The Changing Face of Cyber Attacks

neustar Defense

Table of Contents

A LOOK AT 2018

"THE BIG ATTACKS ARE BACK."

In 2016, we saw a number of huge attacks — many that exceeded 1Tbps. In 2017, by contrast, we saw fewer large distributed denial-of-service (DDoS) attacks, possibly because hackers were finding little advantage in taking a company completely offline. Another explanation is that hackers were simply enjoying the success of the previous year's myriad of extortion and ransomware-oriented attacks, as well as the many DDoS associated data breaches.

So far in 2018, however, the big attacks are back with a vengeance. Earlier this year we saw the largest DDoS attack ever recorded — 1.35Tbps — using a new type of attack called Memcached, which will be discussed later. Then, a 1.7Tbps DDoS attack was recorded. Previous amplification attacks, such as DNSSEC, returned a multiplication factor of 217 times, but Memcached attacks returned amplification records exceeding 51,000 times!

In fact, the potential return from Memcached attacks is so large that they do not require the use of botnets, making them a new and dangerous risk vector. We are hoping that these attacks will go the way of the Simple Service Discovery Protocol (SSDP) amplification attacks, which used the protocol designed to advertise and find plug-and-play devices as a vector. SSDP amplification attacks are easily mitigated with a few simple steps, including blocking inbound UDP port 1900 on the firewall. There are similar steps that organizations can take to mitigate Memcached attacks, including not exposing servers and closing off ports, but until then, Neustar is prepared.

HOW THE RISK OF ATTACK FROM VARIOUS ACTORS HAS CHANGED

During January-February 2018, organizations have perceived the most likely increase in threats to be from criminals and unknown actors.

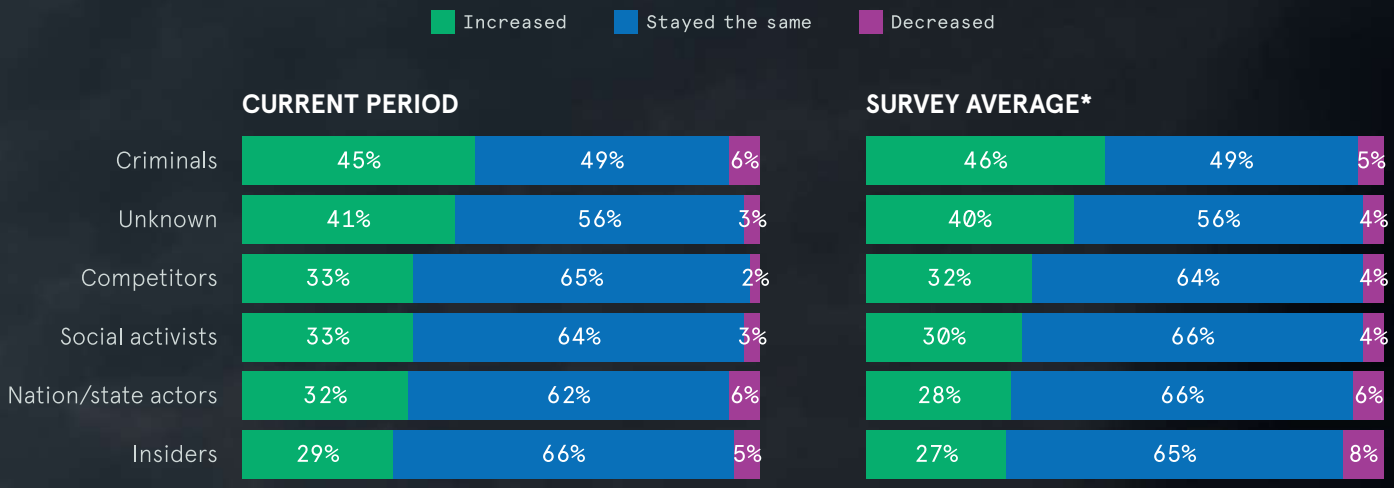
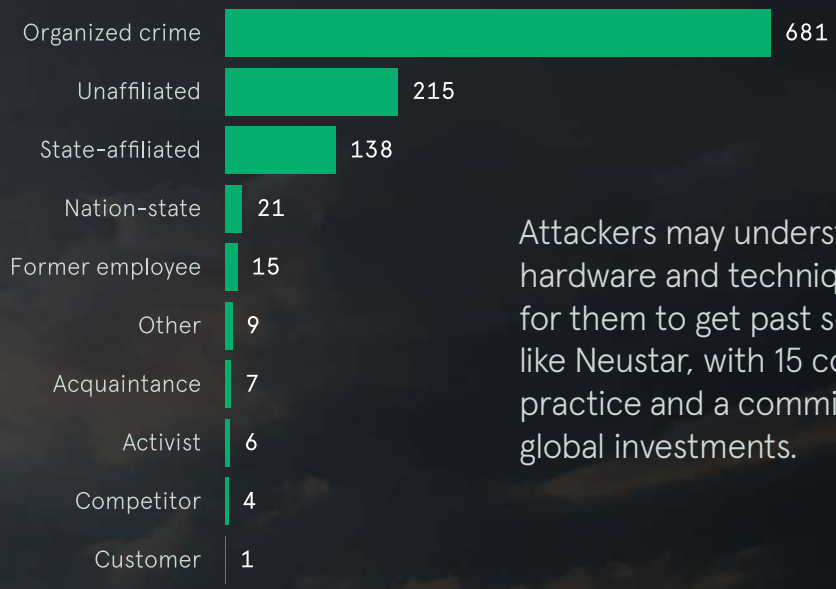


Figure 1. Neustar International Security Council

*Survey Average is the cumulative average of survey data collected bi-monthly from seven different surveys of ~300 security professionals, beginning in May 2017 and completed most recently in March 2018.

TOP EXTERNAL ACTOR VARIETIES IN BREACHES



Attackers may understand DDoS mitigation hardware and techniques, but it's difficult for them to get past security operations like Neustar, with 15 continuous years in practice and a commitment to large-scale, global investments.

Figure 2. Top external actor varieties within confirmed data breaches (n=1,097) - Verizon Data Breach Incident Report 2018

This year we are also seeing different uses for DDoS beyond simple volumetric attacks, including what we call quantum attacks. Quantum attacks are relatively small and designed to bypass endpoint security and avoid triggering cloud failover mitigation. These attacks are being used for scouting and reconnaissance. In a recent incident, Neustar stopped a quantum attack that never peaked over 300 Mbps, but it featured 15 different attack vectors, went on for 90 minutes, and involved all of Neustar's globally distributed scrubbing centers. This attack came from all over the world and was designed to bypass perimeter hardware, using protocols to circumvent their defenses. The attackers behind such campaigns may start small, but they can quickly add botnets, attack vectors, and ports to get what they want.

Neustar recently thwarted what is believed to be the first IPv6 attack. This attack presented a new direction that attackers are likely to pursue as more and more companies adopt IPv6 and run dual IPv4/IPv6 stacks. We believe that IPv6 vectors will continue to emerge as organizations around the world move to adopt the new standard.

You can also expect to see more Layer 7 (application layer) attacks, including those targeting DNS services with HTTP and HTTPS requests. These attacks are often designed to target applications in a way that mimics actual requests, which can make them particularly difficult to detect. It is important to note, however, that Layer 7 attacks are typically only part of a multi-vector DDoS attack. The other parts are aimed at the network and overall bandwidth.

DDoS attacks can be found in a multitude of sizes and for any reason imaginable. They can now be used to find vulnerabilities, to locate backdoors for exfiltration, and as a smokescreen-like distraction for other activities. Today's organized criminals are able to focus on the results that they want and simply buy or rent the malware or botnets they need to get there. Some have gone so far as to comment that criminals are getting more and more like corporations, each with their own specialization.

The simple fact is that if you're online, you're susceptible to an attack. Whether you are vulnerable or not is entirely up to you.

Malware & Breaches

Customers surveyed in the early part of 2018 showed a growing concern over ransomware. And for good reason. According to the Verizon Data Breach Incident Report 2018, this threat has become "... the most prevalent variety of malicious code for this year's dataset."[1] The Verizon report goes on to observe that ransomware is an interesting phenomenon that, when viewed through the mind of an attacker, makes perfect sense.

