

ISSUE 4: FINDINGS FROM 2H 2019

NETSCOUT THREAT INTELLIGENCE REPORT

With key findings from the 15th
Annual Worldwide Infrastructure
Security Report (WISR)

NETSCOUT®

TABLE OF CONTENTS

Introduction	1
Editor's Note	1
Executive Summary	2
<hr/>	
1. DDoS	4
Key Findings	4
DDoS Attack Trends	5
DDoS Highlights	8
<hr/>	
2. WISR Survey	16
Key Findings	16
Service Provider	17
Enterprise	20
<hr/>	
3. IoT Malware	22
Key Findings	22
IoT Highlights	23
<hr/>	
4. Advanced Threat	28
Key Findings	28
Nation-State Actor Highlights	29
<hr/>	
5. Crimeware	32
Key Findings	32
Crimeware Highlights	33
<hr/>	
Conclusion	36
<hr/>	
Appendix	37

EDITOR'S NOTE

RICHARD HUMMEL Threat Intelligence Manager, NETSCOUT

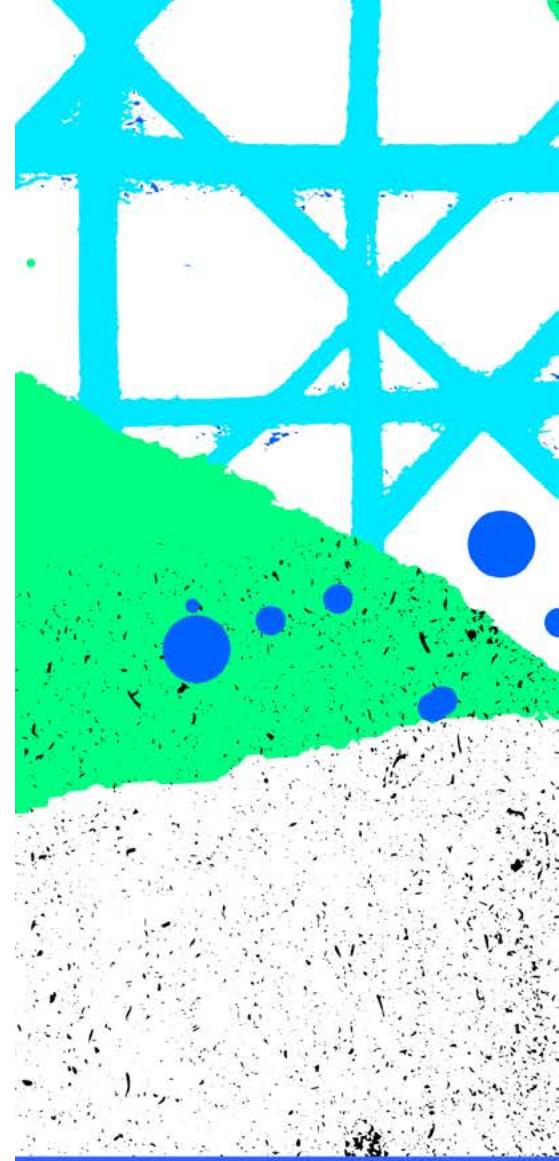
We are in the midst of a major evolution in the world of cybercrime; adversaries are more resilient, and cyber threats are more complex.

Distributed Denial of Service (DDoS) attacks have grown in frequency each year for the past five years, while attackers continue to unleash increasingly sophisticated attacks. As the Internet of Things (IoT) population explodes in size, malware authors are ready and waiting with new strains and capabilities to target the growing diversity of products. Crimeware operators constantly adapt, surviving take-down attempts and renewing operations with vigor. Last, but certainly not least, advanced persistent threat (APT) groups develop innovative new ways to track targets, which often includes monitoring their own country's citizens with mobile malware.

How do we combat this? It starts with awareness. NETSCOUT has unparalleled visibility via our Active Threat Level Analysis System (ATLAS), which shines a light on activity observed across the virtual world, making certain that not only customers, but everyone, everywhere, knows what lurks behind the code of our internet-connected world. This visibility, combined with world-class insights from the ATLAS Security Engineering & Response Team's (ASERT) analysts and engineers, gives us deep insight into ongoing threat landscape activity. We saw attackers ramp up their target reconnaissance and research prior to launching laser-focused DDoS attacks that can reduce the availability of critical internet-facing applications, services, and supporting infrastructure. We also noted their extreme efficiency. Attackers typically leverage only a small proportion of potentially abusable devices in order to carry out successful attacks. In fact, the largest OpenVPN reflection/amplification DDoS attack we observed in the second half of 2019 used less than 1 percent of the available reflector/amplifiers connected to the internet. We observed similar behavior across known UDP reflection/amplification DDoS attack vectors. And finally, IoT risk continues to grow as attackers leverage the millions of IoT devices produced by manufacturers who show a complete lack of concern about device security.

With key findings from the 15th Worldwide Infrastructure Security Report (WISR) and recommendations for defense in the DDoS world, NETSCOUT's biannual Threat Intelligence Report brings you the current state of affairs for the second half of 2019, showcasing trends, techniques, strategies, and new attack vectors across the threat landscape.

We also offer you a new way to see that landscape. Recently made available to the public, [NETSCOUT's Cyber Threat Horizon](#) offers a glimpse into the DDoS world as we see it, putting control into your hands to stay current on DDoS affairs in every region of the world. This online resource lets you observe first-hand the evolutionary transformation of the DDoS threat landscape.



CONTRIBUTORS

Richard Hummel
Carol Hildebrand
Hardik Modi
Gary Sockrider
Roland Dobbins
Steinþor Bjarnason
Jill Sopko
Suweera DeSouza
Ivan Bondar
Oliver Daff
ReversingLabs (Partner)

SEVEN

New or increasingly used attack vectors in 2019

20.4B

Devices forecast to connect to the internet in 2020

▲ 57%

Mirai-based variants from 2018 to 2019

EXECUTIVE SUMMARY

WE WANT YOU TO REMEMBER ONE NUMBER: 8.4 MILLION.

That is the number of DDoS attacks NETSCOUT Threat Intelligence saw last year alone: more than 23,000 attacks per day, 16 every minute. Any way you slice it, that's a huge number of attacks.

