hiding in legitimate connections, multiple reflection vectors (DNS, LDAP, CHARGEN), IoT botnet attacks and Burst DDoS attacks with rapid vectors and characteristics that change within minutes. While many known vectors were used, the rapid changes between many possible permutations presented a new challenge.

Radware's advanced technology relies on unique behavioral analysis of traffic flows to secure availability. Radware's technology enabled it to make a distinction between the traffic coming from legitimate users and the high volumes of the attack traffic. We leveraged our multilayer architecture to divert the load of the attack traffic to our scrubbing center for fast adjustments and mitigation.

The challenge lies not only with mitigation of the attack traffic, but also mostly with filtering the legitimate traffic to enable services to run seamlessly. Trying to fight against such attacks with legacy techniques, such as rate-limiting or manual tuning of security profiles, is not effective in this type of attack. Such approaches lead to a partial — if not complete — service outage from users' perspective and can easily translate into a financial impact.

2016 was the year of DDoS. 2017 was the year of ransom. As Radware predicted in last year's annual security report, 2018 is the year of automation. The growth of the attack surface, techniques and means continued into 2018 through various attacks and attack techniques that were very costly in the past. Tools and methods that were rarely available before are now much more common and widely used by different hacking groups or individuals. An adaptive security service should automatically and quickly detect rapid changes and automatically assign optimal protection policies.

IoT Expands the Botnet Universe

In 2018, we witnessed the dramatic growth of IoT devices and a corresponding increase in the number of botnets and cyberattacks. Because IoT devices are always-on, rarely monitored and generally use off-the-shelf default passwords, they are low-hanging fruit for hackers looking for easy ways to build an army of malicious attackers. Every IoT device added to the network grows the hacker's toolset.

Botnets comprised of vulnerable IoT devices, combined with widely available DDoS-as-a-Service tools and anonymous payment mechanisms, have pushed denial-of-service attacks to record-breaking volumes. At the same time, new domains such as cryptomining and credentials theft offer more opportunities for hacktivism.

Radware's worldwide threat deception network identifies emerging threats as early as possible to distribute mitigation information to Radware security solutions globally. The network combines passive decoys with the attack-specific knowledge generated by Radware's Cloud Security Services. It then takes advantage of machine learning-based big data processing and neural networks to detect and identify emerging threats while there is still time to take proactive protective measures.

2018 Highlights

Let's look at some of the botnets and threats discovered and identified by Radware's deception network in 2018.



Figure 62. Timeline of botnets and threats captured by Radware's deception network in 2018.

JenX

January 30, 2018²⁹

Targets: Vulnerable Huawei routers and devices using the Realtek SDK.

Objective: DDoS stresser services

Family: Mirai based

A new botnet tried to deliver its dangerous payload to Radware's newly deployed IoT honeypots. The honeypots registered multiple exploit attempts from distinct servers, all located in popular cloud hosting providers based in Europe. The botnet creators intended to sell 290Gbps DDoS attacks for only \$20.

Further investigation showed that the new bot used an atypical central scanning method through a handful of Linux virtual private servers (VPS) used to scan, exploit and load malware onto unsuspecting IoT victims. At the same time, the deception network also detected SYN scans originating from each of the exploited servers indicating that they were first performing a mass scan before attempting to exploit the IoT devices, ensuring that ports 52869 and 37215 were open.

The Radware Threat Research Team quickly issued a security advisory and contacted the hosting companies to take down the infecting servers before the botnet could be used for attacks.

ADB Miner

February 5, 2018³⁰

Targets: Android-based devices that expose debug capabilities to the internet such as mobile phones, media players and smart TVs

Objective: Cryptomining

Family: Mirai variant

A new piece of malware that takes advantage of Android-based devices exposing debug capabilities to the internet. It leverages scanning code from Mirai. When a remote host exposes its Android Debug Bridge (ADB) control port, any Android emulator on the internet has full install, start, reboot and root shell access without authentication. Part of the malware includes Monero cryptocurrency miners (xmrig binaries), which are executing on the infected devices.

Radware's automated trend analysis algorithms detected a significant increase in activity against port 5555, both in the number of hits and in the number of distinct IPs. Port 5555 is one of the known ports used by TR069/064 exploits, such as those witnessed during the Mirai-based attack targeting Deutsche Telekom routers in November 2016. In this case, the payload delivered to the port was not SOAP/HTTP, but rather the ADB remote debugging protocol.

Satori.Dasan

February 11, 2018³¹

Targets: Dasan WiFi routers

Objective: Cryptomining

Family: Mirai variant

Less than a week after ADB Miner, a third new botnet variant triggered a trend alert due to a significant increase in malicious activity over port 8080. Radware detected a jump in the infecting IPs from around 200 unique IPs per day to over 2,000 malicious unique IPs per day. Further investigation by the research team uncovered a new variant of the Satori botnet capable of aggressive scanning and exploitation of CVE-2017-18046 – Dasan Unauthenticated Remote Code Execution.

The rapidly growing botnet referred to as "Satori.Dasan" utilizes a highly effective wormlike scanning mechanism, where every infected host looks for more hosts to infect by performing aggressive scanning of random IP addresses and exclusively targeting port 8080. Once a suitable target is located, the infected bot notifies a C2 server, which immediately attempts to infect the new victim.