Ransomware can be:

- **Used in completely opportunistic attacks, affecting individuals' home computers, as well as targeted strikes against organizations**
- **Attempted with little risk or cost to the adversary involved**
- **Successful, with no reliance on having to monetize stolen data**
- **Deployed across numerous devices in organizations to inflict bigger impacts and command bigger ransoms**

Ransomware attacks have grown in such significance that they have been cited by the World Economic Forum[2] as a global security issue. According to the WEF 2018 Global Risk Report, "The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack — which affected 300,000 computers across 150 countries — and NotPetya, which caused quarterly losses of US$300 million for a number of affected businesses." In fact, according to the Cisco 2017 Annual Cybersecurity Report[3], ransomware is growing at a yearly rate of 350%.

CYBER THREATS RANKED IN ORDER OF LEVEL OF CONCERN

During January–February 2018, ransomware was the greatest concern followed closely by system compromise and DDoS.

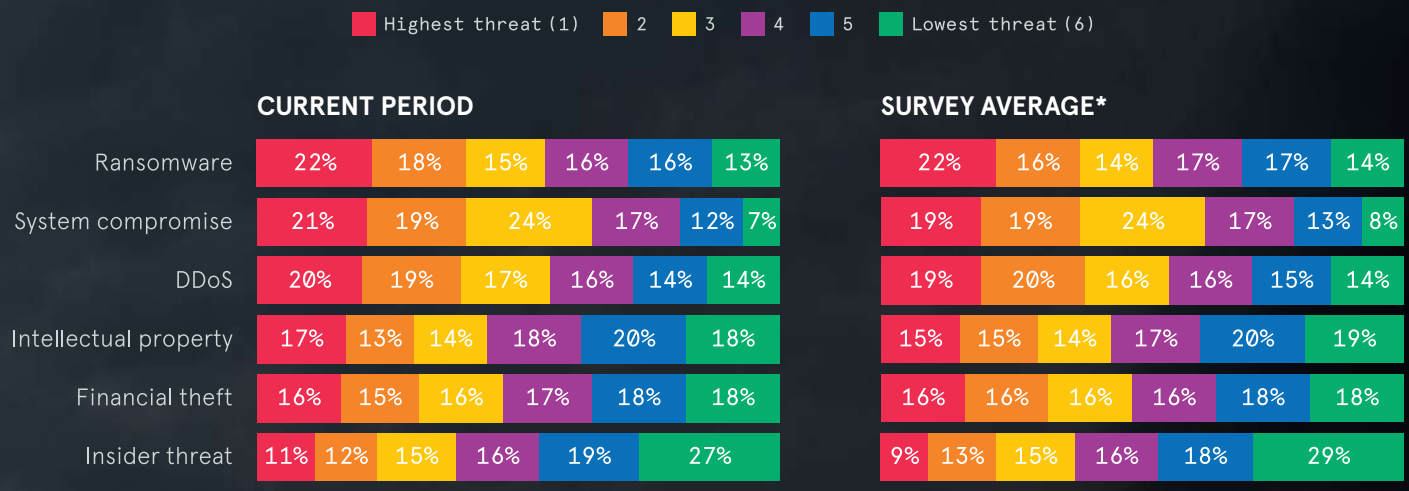


Figure 3. Neustar International Security Council

*Survey Average is the cumulative average of survey data collected bi-monthly from seven different surveys of ~300 security professionals, beginning in May 2017 and completed most recently in March 2018.

RANSOMWARE WITHIN MALWARE INCIDENTS

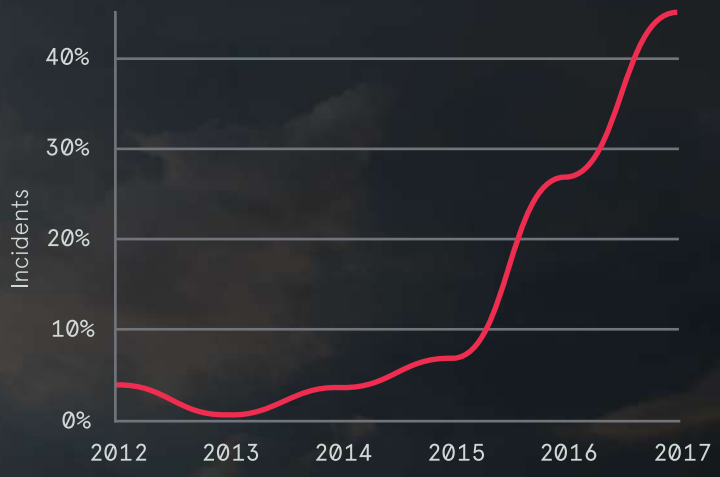


Figure 4. Ransomware within malware incidents over time - Verizon Data Breach Incident Report 2018

In the next section, we will briefly examine incidents of ransomware that had the greatest impact in the last year.

MALWARE & BREACHES

WannaCry

WannaCry is a ransomware cryptoworm targeting machines running certain older versions of the Microsoft Windows operating system. One characteristic that made this exploit dangerous was the variety of different elements that it contained, including a transport mechanism used to spread through a network. The mechanism would scan for vulnerable systems, then use the Eternal Blue exploit to gain access to the system via a vulnerability in the Windows Server Messaging Block. It is thought that this exploit is how the WannaCry infection began. The malware then used the Double Pulsar backdoor tool to create a copy and install itself. Both Eternal Blue and Double Pulsar were released by the hacker group the Shadow Brokers. In a single day, the code was reported to have infected more than 230,000 computers in over 150 countries.

Once executed, the WannaCry malware would check for the presence of a kill switch domain. If the kill switch domain could not be reached, the malware would encrypt the device data, then attempt to spread to other devices on the Internet. The kill switch domain was eventually found in the malware itself, registered, and pointed to a DNS sinkhole, which rendered the malware useless. Attackers released several variants of WannaCry with different kill switch domains, and even attempted a DDoS attack on the domain using a Mirai botnet variant.

MALWARE & BREACHES

Petya and NotPetya

Petya, a reference to an atomic-powered satellite in the James Bond film *Goldeneye*, is encrypting ransomware that pre-dated WannaCry. Propagated via infected emails, Petya works by infecting the master boot record on Microsoft Windows machines. Once executed, the payload encrypts a hard drive's file system table, prevents Windows from booting, and presents a screen demanding payment.

In 2017, after the WannaCry attack, a second variant of the ransomware emerged. This version, named NotPetya by Kaspersky Labs to differentiate it from the previous malware, used Eternal Blue to propagate itself.

Botnets

It is important to note that bots themselves are not necessarily malicious. Bots and botnets can be used in many legitimate ways, including aggregation tools, site indexing, online trading, and more. In fact, as of 2016, bot traffic on the Internet surpassed that of human-initiated traffic.

Even when used destructively, however, it is useful to remember that botnets are themselves merely a tool, and a tool with many uses. Botnets are probably best known for being used in DDoS attacks, but they have also been used to send spam and propagate phishing attacks, sniff traffic for private information displayed in clear text, record keystrokes, and manipulate polls and games.

The primary function of botnets is to recruit more bots. The examples that follow include several of the most recent botnets, and the multiple factors that make them dangerous.

Botnet examples:

- **The malware has been designed to target Internet of Things (IoT) devices, which means that targets are always on and available 24/7/365.**
- **Many of the target hosts are in use with low or no security precautions; in fact, many working IoT devices still use factory default credentials. These devices are often not monitored at all.**
- **The malware includes a means to use infected devices to scan for other vulnerable targets.**
- **End users typically notice little or no changes to their network, except for occasionally slower speeds.**