What does that mean to you? Enterprises and service providers need to defend themselves against attacks—and protect their customers. We found customer-facing services and applications were targets of DDoS attacks at two-thirds of enterprises. Even worse, customers can act as conduits for attacks: adversaries deployed a novel technique that used attacks on client services to access core services at well-protected targets. If you have a mobile phone—or run a mobile network—beware: APT groups are bumping up mobile malware use, while DDoS attacks on mobile networks jumped 64 percent in the second half of 2019. The reality is, attackers are smart and efficient and never give up. They widely weaponized seven new or increasingly popular DDoS attack vectors in 2019 while adding new techniques to existing methods. They can change attack vectors and techniques on the fly—all while effectively husbanding resources and more accurately targeting attacks. In fact, it takes shockingly little to launch an effective attack; most use less than 3 percent of available resources in that attack vector. And let's not forget the legion of IoT botmasters, salivating at the thought of the 20.4 billion devices forecast to connect to the internet in 2020¹—and with access to an ever-growing selection of malware strains that target a growing number of system architectures.

KEY FINDINGS

Lucky Seven for Attackers

Attackers weaponized seven new or increasingly common UDP reflection/amplification attack vectors in 2019. They also combined new variations of well-known attack vectors—all while remaining operationally efficient and launching pinpoint-focused DDoS attacks.

New Methods Pump Up Attacks, Bypass Traditional Defenses

Attackers not only combined attack vectors but also made them stronger than the sum of their parts by combining TCP reflection/amplification attacks with carpet-bombing techniques. Meanwhile, adversaries using advanced reconnaissance discovered how to use the client services of well-protected targets like Internet Service Providers (ISP) or financial institutions to amplify attacks against specific enterprises and network operators.

▲ 87%

Increase in exploit attempts from 2H 2018 to 2H 2019

▲ 16%

Global DDoS attack frequency

622 Gbps

Max attack in 2H 2019

Mobile Networks, Devices in Attacker Crosshairs

Wireless telecommunications companies experienced a 64 percent increase in DDoS attack frequency year over year. This likely reflects the increased tendency of gamers in many Asian countries to use their phone service as wireless hotspots, as well as the increased popularity of gaming on mobile devices with 4G and LTE connectivity. As gaming continues to be a prime motivation for DDoS attacks, adversaries naturally follow their targets, further leading to the growth in attacks. Meanwhile, APT groups are increasingly using mobile malware—including commercially available apps—to infiltrate international targets as well as monitor internal dissidents and protesters.

IoT = Intensification of Threats

Botmasters eagerly await the 20.4 billion IoT devices forecast to connect to the internet in 2020, with an ever-growing selection of malware strains to choose from. From 2018 to 2019, we saw a 57 percent increase in Mirai-based variants targeting 17 system architectures. ASERT honeypots reflect this growth with an 87 percent increase in the number of exploit attempts during the latter half of 2019.

WISR Survey Highlights IoT, Cloud Risk

Survey data from the 15th Worldwide Infrastructure Security Report (WISR) shows that infected and compromised endpoint IoT devices are a top concern for enterprises, along with detection/identification of IoT devices on their networks, software patching and maintenance of IoT devices, and compliance risks posed by IoT. The survey also showed a dramatic increase in DDoS attacks on publicly exposed service infrastructure, reported by 52 percent of service providers in 2019 compared with only 38 percent in the previous year.

DDoS

1

Today's attackers have augmented the DDoS equivalent of sledgehammers with a quiver of custom arrows as they increasingly conduct extensive reconnaissance and choose weapons specifically tailored to exploit the defensive weaknesses they discover.

Even worse, they have an ever-growing range of new or increasingly popular vectors to choose from—seven in 2019 alone. These canny adversaries further integrate existing techniques such as carpet-bombing, unleashing attacks that use the minimum firepower to get results. In other words, we are seeing a devastating combination of attacker innovation married to operational efficiency, as reflected in two contrasting data points: a 54 percent decrease in observed attacks over 200 Gbps accompanied by a 15 percent increase in attacks between 100 Gbps and 200 Gbps.

KEY FINDINGS

- 1 Advanced Recon Bypasses Stout Defenses**
Attackers using advanced reconnaissance were able to bypass traditional defenses by employing a newly weaponized tactic that exploited the client services of well-protected targets such as ISPs or financial institutions to amplify attacks against specific enterprises and network operators.
- 2 Constant Innovation Marries Operational Efficiency**
Adversaries discovered and weaponized seven new or increasingly popular attack vectors in 2019, adding new variations of existing attack methods—all while effectively husbanding resources and more accurately aiming attacks.
- 3 Carpet Bombers Up the Ante**
Attackers not only combined attack vectors but also made them stronger than the sum of their parts by combining TCP reflection/amplification attacks with carpet-bombing techniques. In this equation, two plus two adds up to far more than four.
- 4 Attack Frequency Only Knows One Direction: Up**
Overall DDoS attack frequency jumped 16 percent from the second half of 2018 to the second half of 2019, while adversaries using larger attacks zeroed in on the 100–200 Gbps range.

SEVEN
New or increasingly used vectors in 2019

▼ 54%
Attacks greater than 200 Gbps from 2H 2018 to 2H 2019

▲ 87%
Exploit attempts from 2H 2018 to 2H 2019

▲ 16%
Global DDoS attack frequency

▲ 15%
Attacks 100–200 Gbps+



DDoS ATTACK TRENDS

Attackers have learned that you don't need a nuclear weapon to swat a fly. We observed a significant drop in frequency of attacks larger than 200 Gbps, a reflection of maturation in the attacker market. Indeed, very large attacks are often not only overkill, but they also draw unwanted attention from law enforcement. Nobody wants to be the nail that sticks up—just ask the person who was nabbed in September's World of Warfare takedown². Instead, it's far better to launch attacks using the minimum resources needed to get the right result. Hence, it's not surprising to see the 15 percent overall growth in 100–200 Gbps attacks, although that number varied by region. EMEA and Latin America, for example, saw growth of 62 percent and 100 percent, respectively, in 100–200 Gbps attacks.