Memcached DDoS Attacks

February 27, 2018³²

Targets: Vulnerable Memcached servers

Objective: Amplification DDoS attack

A few weeks later, Radware's system provided an alert on yet another new trend – an increase in activity on UDP port 11211 (see Figure 63).



Figure 63. System alert generated by an increase in activity on UDP port 11211.

This trend notification correlated with several organizations publicly disclosing a trend in UDP-amplified DDoS attacks utilizing Memcached servers configured to accommodate UDP (in addition to the default TCP) without limitation. After the attack, CVE-2018-1000115 was published to patch this vulnerability. Memcached services are by design an internal service that

²⁹<https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicio/>

³⁰<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/adb-miner/>

³¹<https://blog.radware.com/security/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/>

³²<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcached-under-attack/>

allows unauthenticated access requiring no verification of source or identity. A Memcached amplified DDoS attack makes use of legitimate third-party Memcached servers to send attack traffic to a targeted victim by spoofing the request packet's source IP with that of the victim's IP. Memcached provided record-breaking amplification ratios of up to 52,000x.

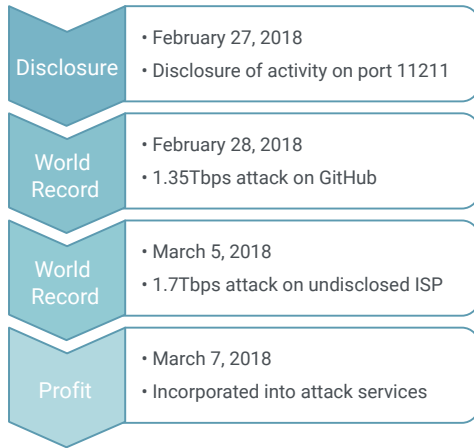


Figure 64. Evolution of the Memcached DDoS attack.

Hajime Expands to MikroTik RouterOS

March 24, 2018³³

Targets: MikroTik RouterOS-based devices

Objective: Vigilante botnet

Family: Hajime

Radware's alert algorithms detected a huge spike in activity for TCP port 8291. After near-zero activity on that port for months, the deception network registered over 10,000 unique IPs hitting port 8291 in a single day.

Port 8291 is related to a then-new botnet that exploits vulnerabilities in the MikroTik RouterOS operating system, allowing attackers to remotely execute code on the device. The spreading mechanism was going beyond port 8291, which is used almost exclusively by MikroTik, and rapidly infecting other devices such as AirOS/Ubiquiti via ports: 80, 81, 82, 8080, 8081, 8082, 8089, 8181, 8880, utilizing known exploits and password-cracking attempts to speed up the propagation.

³³<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/mikrotik-botnet>



What is Memcached?

The Memcached attack had the biggest impact in 2018, but what is it?

Memcached is a distributed memory-caching system typically used to speed up dynamic web applications by caching data and objects in RAM and reducing back-end database or API round trips. The exposure of the Memcached protocol to the internet allowed attackers to exploit the protocol for launching easy three-step UDP-based amplification attacks:

1. The attacker builds an amplification list of vulnerable Memcached servers with UDP port 11211 exposed.
2. The attacker sends a spoofed GET request to the vulnerable Memcached servers on the amplification list.
3. Memcached servers reply to the GET request, forwarding an amplified response to the spoofed IP address — the victim.

The attackers did not need to spend time to find perfect infection tools to generate a massive botnet. They only needed to take advantage of the vulnerabilities of hundreds of thousands of improperly configured, unpatched Memcached servers.

The Radware Threat Research Center published custom signatures to prevent Memcached servers from participating in DDoS attacks as well as signatures designed to mitigate Memcached DDoS attacks reflected by those servers, strengthening and supporting Radware's mitigation devices' inherent abilities.

Satori IoT Botnet Worm Variant

June 15, 2018³⁴

Targets: D-Link DSL-2750B routers and XiongMai uc-httpd 1.0.0 devices

Objective: DDoS botnet

Family: Mirai variant

Another interesting trend alert occurred on Saturday, June 15. Radware’s automated algorithms alerted to an upsurge of malicious activity scanning and infection of a variety of IoT devices by taking advantage of recently discovered exploits. The previously unseen payload was delivered by the infamous Satori botnet. The exponential increase in the number of attack sources spread all over the world, exceeding 2,500 attackers in a 24-hour period.

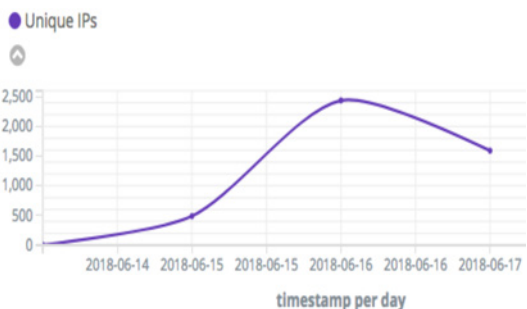


Figure 65. Example of an alert about an upsurge in malicious activity scanning.