GEOGRAPHIC SPREAD OF BOTNET BREACHES

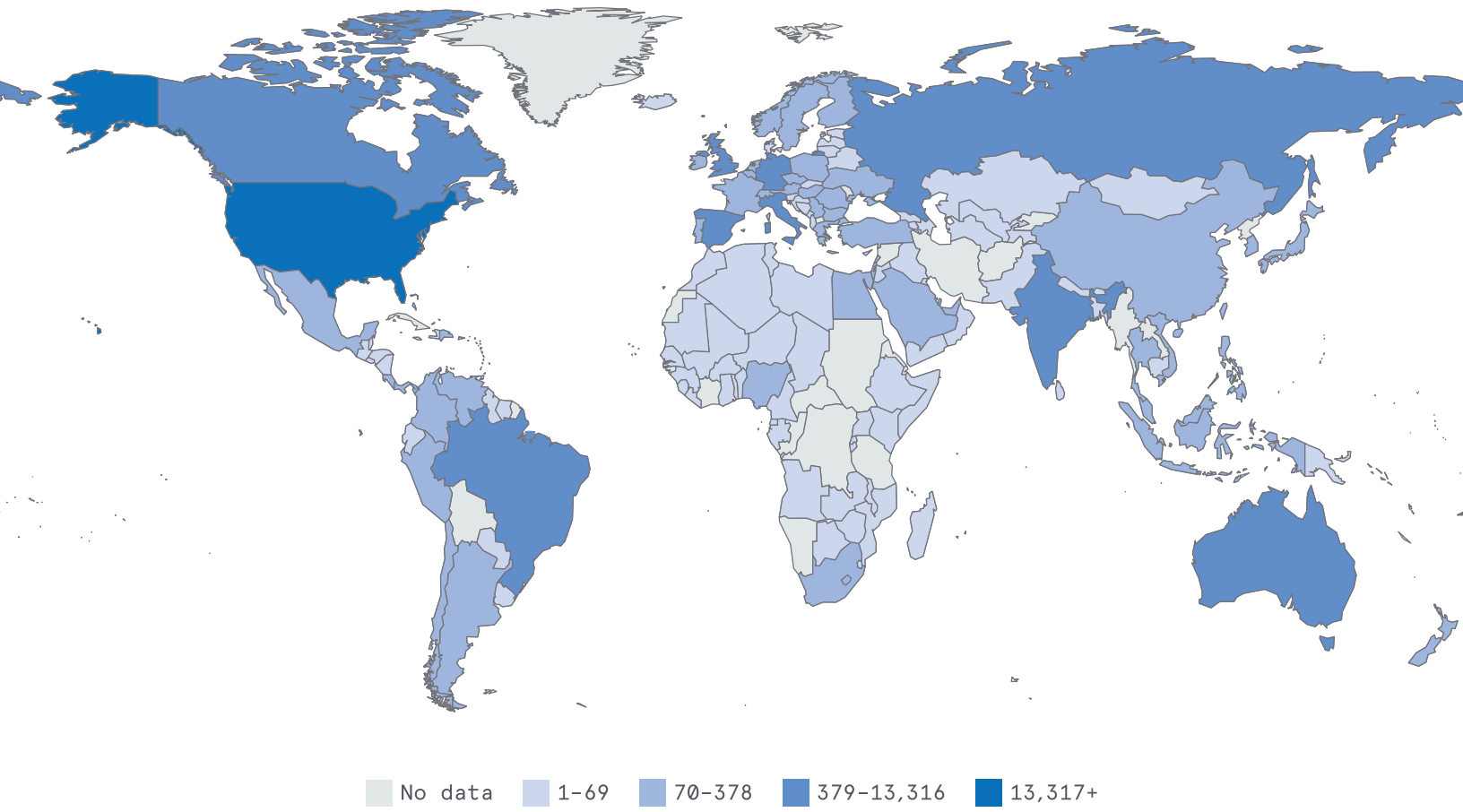


Figure 5. Botnet breaches by country (n=43,112) - Verizon Data Breach Incident Report 2018

As botnets have evolved and spread, they have actually become money makers in their own right. It is possible to "rent" a botnet for any purpose the buyer desires. This not only gives criminals a dangerous weapon, but it makes creating and spreading a botnet a lucrative proposition. In the next section, we will take a look at some of the botnets that came to prominence in 2017.

BOTNETS

Mirai

Among the most notorious known botnets, Mirai was one of the first to make use of IoT devices several years ago. Mirai takes advantage of the publicly released source code that powers everything from routers to closed-circuit television (CCTV) cameras and DVRs to scan the Internet looking for devices that use factory default or hard-coded credentials. Once found, these devices are infected with malware and can be used for DDoS attacks. Mirai inflicted a large-scale, Internet-wide disruption in 2016, when the botnet shut down security expert Brian Krebs' site and targeted DNS provider Dyn. Mirai is said to have generated traffic volumes of over 1Tbps and featured 10 pre-defined attack vectors.

Sartori, Okiru, Masuta, and PureMasuta

The Mirai source code has since been placed on GitHub, ensuring that the threat it posed continues. At least two new variants have been seen, including Sartori, which implements exploits on the web interface of particular routers. Another variant, called Okiru, which some sources describe as another version of Sartori, targets embedded processors. Other variants — Masuta and PureMasuta — exploit a vulnerability in another router's use of the Home Network Administration Protocol (HNAP).

WireX

WireX is a botnet designed to attack content delivery networks (CDNs) and other content providers with DDoS traffic. This botnet is primarily made up of Android devices running malicious apps, and was actually offered on the Google Play store for a time. WireX ran a volumetric DDoS attack at the application layer, with traffic that was primarily made up of HTTP GET requests aimed at a number of different CDNs and content providers. Devices from more than 100 countries participated in the attack, which was finally halted by the cooperative efforts of researchers from a number of different organizations.

IOT VS. HUMANS IN 2017

IoT devices

8.4

Billion

Global population

7.6

Billion

Figure 6. IoT vs. Humans in 2017, WEF GRR 2018

Distributed Denial of Service (DDoS)

The rate of DDoS attacks rose in 2017. In fact, according to Kaspersky Labs, the rate of businesses hit by DDoS attacks almost doubled in 2017, from 17% in 2016 to 33%[4]. Not only are the overall incidents of DDoS attacks up, but the number of companies hit more than once has increased as well.

All DDoS attacks have a common goal: to exhaust network bandwidth, server resources, or applications in such a way that legitimate users cannot access a site. The purpose for such attacks, however, can vary widely.

The methods used include:

- **Volume-based/volumetric attacks use connectionless protocols such as UDP to congest site bandwidth.**
- **Protocol attacks seek to overwhelm specific devices, including web servers, firewalls and load balancers. These connection-based attacks typically work by exhausting the number of concurrent sessions that a device can handle.**
- **Application/Layer 7 attacks target specific applications or servers by establishing a connection and exhausting resources.**

WHETHER RESPONDENTS HAVE EVER BEEN ON THE RECEIVING END OF A DDoS

43% of enterprises surveyed in March 2018 have ever* been on the receiving end of a DDoS, an increase on previous reporting periods.

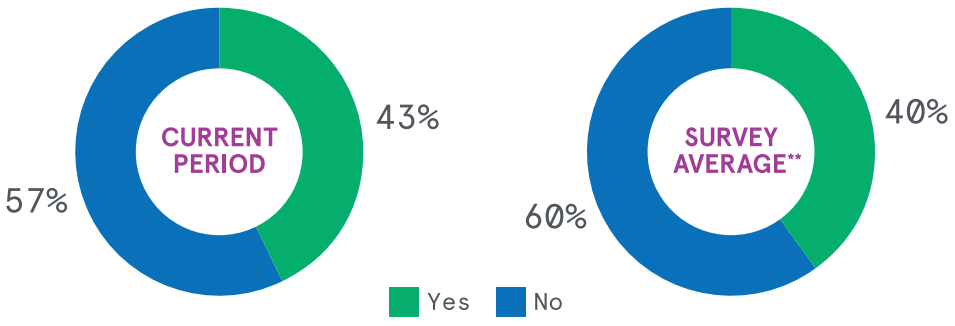


Figure 7. Neustar International Security Council

*Note that the sample composition changes from wave to wave which explains why the trend for this question can be down as well as up.
**Survey Average is the cumulative average of survey data collected bi-monthly from seven different surveys of ~300 security professionals, beginning in May 2017 and completed most recently in March 2018.