Overall DDoS attack frequency increased a relatively modest 16 percent during the second half of 2019 compared with the same time period in 2018. Meanwhile, memcached excepted, max attack size has remained relatively constant over the past several years, emphasizing the importance being able to routinely mitigate attacks in the hundreds of Gbps range.

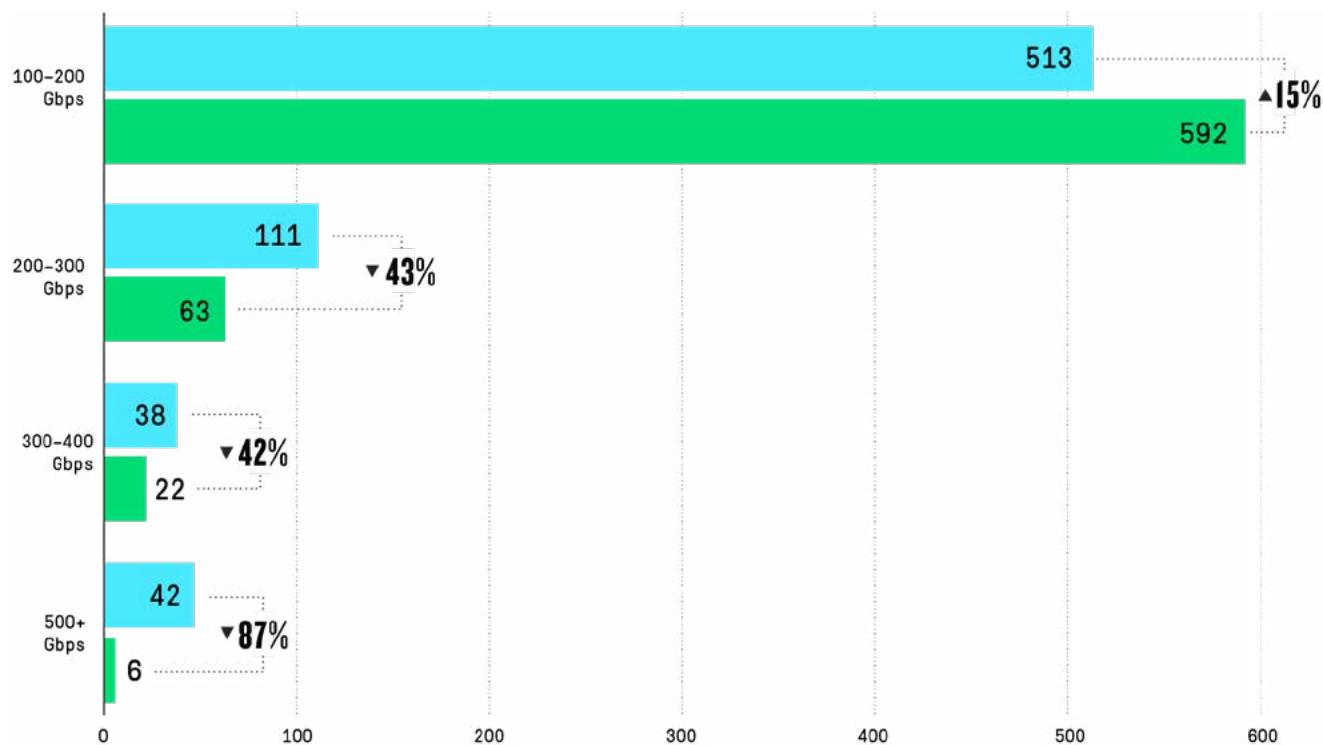


Figure 1: Year to Year Attack Size Trends

● 2018 ● 2019

VERTICAL INDUSTRY ATTACKS

We analyzed attack data by North American Industry Classification System (NAICS) codes, which group companies into 22 broad categories that contain multiple large subvertical sectors.

Looking at the list in more detail reveals continued focus on financially attractive targets, as well as some significant shifts in targets across several vertical sectors.

We witnessed only minor jostling for positioning in the top 10 most targeted sectors year over year, with the exception of satellite telecommunications, which was new to the list. Attackers are increasingly attacking wireless and satellite communications, while attacks on wired telecom are nearly stagnant.

As has been the case for every threat report thus far, the top four subvertical sectors remained the same (Figure 2). We expect to see this top four, since such activity is inherent to their role as connectivity providers, with attacks focused on their residential and business subscribers as well as on their operational infrastructures. Looking at the list in more detail reveals continued focus on financially attractive targets, as well as some significant shifts in targets across several vertical sectors.

The Top Four Sub-Vertical Sectors

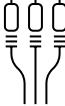
Rank	Vertical	Attack Frequency	Max Attack	Classification
1	 Wired Telecommunications Carriers	1,073,851	421.5 Gbps	Information
2	 Telecommunications	575,749	348.9 Gbps	Information
3	 Data Processing, Hosting + Related Services	467,475	243.4 Gbps	Information
4	 Wireless Telecommunications Carriers	342,327	492.5 Gbps	Information

Figure 2: Top Four Sub-Vertical Sectors

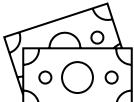
Hot Attack Targets



Focus Point: Mobile Networks

Adversaries turned up the attack volume on the wireless telecommunications sector, with a 64 percent increase in attack frequency and a 33 percent increase in max attack size. Gaming continues to be a large motivation for attacks, and mobile networks are increasingly popular access points, since users in many Asian countries rely on their phone service for wireless hotspots. Attackers naturally follow their targets, leading to the upward attack growth in the sector. Attacks in the wired telecommunications sector, meanwhile, grew at a comparatively modest 3 percent.

▲ 64% Increase in attack frequency



Catnip Level: Achieved for Financiers

The finance and insurance sector retained its catnip status with financially motivated attackers, as attack frequency grew by 56 percent. In particular, the commercial banking subsector experienced 257 percent growth in frequency, likely an effect of the coordinated attacks on European financial organizations earlier in the year, while attacks on direct health and medical insurance carriers leaped 399 percent.

▲ 56% Increase in attack frequency



Carpet Bombers Sideswipe Satellite Telecoms

Satellite telecommunications saw significant increase in attacks, with 295 percent increase in attack frequency, likely due to scenarios such as the high-impact carpet-bombing attacks that targeted financial organizations in Asia Minor and Europe in 2H 2019. By sharing large netblocks with organizations that didn't have their own IP space, the satellite telecommunications providers experienced significant collateral damage from these attacks.