³⁴<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet>
³⁵<https://blog.radware.com/security/2018/08/iot-hackers-trick-brazilian-bank-customers/>

DNS Hijacking Targets Banks

June–August³⁵

Targets: DLink DSL routers

Goal: Obtain sensitive information from Brazilian bank customers

Method: IoT attack combined with hijacking infrastructure

A new malicious agent emerged in Radware’s systems in June using a new and insidious attack method. The user is misled to a phony website without crafting or changing URLs in the user’s browser. This approach is unique in the sense that a user is completely unaware of the change. Users can employ any browser and regular shortcuts. They can type the URL manually or even access it from mobile devices. In all cases, they end up at a malicious website thanks to effective hijacking at the gateway level.

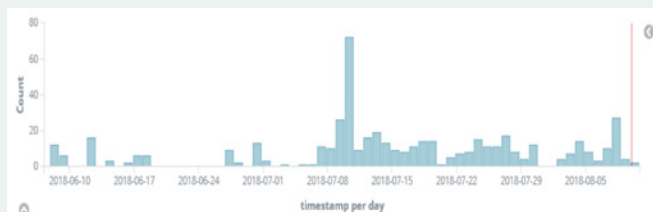


Figure 66. Sensors tracked multiple infection attempts during June, July and August.

The first indication of the threat deception network popped in June when cybercriminals targeted DLink DSL routers in Brazil, taking advantage of outdated exploits. Radware’s sensors started recording multiple such infection attempts.

The criminals were able to leverage these old exploits against vulnerable and unpatched routers more than two years later by attempting to modify the DNS server settings in the routers of Brazilian residents and redirecting their DNS requests through a malicious DNS server operated by hackers. This process effectively enabled the criminals to conduct a man-in-the-middle attack and redirect users to phishing domains for local banks to harvest the users’ credentials. After identifying the targets and hosts, Radware both contacted the banks and filed abuse reports with the cloud providers hosting the malicious DNS and websites to take down the exploiting servers. Though the servers were taken down, the determined attackers found replacements and ramped up their operation.

This attack targets IoT device owners, attempting to obtain their sensitive data. And while it was done using an unauthenticated configuration command, most other exploits on IoT devices witnessed in the past year have been using remote command executions, so it is possible to project this into a malicious agent crafting a similar attack using configuration command scripts embedded in the RCE exploit URLs.

Hakai

September 6, 2018³⁶

Targets: D-Link, Huawei and Realtek routers

Type: DDoS botnet

Family: Qbot/Gafgyt variant

Radware's automation algorithm monitored the rise of Hakai, which was first recorded in July.

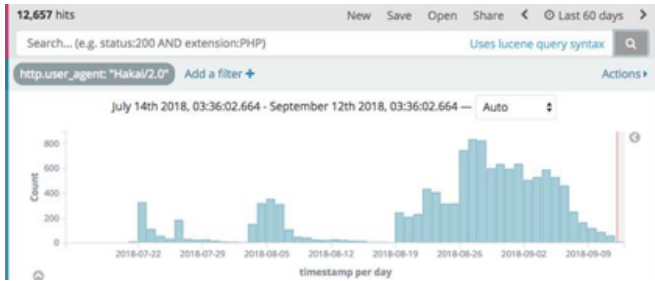


Figure 67. Sensors tracked multiple infection attempts during June, July and August.

Hakai is a new botnet recently discovered by NewSky Security after lying dormant for a while. It started to infect D-Link, Huawei and Realtek routers. In addition to exploiting known vulnerabilities to infect the routers, it used a Telnet scanner to enslave Telnet-enabled devices with default credentials.

DemonBot

October 24, 2018³⁷

Targets: Hadoop cloud infrastructure

Type: DDoS botnet

Family: New

A new stray QBot variant going by the name of DemonBot joined the worldwide hunt for yellow elephant — Hadoop cluster — with the intention of conscripting them into an active DDoS botnet. Hadoop clusters are typically very capable, stable platforms that can individually account for much larger volumes of DDoS traffic compared to IoT devices.

DemonBot extends the traditional abuse of IoT platforms for DDoS by adding very capable big data cloud servers. The DDoS attack vectors supported by DemonBot are STD, UDP and TCP floods.

Using a Hadoop YARN (Yet-Another-Resource-Negotiator) unauthenticated remote command execution, DemonBot spreads only via central servers and does not expose the wormlike behavior exhibited by Mirai-based bots. By the end of October, Radware tracked over 70 active exploit servers that are spreading malware and exploiting YARN servers at an aggregated rate of over one million exploits per day.

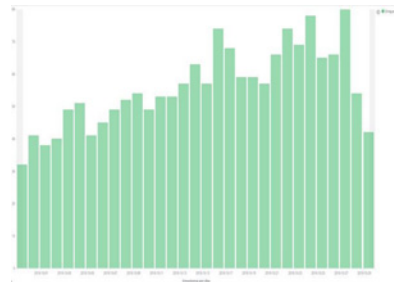


Figure 68. Unique IPs per day identified in the Hadoop attack.

YARN allows multiple data processing engines to handle data stored in a single Hadoop platform. DemonBot took advantage of YARN's REST API publicly exposed by over 1,000 cloud servers worldwide.