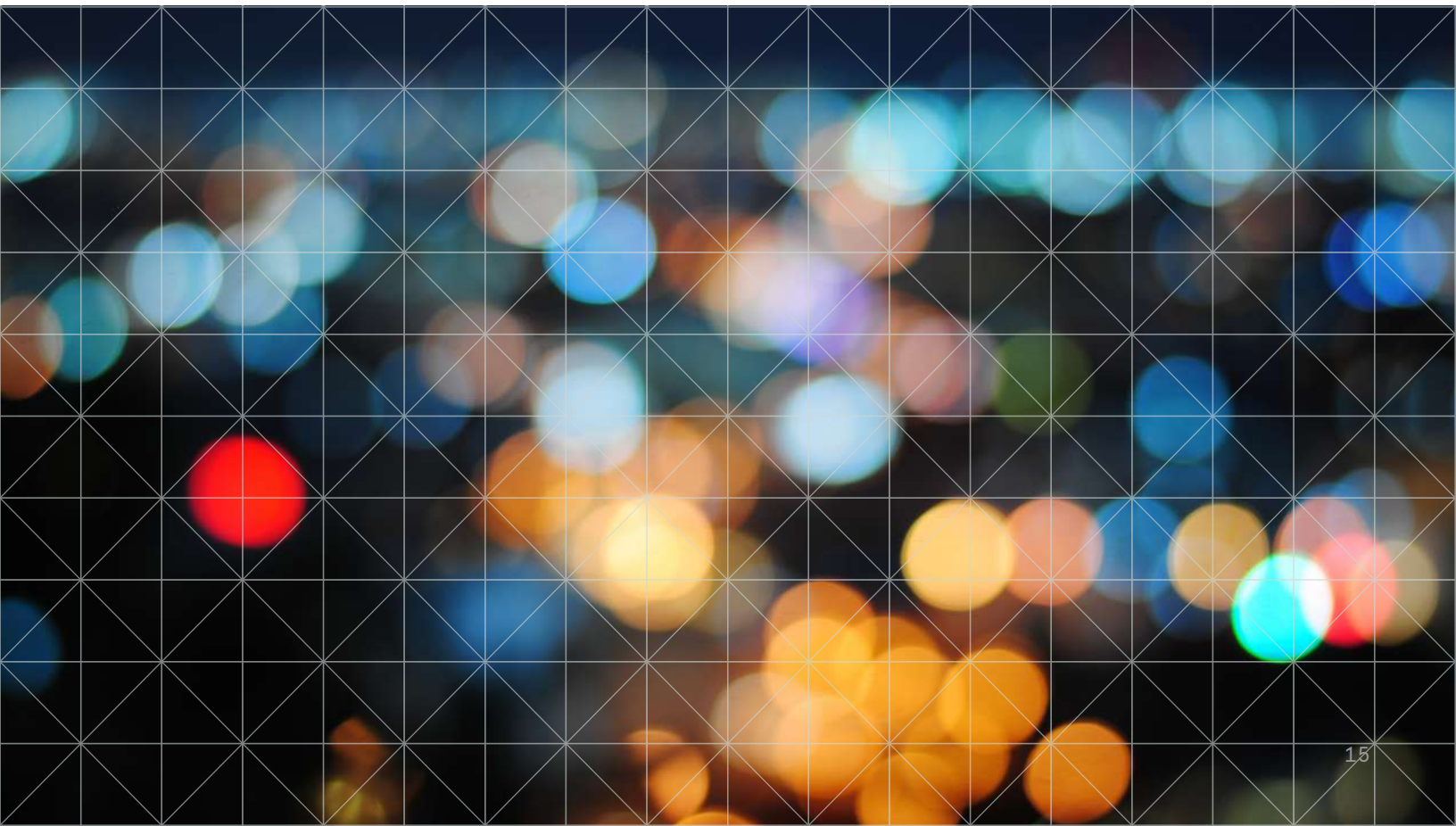
DISTRIBUTED DENIAL OF SERVICE (DDoS)

Volumetric and Protocol Attacks

These attacks are most commonly associated with DDoS attacks. They feature a large volume of traffic, often from botnets, and attempt to overwhelm a network or service.

Traffic can include:

- **UDP floods**
- **ICMP or Ping flood**
- **Syn flood**
- **Slowloris**
- **HTTP flood**
- **UDP fragment, PUSH flood, TCP flood**



DISTRIBUTED DENIAL OF SERVICE (DDoS)

Reflection and Amplification Attacks

Reflection and amplification attacks often come as a pair, though they serve two different but often compatible purposes. By spoofing source addresses, attackers can hide their identity by "reflecting" requests off a third party. Amplification attacks add to this by taking advantage of processes in which a small query will have a large — sometimes very large — response. Amplification attacks are, by nature, always reflection attacks as well.

Amplification attacks begin with the attacker spoofing the target's IP address. This is one reason that the majority of amplification attacks target services that use UDP, as it is a connectionless protocol that does not validate the source IP address. In the next step, the attacker sends a small query to a server or resource that generates a very large response forwarding that response to the target. The answering resource is behaving exactly as it should; in fact, the only real issue is that it is reachable by the attacker. The United States Computer Emergency Readiness Team (US-CERT) publishes a list of services vulnerable to these attacks (entries updated March 2, 2018).[5]

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [6]
NTP	556.9	see: TA14-013A [7]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [8]
CLDAP [9]	56 to 70	—
TFTP [10]	60	—
Memcached [11]	10,000 to 51,000	—

Figure 8. US-CERT Alert (TA14-017A) on UDP-based amplification attacks

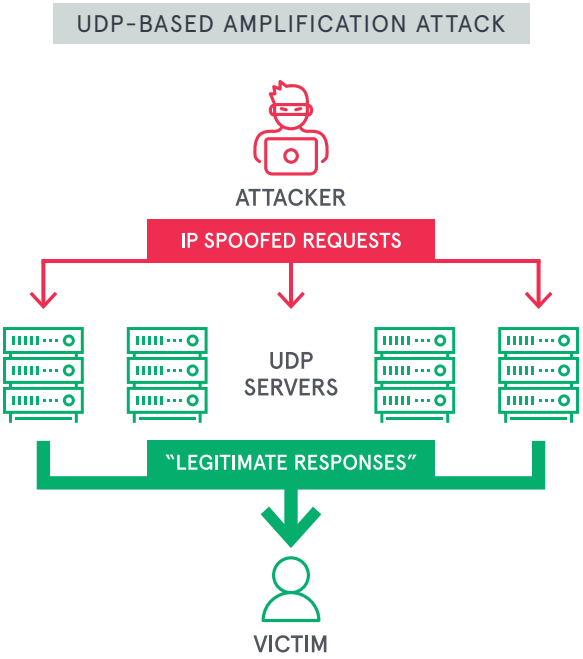


Figure 9. Small requests can yield very large responses, all sent to the spoofed address.

RELATIVE PREVALENCE OF AMPLIFIED DDoS ATTACKS

The Verizon 2018 Data Breach Incident Report shows the dramatic growth of amplified attacks, echoed by peak attack sizes charted by Arbor Networks.

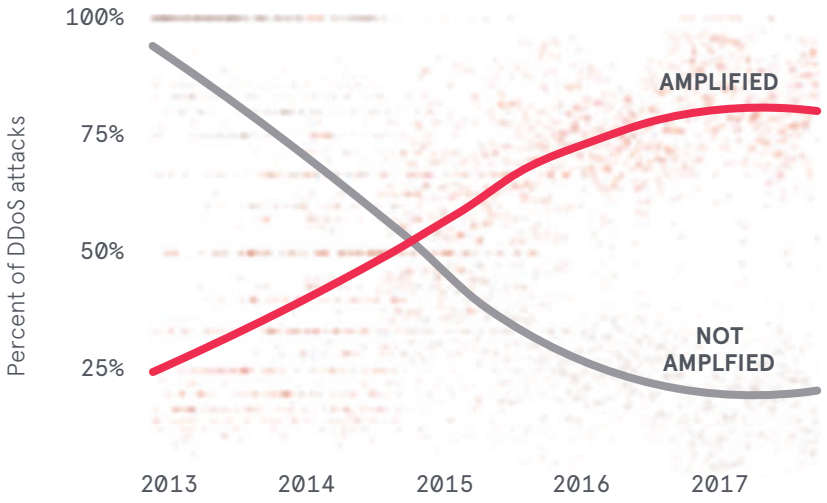


Figure 10. Amplification DDoS attacks over time (n=3,272) - Verizon Data Breach Incident Report 2018

DISTRIBUTED DENIAL OF SERVICE (DDoS)

Memcached Amplification Attack

The recent Memcached attack deserves a closer look, if only for the size of the amplification factor that it generated.

Memcached is a distributed memory caching system that uses free, open source software originally written in 2003. Memcached stores data and objects in RAM to speed up the response of dynamic database-driven websites. Memcached services are typically found in a cloud environment and should be reachable on the local network only, behind a firewall. It should *not* be open to the Internet. Unfortunately, some networks and some Linux servers have left TCP or UDP port 11211 open to the Internet. In a recent example, such a large amount of response traffic was generated that the attack significantly impacted the owner of the amplification server, as well as the actual target of the attack.