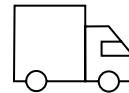
▲ 295% Increase in attack frequency



Chemical Warfare

Chemical manufacturing got hit with a 50 percent increase in attack frequency and 676 percent increase in max attack size.

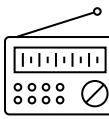
▲ 676% Increase in max attack size



Big Attack in the Trades

Wholesale trade, which includes motor vehicle and motor vehicle parts and supplies as well as computer equipment subsectors, saw an 834 percent increase in max attack size.

▲ 834% Increase in max attack size



Attackers Eye Air Waves

Both the folks who broadcast and the people who make their broadcast equipment came under increased attack in 2H 2019. Radio and television broadcasting saw a 598 percent increase in max attack size and 63 percent bump in attack frequency, while the radio and television broadcasting/wireless communications equipment manufacturing sector had a 502 percent increase in attack frequency.

▲ 598% Increase in max attack size



School's in Session for DDoS

A number of sectors related to education came under increased pressure from attackers. Attack frequency for educational services grew by 41 percent, while the max attack size for technical and trade schools and colleges jumped 58 percent and 6 percent, respectively.

▲ 41% Increase in attack frequency



DDoS HIGHLIGHTS

Consider the dedication of botnet operators. They could rest on their laurels, gleefully adding millions of vulnerable IoT devices to already-formidable botnets and launching attacks with the wealth of methods already available. Instead, this dedicated band combines constant innovation with obsessive devotion to operational efficiency.

Skilled attackers relentlessly uncover and exploit new UDP reflection/amplification DDoS vectors, which are inevitably weaponized by booter/stresser and DDoS-for-hire services for use by casual attackers. Not only do these vectors include protocols responsive to malicious packets, but attackers also leverage abusable devices such as IPMI servers to take part in their reflection/amplification attacks.

Seven New Attack Vectors

In 2H 2019, we noted two attack vectors—Intelligent Platform Management Interface/Remote Management Control Protocol (IPMI/RMCP) and OpenVPN—that came under scrutiny. The grand total for 2019: seven new or increasingly used DDoS attack vectors. There are roughly 2.5 million vulnerable devices worldwide that can be used to launch attacks using these seven vectors.

Carpet-Bombing Techniques

Attackers not only combined attack vectors but also added even more bang for the buck by using target addressing techniques such as carpet bombing when launching TCP reflection/amplification attacks. Combined with advanced reconnaissance of the online business relationships between targeted organizations, these tactics allow attackers to raise the bar for defenders in terms of accurately detecting, classifying, tracing back, and mitigating bespoke DDoS attacks.

Adaptable Attack Vectors

Attackers monitored the efficacy of their attacks and rapidly changed or added new attack vectors as defenders implemented successful defenses.

Bypassing Traditional Defenses

Many of the newer attack vectors often do not have as high packet-per-second rates or bandwidth as traditional attacks. Rather, they either bypass poorly constructed network access policies (IPMI/RMCP and OpenVPN) or combine existing attacks into new powerful attacks (TCP reflection/amplification carpet-bombing).

Here's a rundown of the latest strategies, techniques, and attack vectors:

STRATEGY

Advanced Reconnaissance

Attackers increasingly perform extensive reconnaissance of both the victim's network and other devices that can be used to bypass defenses. In one example, attackers made use of novel reflection mechanisms to bypass recommended best current practices (BCPs) and access well-protected, high-powered DNS servers within an ISP. The attackers then launched large-scale DNS-reflection attacks by using CPE devices *within the ISP network* as DNS forwarders.

Likewise, attackers who combined TCP reflection/amplification with carpet-bombing target-address selection made use of the web server farms of financial institutions, governmental agencies, and other locale-specific enterprise organizations to attack broadband-access networks in those very same locales. This makes it more challenging for defenders to sort out the reflected attack traffic from legitimate server response traffic sourced from those very same enterprise organizations.

In other recent attacks on organizations in specific countries, attackers primarily used only DDoS reflectors and botnet devices within that country to bypass IP location filters.

STRATEGY

Changing Tactics on the Fly

While more sophisticated attackers have always attempted to monitor the efficacy of their attack, this practice is becoming increasingly common. Here, attackers respond by varying their attack methodologies and combinations while the attack is in process. Attackers are also using more automated attacks, combining different attack vectors and attack methods and constantly rotating those to make detection and mitigation more difficult for the defenders. In recent attacks, attackers have changed attack vectors every five minutes, making it very difficult to respond quickly enough to avoid down time. We believe that it is only a matter of time before attackers make use of automated techniques to monitor attack efficacy in real time and make automated on-the-fly adjustments in reaction to mitigation efforts.

TECHNIQUE

TCP SYN Reflection Using Carpet Bombing Techniques

TCP SYN attacks have been with us since the dawn of the internet, but they persist due to a combination of simplicity and the increased firepower available via unsecured IoT devices. Since organizations that lack DDoS defenses are easily taken out by a low-volume TCP SYN attacks, this technique is a logical first weapon of choice for attackers.

Like UDP reflection/amplification, TCP reflection/amplification is implemented by sending spoofed TCP SYN packets to a server on the internet, causing it to send multiple TCP SYN/ACK reply packets to the victim. The default setting on most Linux-based servers is to send as many as three replies when a TCP SYN packet is received, resulting in an amplification factor of 3:1. However, there are some internet devices that will send thousands of replies to spoofed TCP SYNs, as well as devices which will never stop sending replies. Indeed, some are still responding to probe packets sent by security researchers many months after initial TCP SYNs were received.