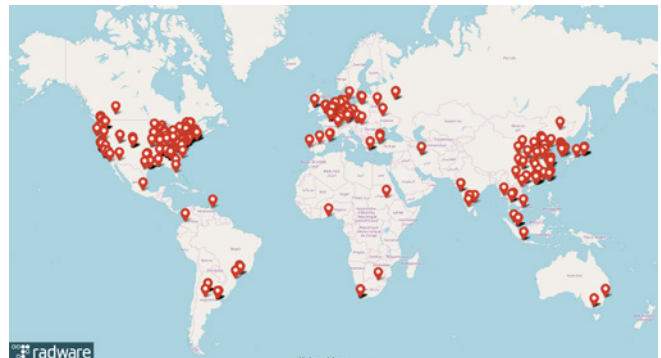


Figure 69. Location of exposed Hadoop YARN servers.

DemonBot effectively harnesses the Hadoop clusters in order to generate a DDoS botnet powered by cloud infrastructure.

Always on the Hunt

In 2018, Radware's deception network launched its first automated trend-detection steps and proved its ability to identify emerging threats early on and to distribute valuable data to the Radware mitigation devices, enabling them to effectively mitigate infections, scanners and attackers. One of the most difficult aspects in automated anomaly detection is to filter out the massive noise and identify the trends that indicate real issues.

In 2019, the deception network will continue to evolve and learn and expand its horizons, taking the next steps in real-time automated detection and mitigation.

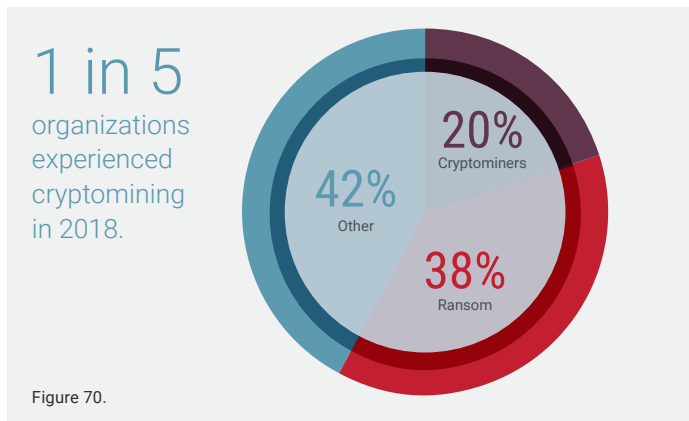
³⁶<https://blog.netlab.360.com/70-different-types-of-home-routers-all-together-10000-are-being-hijacked-by-ghostdns-en>

³⁷<https://blog.radware.com/security/2018/10/new-demonbot-discovered/>

The Rise of Cryptomining

There are four primary motivations for cyberattacks: crime, hacktivism, espionage and war. Setting aside nation-state sponsored groups, the largest faction of attackers are cybercriminals, individuals or well-established organizations looking to turn a profit.

For the last several years, ransom-based cyberattacks and ransomware had been the financial modus operandi for hackers, but 2018 flipped the coin to unveil a new attack vector: cryptomining (see Figure 70).



Always Crypto

Radware's Malware Threat Research Group monitored this phenomenon throughout the year and identified two recurring trends. Some groups use cryptomining to score a quick, easy profit by infecting machines and mining cryptocurrencies. Other groups use cryptomining as an ongoing source of income, simply by reselling installations on infected machines or selling harvested data.

While there is no definitive reason why cryptomining has become popular, what is clear are some of the advantages it has over older attacks methods:

- ▶ **It's easy** – There's no need to develop a cryptomining tool or even buy one. An attacker can just download a free tool into the victim's machine and run it with a simple configuration that instructs it to mine the pool.
- ▶ **CPU** – While Bitcoin requires a graphic processing unit (GPU) to perform effective mining, other cryptocurrency, such as Monero, require only CPU to effectively mine a machine. Since every machine has a CPU, including web cameras, smartphones, smart TVs and computers, there many potential targets.
- ▶ **Minimal footprint** – Other attack types require the hackers to market their "goods" or to actively use the information they acquired for malicious purposes. In cryptomining, the money moves directly to the attacker.

- ▶ **Value** – The value of cryptocurrencies skyrocketed in late 2017 and early 2018. The outbreak quickly followed. More recently, as monetary value declined, so has the number of incidences.
- ▶ **Multipurpose hack** – After successfully infecting a machine, hackers can leverage the installation of the malware program for multiple activities. Stealing credentials from machines? Why not use those machines to cryptomine as well (and vice versa)? Selling data mining installations on machines to other people? Add a cryptomining tool to run at the same time.

The Malware Ecosystem

There are few popular ways for cybercriminals to launch cryptomining attacks:

- ▶ **Information stealing** – By distributing a data harvesting malware, attackers steal access credentials or files (photos, documents, etc.), and even identities found on an infected machine, its browser or inside the network. Then, the cybercriminals generally:
 - Use the stolen data to steal. In the case of bank credentials, the hackers use the information to steal money from accounts.
 - Sell the stolen data through an underground market on the dark web to other hackers. Credit cards, social security numbers and medical records go for just a few dollars. Social media accounts and identities are popular, as well. Facebook and Instagram accounts have been hijacked and used for propagation.
- ▶ **Downloaders** – Malware is distributed with simple capabilities to download additional malware and install on other systems. The motivation is to infect as many machines as possible. The next step is to sell malware installations on those machines. Apparently, even infected machines enjoy brand premium fees – machines from a Fortune 500 company cost a lot more.
- ▶ **Ransomware** – Machines are infected with a malware that encrypts files, which are usually valuable to the victim, such as photos, Microsoft files (.xlsx, docx) and Adobe Acrobat files. Victims are then asked to pay a significant amount of money in order to get a tool to decrypt their files. This attack was first introduced against individuals but grew exponentially when hackers figured out that organizations can pay a higher premium.
- ▶ **DDoS for ransom (RDoS)** – Attackers send targets a letter that threatens a DDoS attack on a certain day and time unless the organization makes a payment, usually via Bitcoin. Often hackers know the IP address of the targeted server or network and launch a small-scale attack as a preview of what could follow.