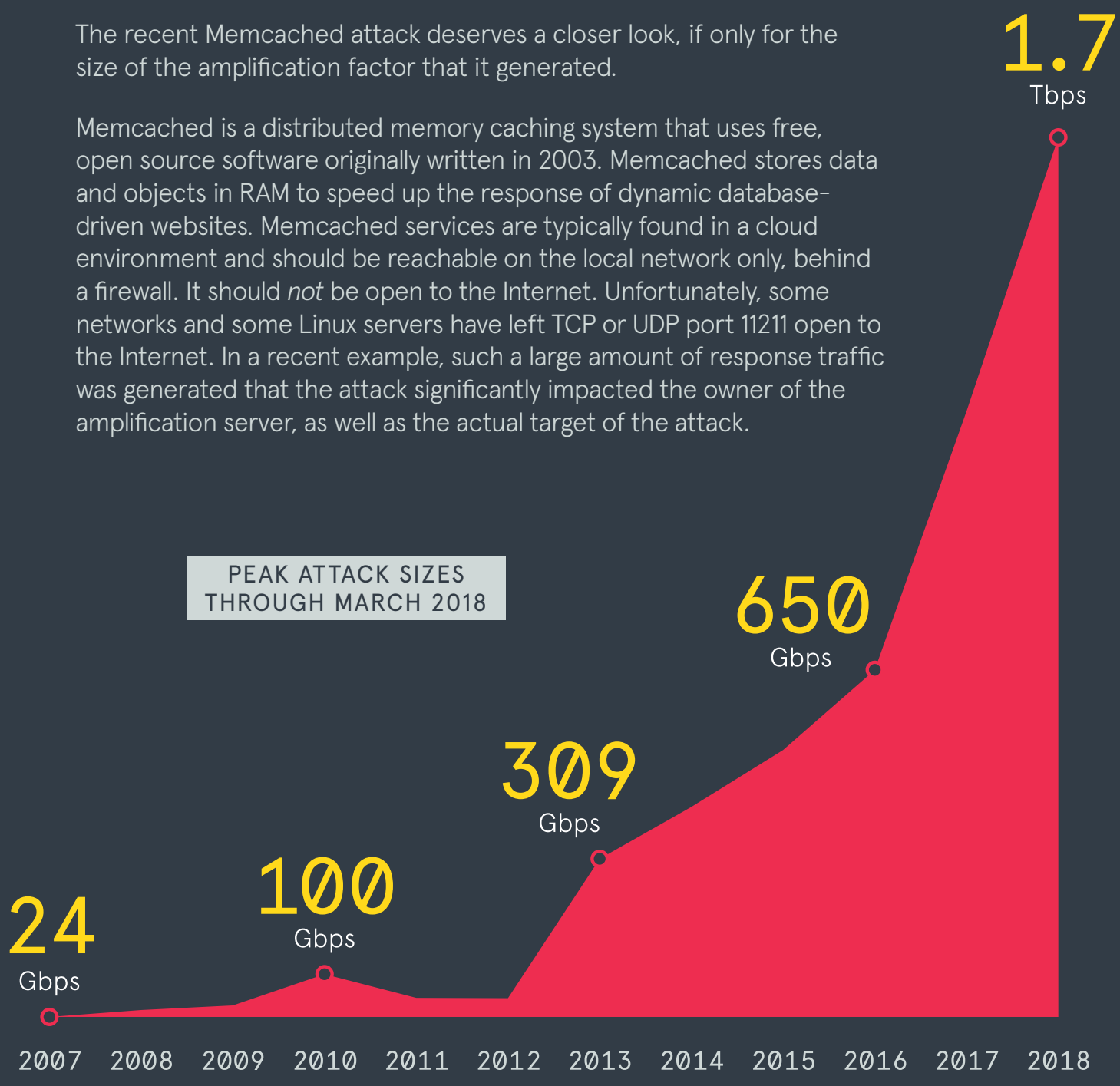
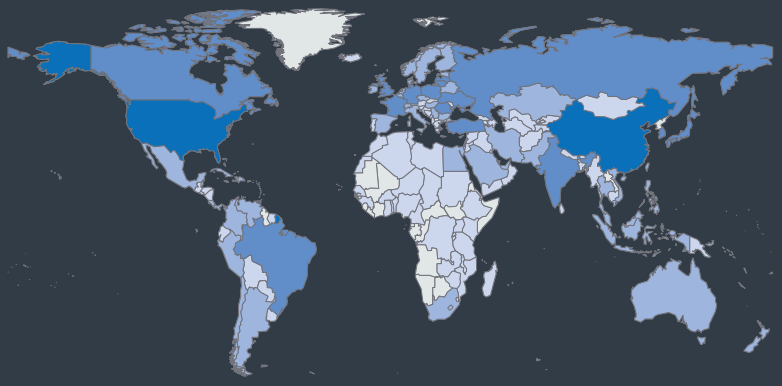


Figure 11. Arbor Networks, from Geekwire

GLOBAL VIEW OF POTENTIALLY VULNERABLE SERVERS



1.	United States	30,526
2.	China	23,639
3.	France	4,919
4.	Japan	4,138
5.	Hong Kong	4,123
6.	Netherlands	3,046
7.	Russian Federation	2,730
8.	Canada	2,629
9.	India	2,553
10.	Germany	2,517

Figure 12. Servers listening on TCP or UDP port 11211 as of March 7 - Shodan

Memcached uses UDP, a connectionless protocol that does not require authentication. This makes it easy for attackers to spoof a target's IP address to launch an attack. Attackers can take advantage of a simple "stats" command from a spoofed target IP address—a payload of approximately 15 bytes. The reply, on the other hand, can range from 1500 bytes to hundreds of kilobytes. Memcached servers typically have high-bandwidth access links because of the nature of their function and are often located on networks with high-speed transit links, making it possible to launch volumetric attacks quickly without the need for a botnet.

Because of how Memcached is configured, it is possible for hackers to search for servers listening on TCP or UDP port 11211 to find vulnerable servers.

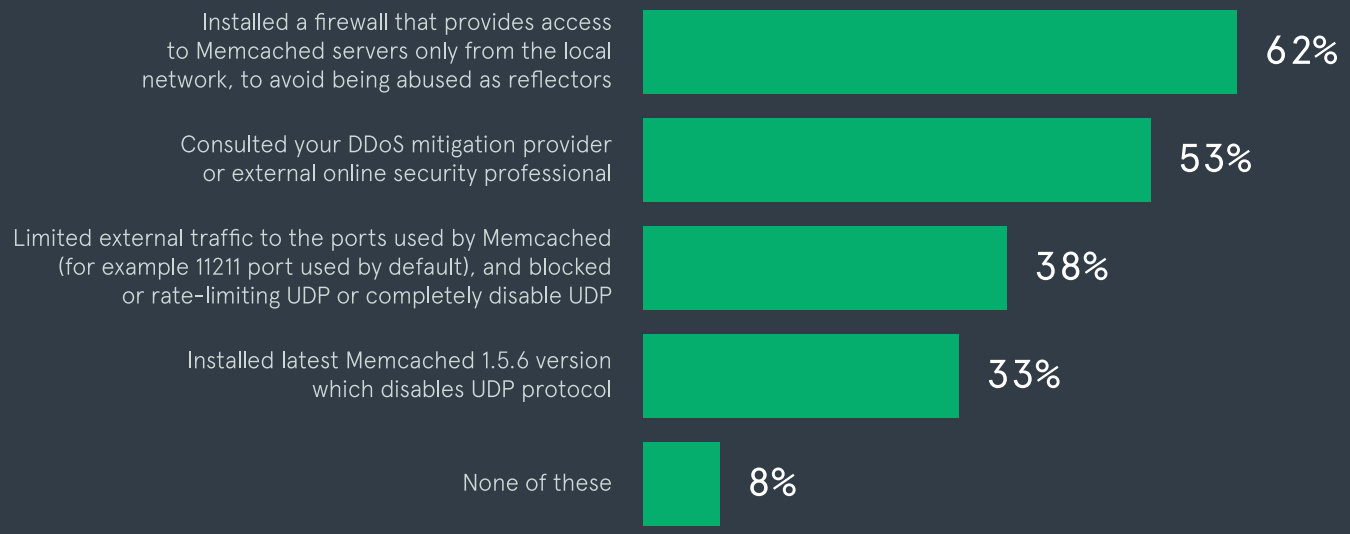
According to Krebs on Security, the potential devastation of Memcached DDoS attacks is now being used to threaten sites, demanding ransoms to stop assaults.[12]

This information also makes it relatively easy to block Memcached attacks, according to Johannes B. Ullrich, Dean of Research at SANS Technology Institute. "You should see traffic *from* port 11211 if you are hit by this attack. Blocking all traffic from port 11211 should be possible as all modern operating systems tend to use a source port higher than that for client connections. But given the traffic volumes people are seeing, you will likely need help 'upstream' or from an anti-DDoS company."[13]

MEMCACHED ATTACKS – ACTIONS TAKEN TO MINIMIZE RISKS AND WHETHER THESE WILL BECOME THE 'NORM'

Vast majority of companies (92%) have taken steps to minimize the risk from amplification attacks utilizing memcached servers and nine of ten agree these types of attacks will become the 'norm'.