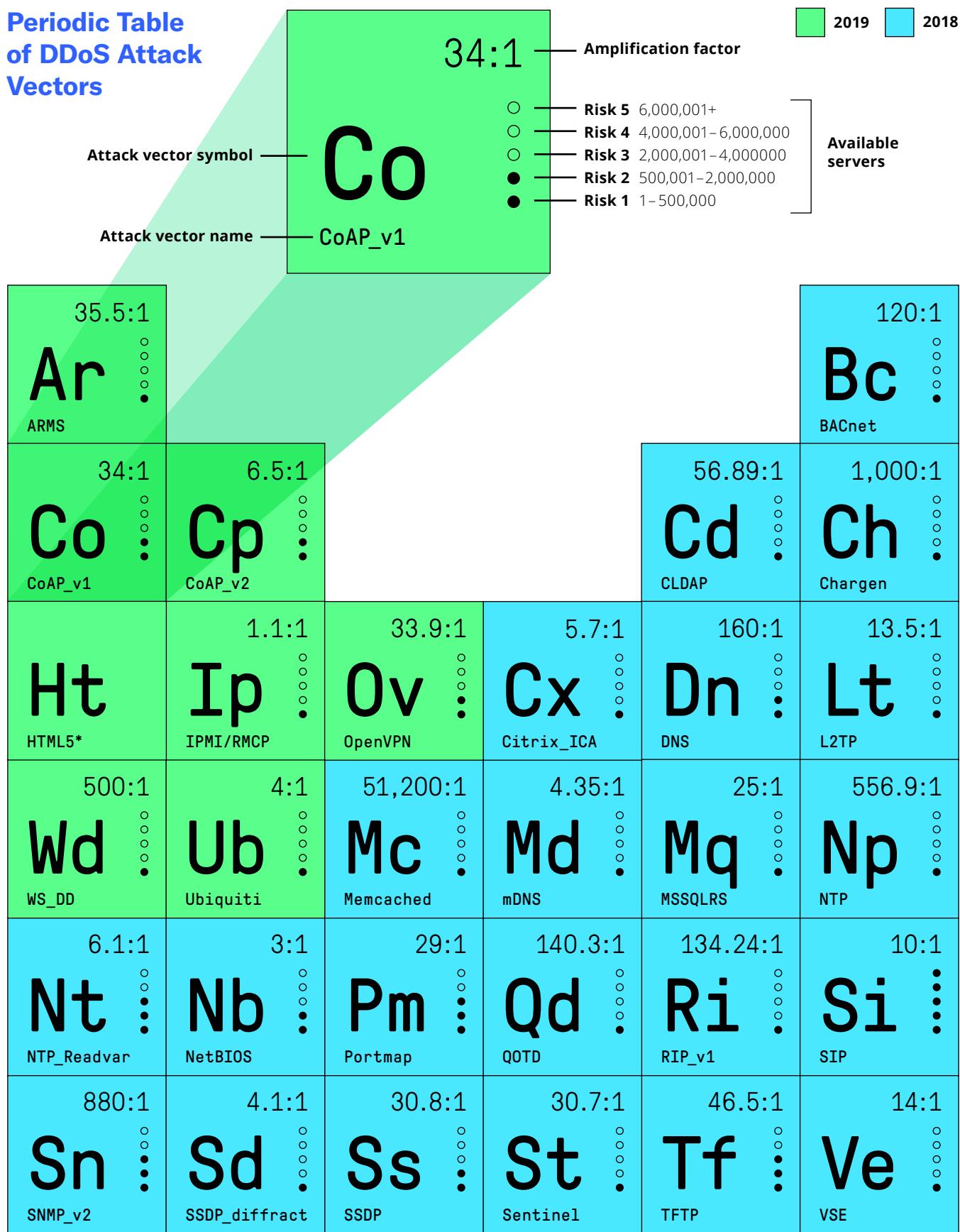
A well-defended organization should still be able to stop TCP reflection/amplification attacks but watch out for the new twist: In late 2019, attackers combined carpet-bombing techniques with TCP reflection/amplification attacks. The attacker will deliberately randomize the least-significant octets in the spoofed TCP SYN attack-initiator packets, resulting in a stream of TCP SYN/ACK packets continuously sweeping across an entire CIDR block for the duration of the attack. This target addressing technique can increase the difficulty of detection and mitigation.

Attackers began widely using this newly weaponized form of attack globally in November 2019, once again likely due to the indefatigable rapid-turnaround skills of the booter/stresser community.

Mapping the precise number of vulnerable devices on the internet is impossible, since basically every device offering a TCP-based service (HTTP/HTTPS, SSH, etc.) potentially can be used as a TCP reflector/amplifier. The population of abusable TCP-enabled nodes is certainly well in excess of 1 billion devices and counting.



Periodic Table of DDoS Attack Vectors



ATTACK VECTORS

Ip

Intelligent Platform Management Interface (IPMI)/Remote Management Control Protocol (RMCP)

Used for remote access to IPMI-enabled servers and systems, IPMI/RMCP has gone through a number of revisions and enhancements. However, almost all implementations support one of the older variants of the protocols, which allows the use of UDP port 623 for network transport. This means that if the server is not secured properly, anyone on the internet can send UDP-encapsulated queries to the server, not only gathering information about the server's hardware and software—which subsequently can be used to breach the server—but also using it to launch UDP reflection-type DDoS attacks by spoofing the source address.

IPMI/RMCP has a very low amplification factor of around 1.1:1, which sounds minimal compared with attack vectors such as Chargen, which has an amplification factor between 18:1 and 1,000:1. However, many organizations will allow UDP port 623 traffic through their firewalls, allowing a skilled attacker to either directly and repeatedly send IMPI RMCP queries to unsecured servers or bombard those servers with reflected responses from other unsecured IPMI servers on the internet. This can cause the IPMI service on the servers to crash, potentially causing collateral damage to all other services residing on those servers.

Attackers began widely using IPMI/RMCP as a DDoS vector in the second half of 2019, most likely as the botnet/stresser community rapidly weaponized it. At the latest count in December 2019, there were around 110,000 vulnerable IPMI servers on the internet.

At the latest count in December 2019

830,000

Vulnerable OpenVPN servers on the internet

0v

OpenVPN

The most popular VPN technology in use today, OpenVPN is used for remote-access and site-to-site VPN connections. OpenVPN uses its own SSL/TLS-based protocol, which also allows UDP-based communications. As with many other UDP-based protocols, attackers began using OpenVPN servers for DDoS reflection-type attacks in late 2019, for generic attacks as well as for targeted attacks against other VPN implementations. OpenVPN has a respectable amplification factor of 33.9:1, allowing it to be used for both typical reflection-type flooding attacks and more directed attacks.