Social Propagation

Malware protection is a mature market with many competitors. It is a challenge for hackers to create a one-size-fits-all zero-day attack that will run on as many operating systems, servers and endpoints as possible, as well as bypass most, if not all, security solutions. So in addition to seeking ways to penetrate protection engines, hackers are also looking for ways to bypass them.

During the past year, Radware noticed several campaigns where malware was created to hijack social network credentials. That enabled hackers to spread across the social network accessing legitimate files on the machine and private information (or computing resources, in the context of cryptomining).

Here are a few examples:

- ▶ **Nigelthorn** – Radware first detected this campaign, which involved a malicious chrome extension, in a customer's network. The hackers bypassed Google Chrome native security mechanisms to disguise the malware as a legitimate extension. The group managed to infect more than 100,000 machines. The purpose of the extension was cryptomining Monero currency by the host machine, as well as stealing the credentials of the victim's Facebook and/or Instagram accounts.

The credentials were abused to propagate the attack through the Facebook user's contact network. It is also possible that the credentials were later sold on the black market.

- ▶ **Stresspoint** – In this spree, hackers used a benign-looking drawing application to hijack Facebook users' cookies. They deceived victims by using an allegedly legitimate AOL.net URL, which was actually a unicode representation. The true address is "xn--80a2a18a.net."

The attackers were building a database of users with their contact network, business pages and payment details (see Figure 72). Radware suspects that the ultimate goal was to use this information to fund public opinion influence campaigns on the social network.

- ▶ **CodeFork** – This campaign was also detected in some of Radware's customers' networks when the infected machines tried to communicate with their C&C servers. Radware intercepted the communication and determined that this group was infecting machines in order to sell their installations. The group has been active for several years during which time we have seen them distributing different malware to the infected machines. The 2018 attack included an enhancement that distributes cryptomining malware.

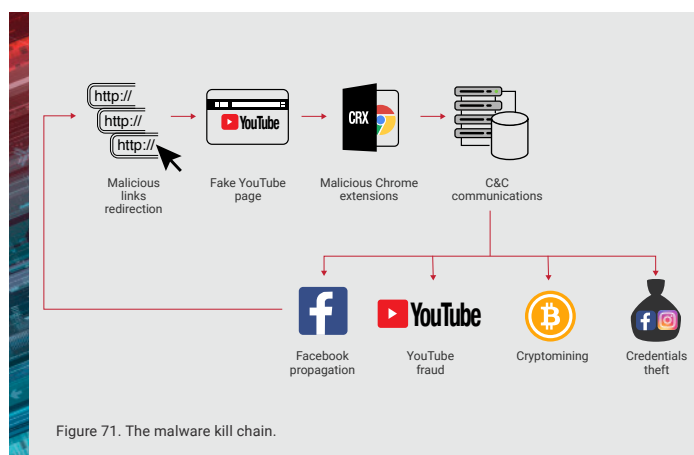


Figure 71. The malware kill chain.

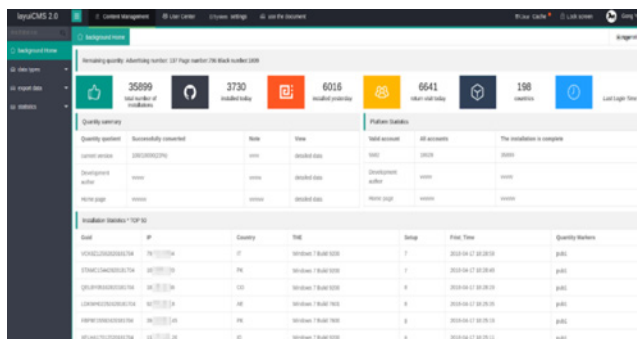


Figure 72. The group control panel and account information database.

```

nov [ebp+var_40], eax
nov [ebp+var_34], offset aSafe ; "--safe"
nov [ebp+var_30], offset a0 ; "-0"
nov [ebp+var_2C], offset aXmr_cryptoPool ; "xmr.crypto-pool.fr:443"
nov [ebp+var_28], offset aU ; "-U"
nov [ebp+var_20], offset aPx ; "-px"
nov [ebp+var_1C], offset aB ; "-B"

```

Figure 73. Monero mining executable process.

Moving Forward

Radware believes that the cryptomining trend will persist in 2019. The motivation of financial gain will continue, pushing attackers to try to profit from malicious malware. In addition, hackers of all types can potentially add cryptomining capabilities to the infected machines that they already control. Our concern is that during the next phase, hackers will invest their profits to leverage machine-learning capabilities to find ways to access and exploit resources in networks and applications.