ACTIONS TAKEN TO MINIMIZE RISK FROM AMPLIFICATION ATTACKS UTILIZING MEMCACHED SERVERS



LEVEL OF AGREEMENT THAT MEMCACHED ATTACKS WILL BECOME THE 'NORM'

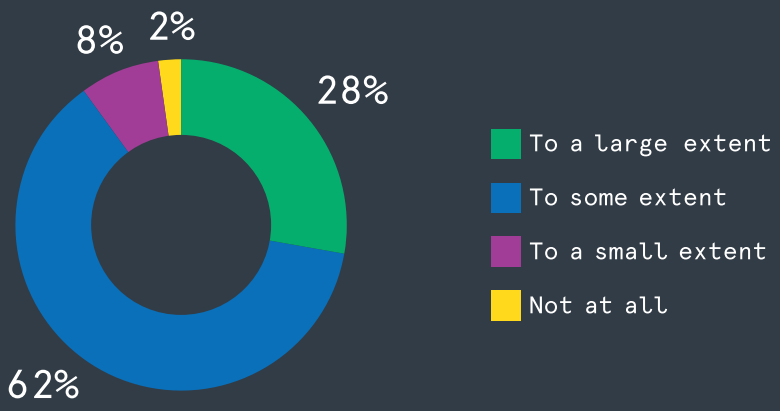


Figure 13. Neustar International Security Council

DISTRIBUTED DENIAL OF SERVICE (DDoS)

Layer 7 Attacks

Large-scale DDoS attacks have captured the media's attention, but from the perspective of cybercriminals, the focus is increasingly toward web application, or Layer 7, attack. In fact, according to the Cisco 2018 Annual Cybersecurity report, application DDoS has overtaken network DDoS this year.[14] Such attacks provide virtually no warning, are much more difficult to spot than DDoS attacks, and because they often target consumers, they can do irreparable damage in a very short amount of time.

Techniques include:

- **Cross-site scripting (XSS) is a form of injection in which an attacker injects malicious script into a web application. The end user will have no idea that a hacked site should not be trusted.**
- **Cross-site request forgeries (CSRF) trick end users into executing state-change actions on a web app with which they are authenticated. Such attacks can instigate actions such as transferring funds or changing email addresses.**
- **SQL injections are a well-known exploit in which SQL data is inserted into a query response from a client.**

Web applications are increasingly seen as part of DDoS attacks, in which the goal is not to bring down the target, but to smokescreen a vulnerability assessment of web applications.

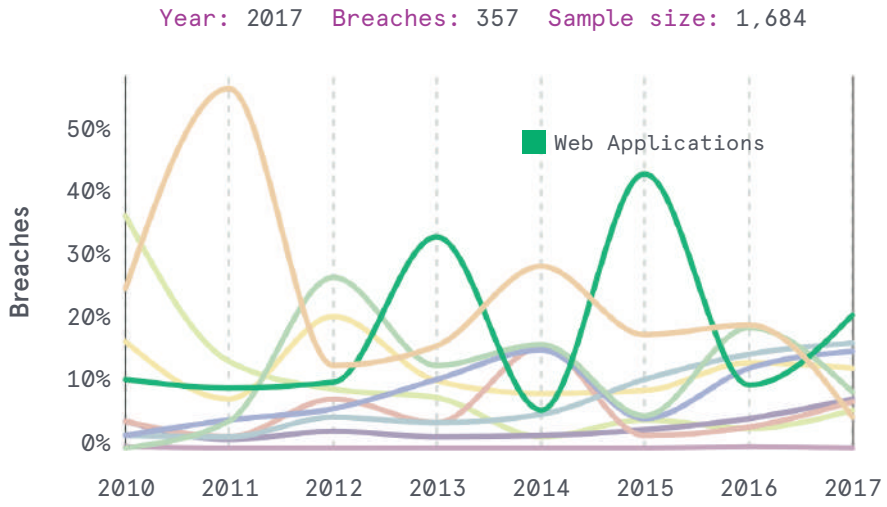


Figure 14. Verizon Data Breach Incident Report 2018

Web applications are increasingly indicated in breaches, growing even more strongly in 2017 to surpass privilege misuse, cyber-espionage, and point-of-sale and payment card skimmers, among others.

When considering industries that have been breached, Verizon reports that the retail industry has been most affected, with healthcare coming in second. Payment Card Industry Data Security Standard (PCI-DSS) requirement 6.6 suggests "installing an automated technical solution that detects and prevents attacks" as a method of mitigating dangerous web application attacks. Most companies utilize a Web Application Firewall (WAF) to meet this requirement, but it is not a "one-size-fits-all" solution. To be effective, a WAF must protect your applications regardless of platform, and must take into account that many applications are housed in more than one environment. An effective WAF must be a cloud, hardware, or CDN-agnostic solution. In many cases, the best approach is to combine WAFs with DDoS mitigation vendors. This combination ensures that an attack will not sneak in via a gap in coverage, which can occur when protections are provided by disparate vendors.

WEB APPLICATIONS BREACHES BY INDUSTRY

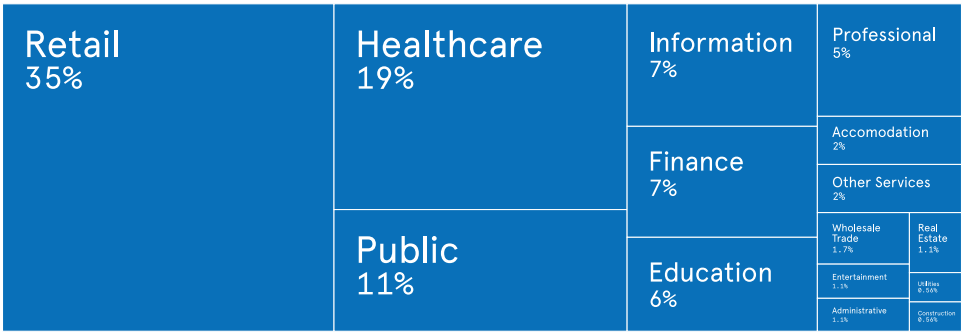


Figure 15. Verizon Data Breach Incident Report 2018

Notable Exploits — Rasputin

The name Rasputin has frequently come up in discussions about web application exploits over the past year. Rasputin is not the name of an exploit, but rather the alias of the author, said to be a Russian-speaking, financially motivated hacker. Rasputin is believed to have breached over 60 prominent targets, state and local governments, and colleges and universities in the U.S. and the UK. Rasputin apparently developed his own SQL injection scanner, which he used to find and take over vulnerable targets. This approach is noteworthy, not because SQL injection scans are unusual, but because they have become so common that most hackers take advantage of freely available scanners to conduct reconnaissance, rather than go to the trouble to write their own. Once vulnerable targets have been identified, Rasputin conducts an SQL injection attack, making off with personal data that is then offered for sale.

IPv6 Attacks

IPv4 addresses are exhausted. This forecast, first examined in the 1980s, has been in the process of being fulfilled since 2011 in some regions. As of September 2015, North America exhausted its pool of addresses. While ISPs in each region may have unassigned pools of IP addresses, and can recycle those that are no longer needed by subscribers, the fact is that IPv6 is finally beginning to make its way into the mainstream. Because of the fundamental differences between them, it has been vitally important that existing IPv4 networks can still operate as IPv6 gets implemented. Some companies have begun the process by running "dual stacks," running IPv4 and IPv6 in parallel, often with two different teams. This approach speeds IPv6 network implementation but works against consistent security. Complicating matters even further, many security tools still do not support IPv6, or may not be configured properly. This allows attackers to bypass firewalls and intrusion preventions systems, generating malicious IPv6 traffic that these controls do not recognize. Another attack features both IPv4 and IPv6 traffic. Such an attack can proceed while target security teams implement IPv4 defenses, and cause confusion when the usual tools do not completely mitigate the offensive. IPv6 could then be used to compromise the networking infrastructure used to run the dual protocols side by side, attacking the IPv4 stack through a backdoor.

IPv6 addresses can also be used for amplification attacks, including a recent DNS attack. The Internet community has recently been dedicated to plugging these holes in IPv4 DNS open resolvers, aided by the fact that the address space is scanable. The IPv6 space, however, is new and much larger. In the most recent attack, computers behind 1,900 IPv6 addresses attacked a DNS server as part of a larger army of commandeered systems, most of which used IPv4 addresses. Of the 1,900 IPv6 addresses, 400 were used by poorly configured DNS systems, producing roughly one-third of the overall attack traffic. Because DNS configuration for IPv6 is very different than that used for IPv4, DNS-based amplification attacks could become an enormous problem in the future.