Organizations that use OpenVPN will in many cases allow unrestricted communications via UDP source/destination port 1194, allowing attackers to flood the destination with OpenVPN packets, either as a direct attack or as reflected responses from other unsecured OpenVPN servers on the internet. This might cause the OpenVPN servers to become unresponsive, blocking legitimate users from using VPN services.

At the latest count in December 2019, there were around 830,000 vulnerable OpenVPN servers on the internet. The largest OpenVPN DDoS attack we observed used less than 1 percent of the available reflectors connected to the internet—a tiny portion of the available vulnerable devices.

At the latest count in December 2019

110,000

Vulnerable IPMI servers on the internet

What can be done?

DDoS attacks are inevitably growing in power and sophistication, driven by the ongoing back and forth between attackers and defenders.

As organizations put forth increasingly advanced DDoS defenses, attackers naturally respond with sophisticated techniques that are then rapidly weaponized and widely disseminated by botnet/stresser services. Even a well-prepared organization will often experience downtime when hit with a new attack due to the time needed for detection, mitigation, and follow-up. However, there are critical steps you can take to minimize the impact.

- **Defending attacks based on reconnaissance.**

Network operators and DDoS mitigation specialists must game out in advance tactics of this nature that are likely to be employed by skilled attackers, and ensure that they have situationally appropriate architectural principles, operational practices, and mitigation countermeasure capabilities in place to provide effective defenses against such bespoke attack methodologies. Organizations need to secure vulnerable devices and services in their own networks, making sure that only legitimate users can access these services. Otherwise there is a very high risk that these devices or services will be used to launch DDoS attacks against other organizations—or in the worst case, against the organization itself. Also, any other vulnerable services or devices that are not controlled by the organization itself should be isolated in quarantine networks so that they do not become a threat.

Fighting rapidly changing multivector attacks.

Here, it is extremely important to optimize DDoS defenses around the systems, services, and applications under protection, rather than solely against specific attack vectors. Moreover, organizations need automated DDoS detection and mitigation tools that can not only quickly identify and respond to DDoS attacks, but also adjust the mitigation methods as the attacker changes attack vectors. Regular attack mitigation drills are highly recommended for network operators and DDoS mitigation service providers to find and adjust to any changes in architecture, bandwidth, and servers, services, and applications. It's also extremely important to take into account ancillary supporting services such as DNS, as well as network infrastructure self-protection BCPs.

Preparation and DDoS training is a key element.

Organizations must take the time to understand their own network architecture and traffic flows during peace time, since trying to do so while under attack can be very difficult, often resulting in DDoS defenses blocking legitimate user traffic.

LIFE CYCLE OF AN ATTACK VECTOR

As part of our ongoing efforts to monitor the state of global DDoS threats, NETSCOUT also employs a high-powered scanner to look for vulnerable devices that respond to known attack vectors such as ARMS, CoAP, IPMI/RMCP, OpenVPN, Ubiquiti, and WS-DD.

Discovery

Figure 3 shows the number of devices/servers vulnerable to attackers as of December 31, 2019, when we focus specifically on these six vectors.

Attack Vector	Server Count	Change in Available Servers Per Day
Ar ARMS	47,790	-14.6
Ub Ubiquiti	166,255	-796.6
Co COAP_v1	616,252	234.7
Cp COAP_v2	689,812	77.2
Wd WS-DD	37,029	-8.6
Ip IPMI/RMCP	108,739	-25.0
Ov OpenVPN	822,891	190.2

Figure 3: Vulnerable Devices/Servers for the Top Six Attack Vectors

Inquiry

One of the things we wanted to do was to track their lifecycles over time. We wanted to collect data on questions such as:

- "How long does it take to clean up a vector?"
- "Does a vector decay or grow?"
- "Which vectors pose the greatest risk?"

The answers are not always straight forward, because there are a number of variables involved, such as the growth of IoT devices available to attackers, or organizations mass-deploying devices that may be at risk. Using data gleaned from our scanner, we mapped the six vectors over time.

Results

Although the results are anything but clear, some interesting conclusions can be drawn:

Decline

Some vectors do indeed decline over time, as we see with Ubiquiti.

Fluctuation

Other vectors fluctuate wildly. With CoAP v1/v2, for example, we observed drops as great as 200,000 devices, only to see the vector regain that ground within days and, in fact, gradually increase over time.

Consistency

Many vectors remain consistent for months, even after public disclosures of a new vector surfacing or an older vector becoming more active. ARMS, OpenVPN, and WS-DD are good examples of such consistency.