Cybersecurity Predictions — 2019

The cybersecurity threat landscape evolves at a breakneck pace. The proverbial game of whack-a-mole continues as attack vectors, techniques and types quickly adapt and change in response to network protection policies.

Radware continually monitors the security threat landscape and offers a “Dirty Dozen” list of attack types that we can expect to see in 2019, ranking them according to their effectiveness and value.

Radware’s “Dirty Dozen” Attack Types:

- # 1 — APT
- # 2 — Organized Cybercrime
- # 3 — Ransom
- # 4 — DDoS Groups
- # 5 — Hacktivists
- # 6 — Patriotic Hackers
- # 7 — Exploit Kits
- # 8 — Trojans
- # 9 — Botnets
- # 10 — Insider Threats
- # 11 — Defacements
- # 12 — Consumer Tools

Each attack type warrants a conversation about how it continues to develop and stay relevant as technology evolves. In fact, each year new attack types and the advancement of old techniques reveal themes, such as:

2016 – Year of DDoS, with the introduction of IoT botnets, including DynDNS.

2017 – Year of Ransom, when financial motivations spurred attacks on organizations, including worldwide campaigns such as WannaCry and NotPetya.

2018 – Year of automated attacks, with sensational attacks on APIs (85% according to Radware research), especially bot attacks. Attackers took advantage of the ability to leverage weaponized artificial intelligence, both for enhanced speed of decisions and the defeat of cybersecurity tools. We also saw growth in side-channel attacks, such as the much-publicized British Airways attack, and proxy-based attacks through CDNs, ADCs and web servers, such as the attack on Equifax.

Where does the landscape lead in 2019? No one knows for sure what the future holds, but strong leading indicators help Radware build a logic chain to forecast where the state of network security is headed.

In 2019, Radware predicts:

1. The public cloud will experience a massive security attack that shakes the confidence of all users
2. Ransomware hijacks the IoT
3. The rise of the nation-state availability-based attacks
4. The rise of DDoS swarmbots and hivenets

Prediction 1: The public cloud will experience a massive security attack that shakes the confidence of all users

In 2019, the adoption of the public cloud as part of enterprises' IT infrastructure will continue to grow in popularity as a way to efficiently deliver services and run applications. The shift introduces a greater need to prevent data breaches and infiltrations and ensure data and process integrity, while allowing for nonrepudiation of users and attackers.

What are some of the attack vectors for this new landscape?

- ▶ Attacking the IaaS architecture itself:
 - Workloads
 - Containers
 - Ephemeral/serverless environments
 - Cloud-driven optional services such as CDNs, application acceleration, etc.
- ▶ App stores and marketplaces
- ▶ Security updates and cyberthreat intelligence services
- ▶ Rise of east/west DDoS, intrusions and malware on public clouds
- ▶ Domain name systems (DNSs)
- ▶ Public code repositories to build websites
- ▶ Web analytics platforms
- ▶ Identity and access single sign-on platforms
- ▶ East/west traffic patterns, such as open-source code commonly hosted by vendors on a public cloud
- ▶ Third-party vendors that participate in the public cloud infrastructure via license arrangements

Prediction 2: Ransomware hijacks the IoT

Ransom can be a very profitable high-tech business for attackers seeking financial gain. Various methods of ransom include:

- ▶ **Ransomware** – encrypting a victim's data and asking for payment to release the data
- ▶ **Ransom distributed denial of service (RDoS)** – attacking a victim through DDoS and asking for a payment to stop the DDoS

These techniques show up as various attack formats depending on what an attacker is seeking.

Hijack Ransom – Attackers hijack the availability of a service and ask for ransom to return the service back to normal. Examples include the hijacking of stock trading services, video or music services, emergency services such as 9-1-1 or emergency broadcasts, and AI-enabled services such as Alexa, Cortana and Siri.

IoT Device Ransom – This is similar to a hijack ransom, except the attackers go after the device itself. Any device connected to the internet is susceptible to security lapses. The market will soon determine if users are willing to pay on the spot to regain control of IoT devices.

Health Ransom/Tech Hostage – The most disturbing ransom attack is one that seeks to take advantage of people who are dealing with health issues. Many ailments are treated with cloud-based monitoring services, IoT-embedded devices and self or automated administration of prescription medicines. Common ransom attacks could establish a foothold in the delivery of health services and put people's lives at risk.

Prediction 3: The rise of the nation-state availability-based attacks

As trade and other types of “soft-based,” nonmilitary-based power conflicts increase in number and severity across the globe, nation-states and other groups will seek new ways to cause widespread disruption. These disruptions can be conducted as solo endeavors or combined with armed conflicts. Techniques include internet outages at the local or even regional level and service outages and application blacklisting regionally, such as China's policy to ban certain technologies and vendors.

Commercial and government organizations are likely to be considered legitimate targets. Industries stand to lose millions of dollars if communications systems fail and trade grinds to a halt. Supply chain availability makes a great target for nation-states to spot target and influence their will over time, leading to a cascade of failures.

Government services are also vulnerable to attack, such as law enforcement organizations that depend on internet connectivity for communications. Attacks in this realm could involve physical disruption to cables and satellites, the rendering of rules and architectures within certain geographies to make routing and name resolutions nearly impossible, or the wide-scale use of various sophisticated DDoS attacks that could pinpoint target applications and certain technologies.