On the plus side, IPv6 networks are still not ubiquitous enough for attackers to focus on and develop new attack methods specifically for the new protocol—IoT products and the botnets that target them are focused almost entirely on IPv4. But on the downside, pretty much every modern mobile device and PC has IPv6 support included and turned on as a default, so when those IPv6 attacks come, they are going to hit hard.

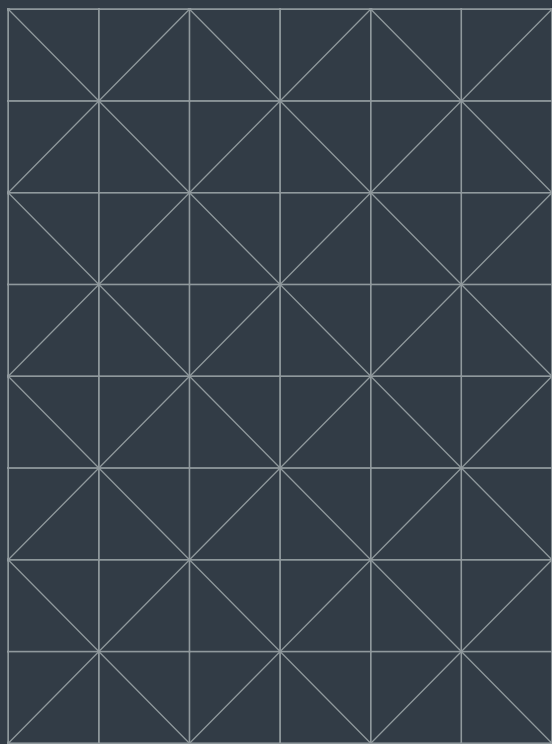
Mitigation

Today's threats are not standing still. New malware types are evolving every day. The astronomical growth of often-vulnerable IoT devices has created a fertile ground for botnets of all types. Amplification attacks are as close as the next unsecured service or unapplied patch. The question has become not if you will be attacked, but when.

Perhaps the best advice comes from the Verizon Data Breach Incident Report, 2018, which suggests, "Don't roll the dice. While we are not seeing the biggest and baddest attacks on a daily basis, ensure that you have retained DDoS mitigation services commensurate to your tolerance to availability loss. Verify that you have covered all of your bases from a scoping standpoint."[15]

Organizations often focus on defending against a single type of threat, but attacks are increasingly blending. Such blended attacks raise the importance of a holistic and comprehensive defense. For example, the combination of a WAF and DDoS mitigation system from the same vendor often provides a more seamless and comprehensive defense.

THE QUESTION HAS BECOME NOT IF YOU WILL BE ATTACKED, BUT WHEN.



HOW ORGANIZATIONS' ABILITY TO RESPOND TO THREATS HAS CHANGED

During January–February 2018, organizations have focused most on their ability to respond to ransomware, DDoS, generalized phishing and targeted hacking.

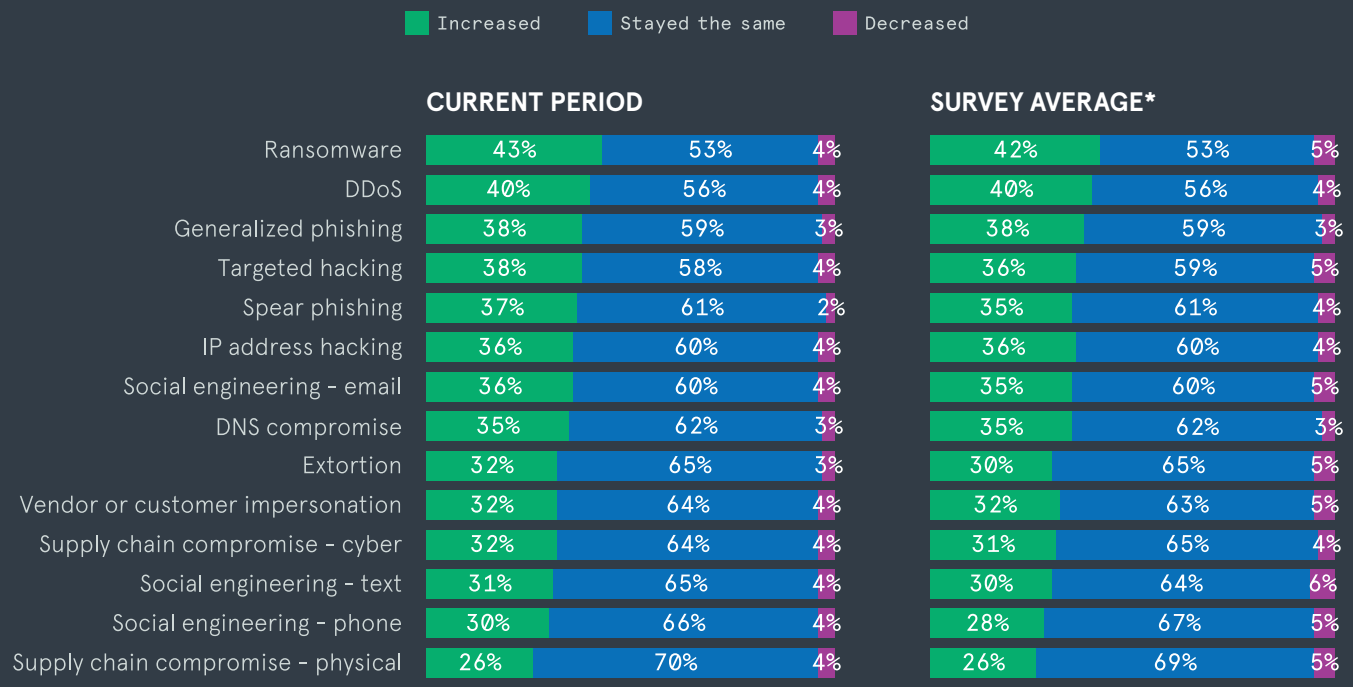


Figure 16. Neustar International Security Council

*Survey Average is the cumulative average of survey data collected bi-monthly from seven different surveys of ~300 security professionals, beginning in May 2017 and completed most recently in March 2018.

MITIGATION

On-Premise or Cloud?

Organizations are increasingly faced with the question of where to place their DDoS mitigation infrastructure. Some companies have followed the practice of keeping their defenses on-premise to ensure unified control. But this approach simply cannot succeed in the face of today's large threats, nor is it always effective in finding quantum or pulse attacks that may be of insufficient size to stand out. But still, some organizations hesitate to move all of their defenses to the cloud.

Often the best answer to the on-premise or cloud conundrum is to implement both. Groups are increasingly moving to hybrid DDoS and WAF solutions. On-premise systems are able to provide immediate response to day-to-day attacks and fail over to the high-capacity cloud-based component if required.

IMPACT OF CYBER ATTACKS

Over nine out of ten participants agreed escalating costs of on-premise hardware mean they are looking to move towards cloud solutions for DNS and DDoS mitigation. This increases the survey average by three points.

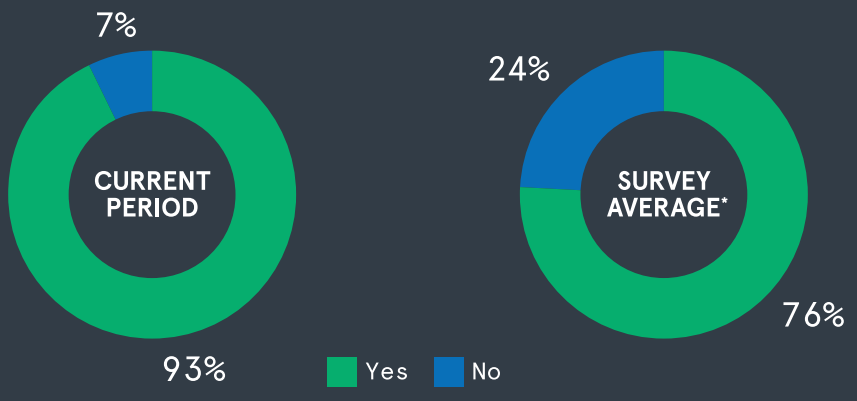


Figure 17. Neustar International Security Council

*Survey Average is the cumulative average of survey data collected bi-monthly from seven different surveys of ~300 security professionals, beginning in May 2017 and completed most recently in March 2018.