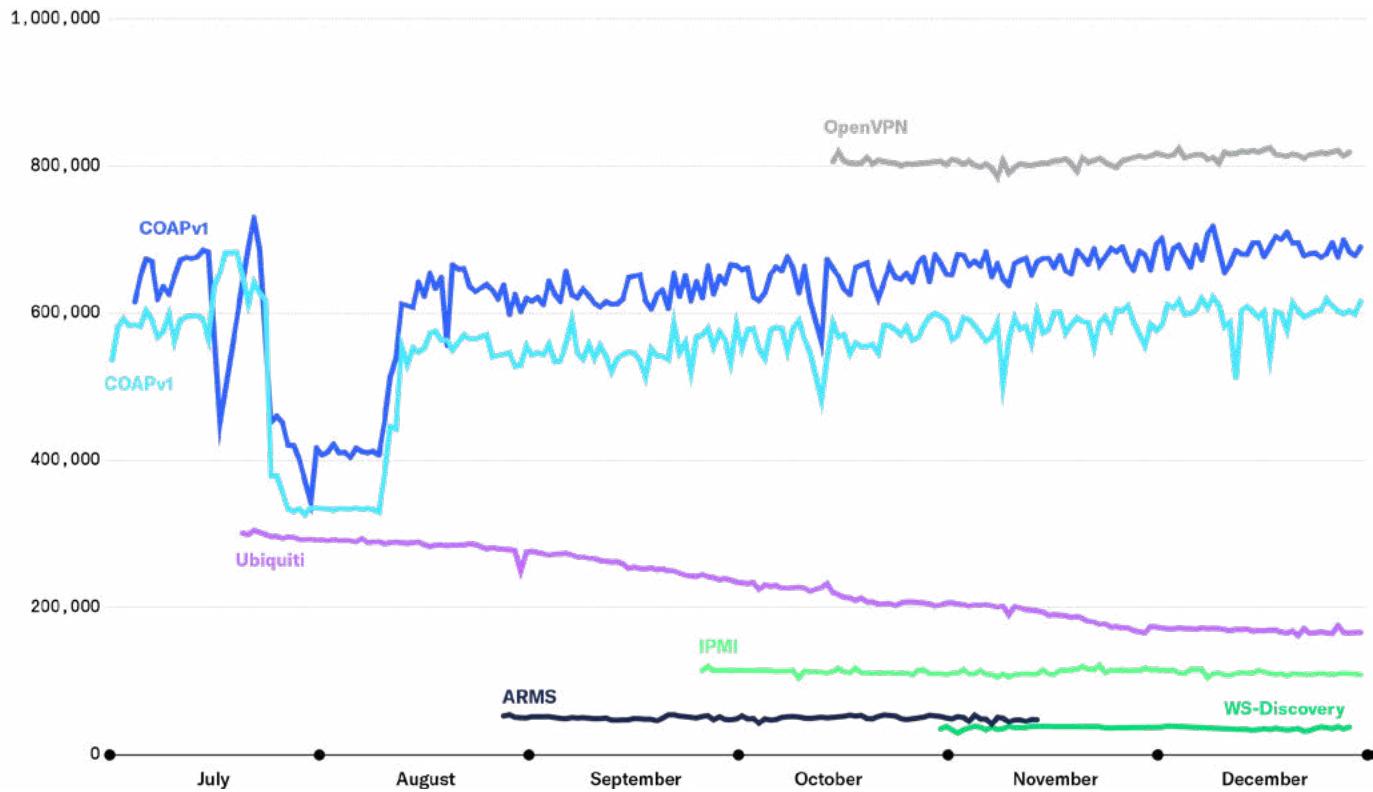


Figure 4: The Seven Vectors Server Counts for 2H 2019

14 Different Vectors

Used in at least one single attack in 2H 2019

717 Attacks

Using DNS, NetBIOS, Portmap, SNMP-v2, SSDP, TFTP

Dn	Nb	Pm
Sn	Ss	Tf

Lifecycle of an Attack

We then wanted to discover exactly how attackers leverage these vulnerable devices by looking at how many vulnerable devices attackers use in attacks. The answers surprised us more than the previous results on a vector's lifecycle.

Figure 4 illustrates how an attacker leverages existing vulnerable devices. These are based on our scans for vulnerable devices, correlated with the feedback we get from customer deployments around the world as part of our ATLAS data collection efforts. In this case, we expanded beyond the original six vectors to examine all of the vectors we currently track using this method.

In Figure 5, you'll see the protocol/vector in the first column, followed by the largest number of available servers for that vector used in an actual attack as observed by NETSCOUT. The last column shows the number of servers used in the attack compared with the entire population of servers available to an attacker.

The results are rather frightening when we consider that attackers use less than 25 percent of available resources for nearly every protocol out there—and yet, we still see attacks of more than 500 Gbps, or attacks combined with numerous other vectors that successfully take down networks.

Attack Vector		Max Servers in Attack	Percent of Population
Ar	ARMS	7,422	17.8%
Bc	BACnet	190	1.13%
Ch	CHARGEN	3,001	9.73%
Cd	CLDAP	8,874	86.87%
Co	COAP_v1	2,296	0.46%
Cp	COAP_v2	2,311	0.42%
Cx	Citrix-ICA	809	12.84%
Dn	DNS	107,786	6.32%
Ip	IPMI/RMCP	13,229	14.01%
Lt	L2TPw	13,235	1.43%
Mc	Memcached	380	7.92%
Md	mDNS	4,106	1.03%
Mq	MSSQLRS	1,591	1.51%
Nb	NetBIOS	8,362	1.22%
Np	NTP	2,010	7.05%
Nt	NTP-readvar	16,734	0.64%
Ov	OpenVPN	3,907	0.59%
Pm	Portmap	6,661	0.26%
Qd	QOTD	4,286	12.85%
Ri	RIP_v1	938	10.33%
Sd	SSDP_diffraction	25,367	2.16%
Si	SIP	8,836	0.19%
Sn	SNMP_v2	19,656	0.99%
Ss	SSDP	28,348	1.99%
St	Sentinel	836	8.99%
Tf	TFTP	11,239	0.49%
Ub	Ubiquiti	41,339	24.57%
Ve	VSE	811	5.9%
Wd	WS-DD	834	2.84%

Attacks Using 11+ Vectors**▲ 1800%**

Attacks in 2H 2018

30

Attacks in 2H 2019

570**Multivector Attacks**

The research into attack vectors and how attackers leverage them illuminates the ever-evolving nature of the DDoS threat landscape. When a door closes, attackers find a window. When the window closes, they find a rock to smash through the glass. It is a constant game of cat and mouse and requires defenders to refine their security and defensive measures as frequently as attackers find new ways to exploit them.

Figure 5: Percentage of Available Server Population Used in Max Attack Per Protocol



WISR SURVEY

While DDoS attacks evolve in size, volume, frequency, and complexity each year, attackers never stray from one bedrock principle: If it's important to network operators and enterprises, it's important to them.

These days, that translates to top targets such as customer-facing applications and cloud services. Adversaries can leverage a never-ending stream of vulnerable IoT devices in their attacks, and criminal activity such as extortion is a growing motivation. Meanwhile, there aren't enough White Hats to hire: service providers and enterprises report that they are defending against an increasing volume of complex threats while struggling to find qualified people to staff security teams. Small wonder that interest in outsourcing to Managed Security Service Providers (MSSP) is on the rise.

KEY FINDINGS

NETSCOUT's 15th annual Worldwide Infrastructure Security Report (WISR) delivers insights from a global survey of network, security, and IT decision makers across enterprise and service provider organizations. It focuses on the operational challenges they face daily from network-based threats and the strategies adopted to address and mitigate them.

1 Increasing Cloud Risk

Attacks on publicly exposed service infrastructure increased dramatically, reported by 51 percent of service providers in 2019 compared with only 38 percent the previous year. Considering the rapid rise of these attacks, it's no surprise that they are also a top 2020 concern for 55 percent of service providers.