The geopolitical risk can rise substantially so that the global nature of the internet is replaced by a more regional approach.

Prediction 4: The rise of DDoS swarmbots and hivenets

There is a concept in physical computing called *swarmbots* (swarm robotics) which is now being applied to the logical world of code writing and internet threats. Swarmbots are “a collection of mobile robots able to self-assemble and to self-organize in order to solve problems that cannot be solved by a single robot. These robots combine the power of swarm intelligence with the flexibility of self-reconfiguration as aggregate swarmbots can dynamically change their structure to match environmental variations.”³⁸

Attackers have embraced the bot concept. For example, over the past years we have seen the development and deployment of massive IoT-based botnets, such as Mirai, BrickerBot, Reaper and Hajime systems, built around thousands of compromised IoT devices. Most of these weaponized botnets have been used in cyberattacks to knock out devices or services in a relatively straightforward manner.

Based on developments that Radware sees in places like the dark web, Radware predicts that cybercriminals will begin effectively upgrading IoT-based botnets with swarm-based technology to create better efficacy in their attacks. Traditional botnets are generally mindless slaves; they wait for commands from the bot herder (master) in order to execute an attack.

The idea in swarmbots is to make these nodes more self-sufficient as they are able to make autonomous decisions with minimal supervision, use their collective intelligence to solve problems, or opportunistically and simultaneously target multiple vulnerability points in a network. Swarmbots can use peer-based self-learning to target vulnerable systems at an unprecedented scale.

Hivenets are self-learning clusters of compromised devices that simultaneously identify and tackle different attack vectors. Hivenets direct what actions swarmbots take and are especially dangerous because, unlike traditional botnet zombies, they could take advantage of increases in fidelity and latency reductions in 5G to become even more effective. Hivenets are able to talk to each other, take action based on shared local intelligence, use swarm intelligence to act on commands without the botnet herder instructing them to do so, and recruit and train new members of the hive. As a result, as a hivenet identifies and compromises more devices, it will be able to grow exponentially and thereby widen its ability to simultaneously attack multiple victims.

Striving for Cyber Serenity: Is the Best Behind Us?

2018 was a monumental year. Cloud-based DDoS attacks like Memcached pushed a 1Tbps attack to the evolution of autonomous attacks, and proxy-based attacks have made the landscape both complicated and high risk.

If growth of attack surfaces, techniques and means continues into 2019 through various attacks on automated technologies, the best years of system security may be behind us. As we move into 2019, Radware offers two key questions:

1. How will the rise of the public cloud threat vectors fuel corresponding rises in new vectors for exploits?
2. How will nation-state resources, tools and techniques be used against commercial enterprises and public entities?

Peace in cyberspace is an optimistic, yet unrealistic hope. Radware knows the next phase of the threat evolution will emerge in 2019. Unfortunately, our collective behavior creates more network breaches for both individual and organized groups of hackers. As long as there is no clear stance on topics such as a cybersecurity privacy bill, the status of virtual currencies as a means of trade, the responsibility for hardening vulnerable IoT devices, and the existence of fictitious identities, the tug-of-war game will continue with each side exploiting the vulnerabilities of the other.

In the coming months, weaponized AI, large API attacks, proxy attacks and automated social engineering will target the hidden attack surface created by automation. Radware urges you to pay special attention and remain vigilant.

³⁸Swarm-Bots: Swarm of Mobile Robots able to Self-Assemble and Self-Organize," RECIIM News No. 53, April 2003 at https://www.ercim.eu/publication/Ercim_News/enw53/nolfi.html



Respondent Profile

In fall 2018, Radware conducted a survey of the global security community and collected 790 responses. The survey was sent to a wide variety of organizations globally and was designed to collect objective, vendor-neutral data about the issues that organizations face while preparing for and combating cyberattacks. Following is responder profile information. Note that not all answers total 100% because some responders may have skipped the question.

What best describes your title within your organization?

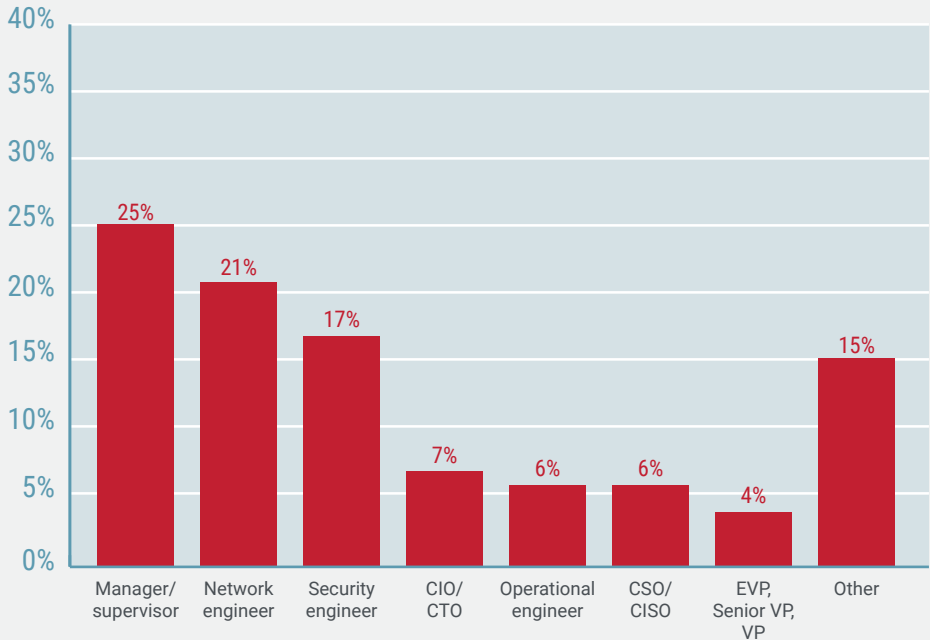


Figure 74. Title within organization.