MITIGATION

In-House or Outsource?

Another question in organizational security is whether to outsource DDoS mitigation or try to handle it in-house. Most industry experts suggest that companies outsource mitigation. Buying and maintaining up-to-date infrastructure is one hurdle, but often, the more daunting hurdle is finding, training, and maintaining the expert staff. Another consideration is the size and types of threats to which mitigation infrastructure is exposed.

WHETHER SURVEY RESPONDENTS OUTSOURCE DDoS MITIGATION

48% of enterprises surveyed in March 2018 outsource their DDoS mitigation, higher than any previous reporting period, and pushing the average up to 42%.

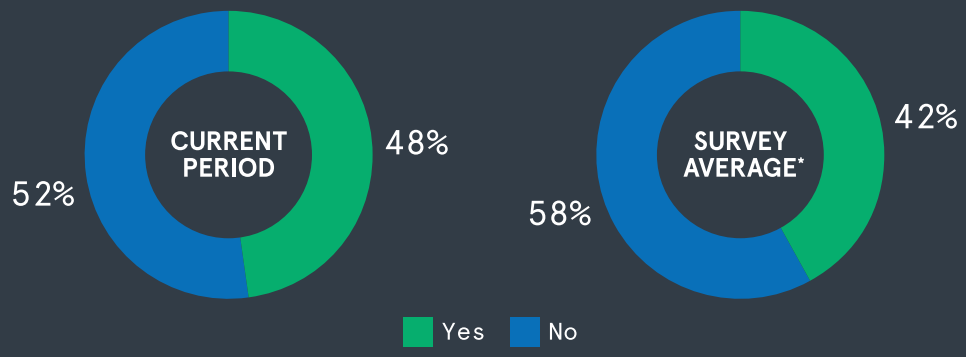


Figure 18. Neustar International Security Council

*Survey Average is the cumulative average of survey data collected bi-monthly from seven different surveys of ~300 security professionals, beginning in May 2017 and completed most recently in March 2018.

Summary

A look at the different types of threats propagating today, combined with the sheer volume of attacks, can paint a discouraging picture. Even more alarming, however, is the fact that today's threats seldom occur in isolation. A DDoS threat in one segment can divert attention from malware in another. Ransomware can be used to hasten data exfiltration. IPv6 attacks can be used to access parallel IPv4 constructs.

Another consideration is that, with individual components available for sale, attackers no longer need overall computer or network expertise. Botnets can be rented and application exploits simply purchased. This allows perpetrators to concentrate on results that they desire without having to actually create the means to commit the crime. This is obvious from the results of Verizon's 2018 Data Breach Incident Report, which shows that 50% of breaches were carried out by organized criminal groups, and 12% involved nation-state or state-affiliated actors.

The bottom line is that for today's enterprise, the question is not whether you will be attacked. It's when, by what, and how badly your company's reputation or finances will be damaged. And one thing is sure in the uncertain world of cybersecurity — the wrong time to consider defense is after the attack has occurred.

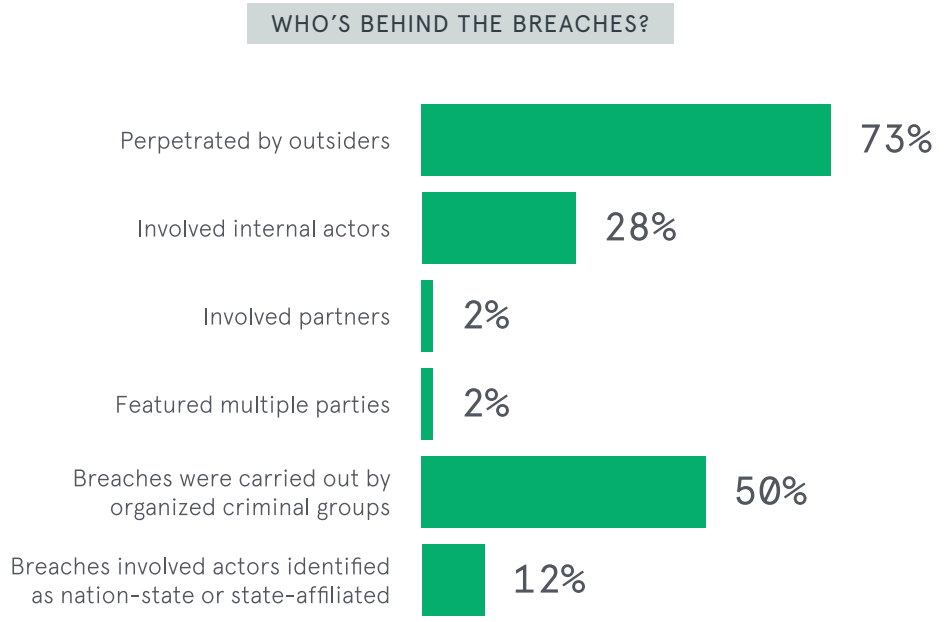


Figure 19. Verizon Data Breach Incident Report 2018

Call on Neustar

Neustar is in a unique position to provide protection to our customers because we are a target as well as a service provider. Neustar manages, maintains, and delivers one of the largest DNS services in the world, which means we are constantly under attack. Neustar defenses are not just created for our customers, we literally have to stay a step ahead of attackers to stay in business.

The benefits of outsourcing DDoS defense are growing, not just due to the large attacks, but the small, quantum attacks we've started to see as well. If you're running multiple data centers, with thousands of internal and external users, and tens of thousands of applications running in the cloud, you are probably never going to see an anomaly of 300 Mbps. It won't trigger cloud failover, it won't trigger any massive alerts...and attackers know it. This reality reveals one of the key advantages of working with Neustar, because when it comes to threats, we see both the very big and the very small. Our investments enable us to protect our customers just as we protect ourselves.

The Neustar SiteProtect NG DDoS mitigation service is constantly being expanded and enhanced such as adding different types of triggering, as well as new, flexible options. We also recognized that a cloud-based Web Application Firewall (WAF) was key to protecting against threats at the application layer. While the WAF market is mature, the Neustar difference is that our WAF is part of our dedicated DDoS mitigation network, with an industry-leading 10TBps of scrubbing capacity, designed to provide global protection from Layer 3 to Layer 7.

A network of that size has other benefits, as well. Other companies may talk about rapid response and fast SLAs, but Neustar responses are designed to be nearly instantaneous. This means that Neustar can put an attack down and update global rulesets in the same amount of time other vendors are just starting to respond.

Finally, in order to ensure that organizations are getting protection that fits their needs, we believe it is important to step back and assess, rather than assume. Neustar provides vulnerability and penetration testing to help customers establish a baseline, so they can make the correct investments into their security.

How We Can Help

To learn how your organization can do more to combat the DDoS threat, visit us online at **www.defense.neustar** or call **+1 855-727-1209 (US), +44 1784 676062 (EMEA), +61 3 9866 3710 (APAC).**

Appendix

1 Verizon Data Breach Incident Report 2018
2 World Economic Forum Global Risk Report, 2018
3 Cisco 2017 Annual Cybersecurity Report
4 Kaspersky Lab's Global IT Security Risks Survey 2017
5 https://www.us-cert.gov/ncas/alerts/TA14-017A
6 https://www.us-cert.gov/ncas/alerts/TA13-088A
7 https://www.us-cert.gov/ncas/alerts/TA14-013A
8 https://ldapscan.shadowserver.org/
9 https://www.akamai.com/us/en/about/our-thinking/threat-advisories/connection-less-lightweight-directory-access-protocol-reflection-ddos-threat-advisory.jsp
10 https://www.researchgate.net/publication/284077229_TFTP_DDoS_amplification_attack
11 https://memcachedscan.shadowserver.org/
12 https://krebsonsecurity.com/tag/memcached-attack/
13 https://isc.sans.edu/forums/diary/Why+we+Dont+Deserve+the+Internet+Memcached+Reflected+DDoS+Attacks/23389/
14 Cisco 2018 Cybersecurity Report
15 Verizon Data Breach Incident Report 2018

About Neustar.

Neustar, Inc. is a leading global information services provider driving the connected world forward with responsible identity resolution. As a company built on a foundation of Privacy by Design, Neustar is depended upon by the world's largest corporations to help grow, guard and guide their businesses with the most complete understanding of how to connect people, places and things. Neustar's unique, accurate and real-time identity system, continuously corroborated through billions of transactions, empowers critical decisions across our clients' enterprise needs.

More information is available at

www.home.neustar

WP-SS-132495-01.17.2019