In total, how many employees work in your organization?

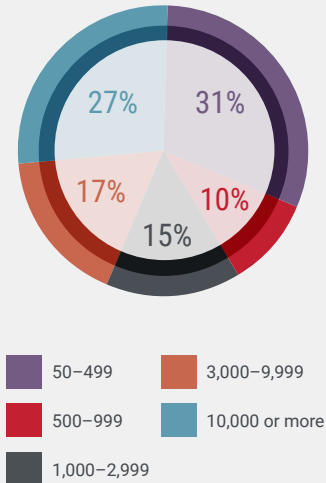


Figure 75. Number of employees in organization.

Which best describes your company's industry?

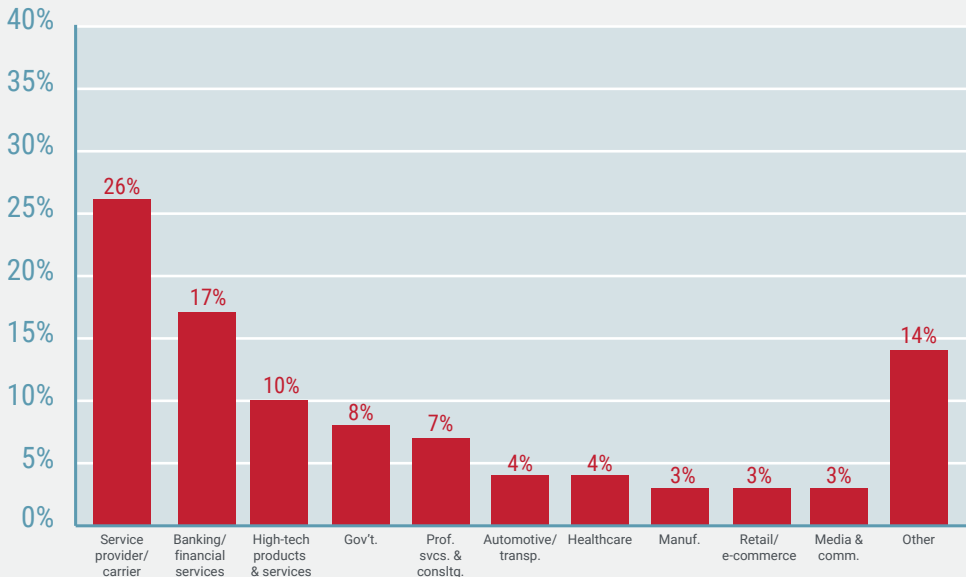


Figure 77. Industries represented.

What is the scope of your organization's business?

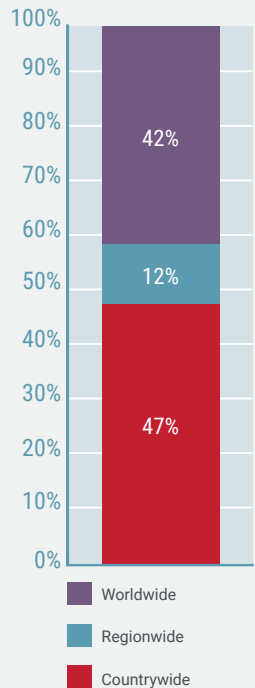


Figure 76. Geographic scope of business.

Credits

Authors

Carl Herberger

VP, Security Solutions
Radware

Yotam Ben Ezra

VP, Security Innovation
Radware

Nissim Pariente

Director of Security Analytics
Radware

Ben Zilberman

Manager, Security Product Marketing
Radware

Daniel Smith

ERT Researcher
Radware

Michael O'Malley

VP, Corporate and Strategic Marketing
Radware

Pascal Geenens

Security Evangelist
Radware

Sharon Aran

Senior Product Manager
Radware

Itamar Orlov

ERT Team Leader
Radware

Adi Raff

Security Research Team Leader
Radware

Additional Contributors

Shira Sagiv

Director, Security Product Marketing
Radware

Eyal Arazi

Manager, Security Product Marketing
Radware

Maureen Shaw

Digital Marketing Manager
Radware

Carolyn Muzyka

Director, Marketing Communications
Radware

Laura Ann Tillotson

Manager, Marketing Communications
Radware

Colin Beasty

Manager, Content Marketing
Radware

Editors

Deb Szajngarten

Director, Public Relations
Radware

Ben Zilberman

Manager, Security Product Marketing
Radware

socket.sys.os
= sys.argv(2)
DDOS
print "[REMOTE DDOS AT
(SOCKET.P
app
activeDocument.activeLayer



Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.



This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2019 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this report are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.