2 From Hacktivists to Smooth Criminals

For many years, political issues, or hacktivism, was the top motivation for attacks. These days, however, adversaries are all about growing their cybercrime business: the top motivation in 2019 was criminal extortion, jumping from 5th place in 2018. Meanwhile, the second motivation was criminals demonstrating DDoS attack capabilities to potential customers. It's all about the marketing.

3 Outbound DDoS Attack Threat

While inbound DDoS attacks remained the top service provider threat, watch out for the increase in outbound/crossbound DDoS attacks from on-net customers and devices. Reported by 32 percent of respondents, this growing threat deserves more attention.

4 The Need for Outside Help

Enterprises are turning to MSSPs for security help, a likely reflection of the ongoing shortage of qualified security professionals. Service provider Security Operation Center (SOC) teams are also feeling the pressure, with 30 percent of service providers using third-party resources in some capacity. It also represents a promising market opportunity, as more than half of service providers reported increased interest in DDoS managed services from enterprise customers. This has led to an explosion in managed security services offerings, with DDoS and firewall services being most common among respondents.

SERVICE PROVIDER



Service Provider Threats and Concerns

Once again, DDoS attacks lead the list of threat concerns for service providers. However, the real story lies in the growing number of difficult-to-defend techniques being used. Thanks to IoT botnets, reflection/amplification techniques, and DDoS-for-hire services, attacks are more distributed, complex, and powerful than ever before. One growing threat that deserves more attention is that posed by outbound/crossbound DDoS attacks from on-net customers and devices—reported by 31 percent of respondents. Similarly, cloud risk has also risen. In a dramatic increase from the previous year, attacks on publicly exposed service infrastructure were reported by 51 percent of service providers in 2019 compared to only 38 percent in the previous year.

58%

Reported
multivector
attacks

65%

Say DDoS attacks
are top concern
for 2020

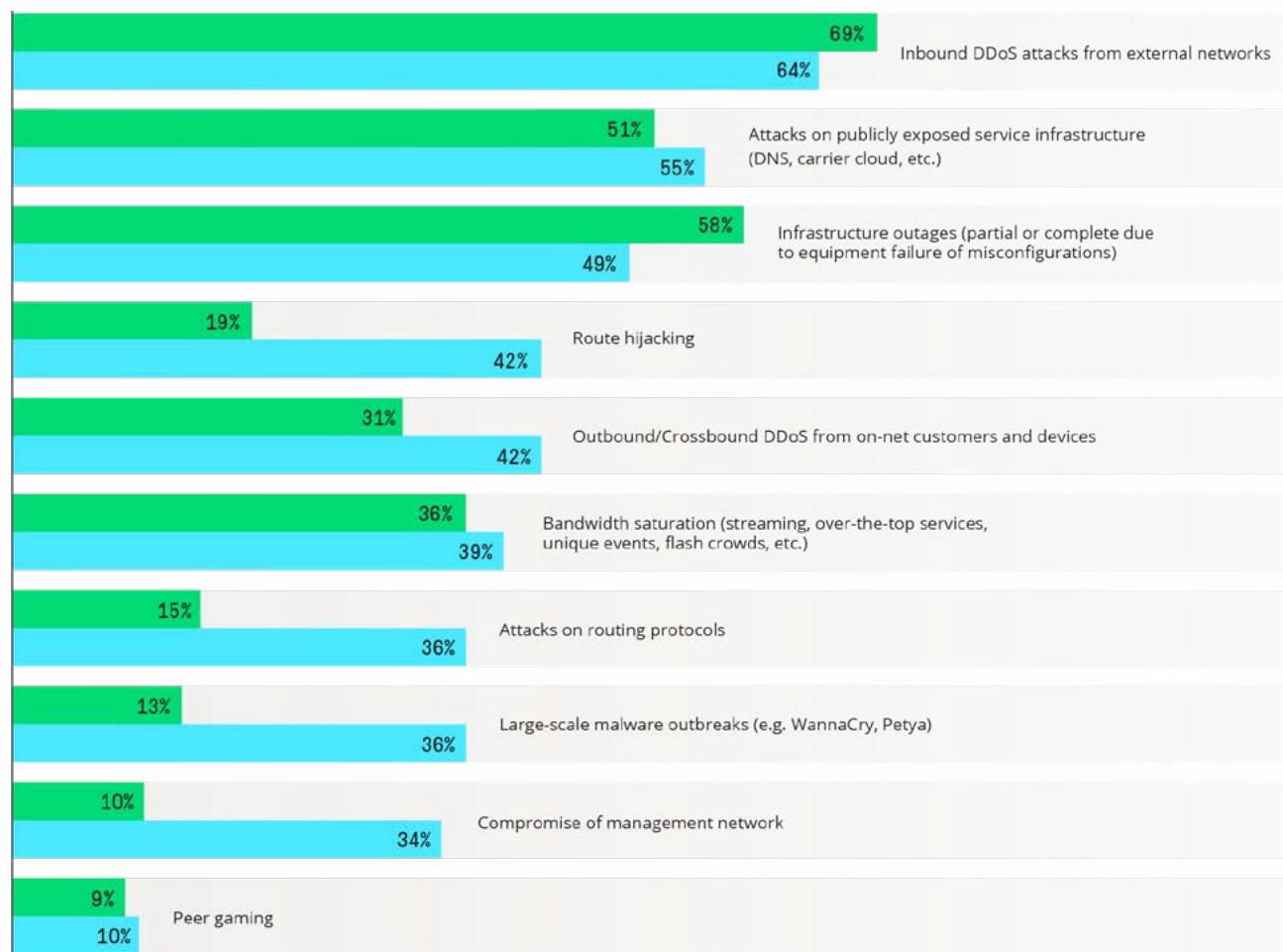


Figure 6: Service Provider Threats vs. Concerns

● Threat ● Concern

Follow the Money

DDoS truly is the people's attack in that it is available to anyone with an internet connection and bad intentions—making it the perfect building block for today's booming cybercrime economy. Attempts at criminal extortion top the list, while cybercriminals launching attacks to show off their capabilities comes in a close second. In a sense, many DDoS attacks are advertisements for illegal DDoS-for-hire services.

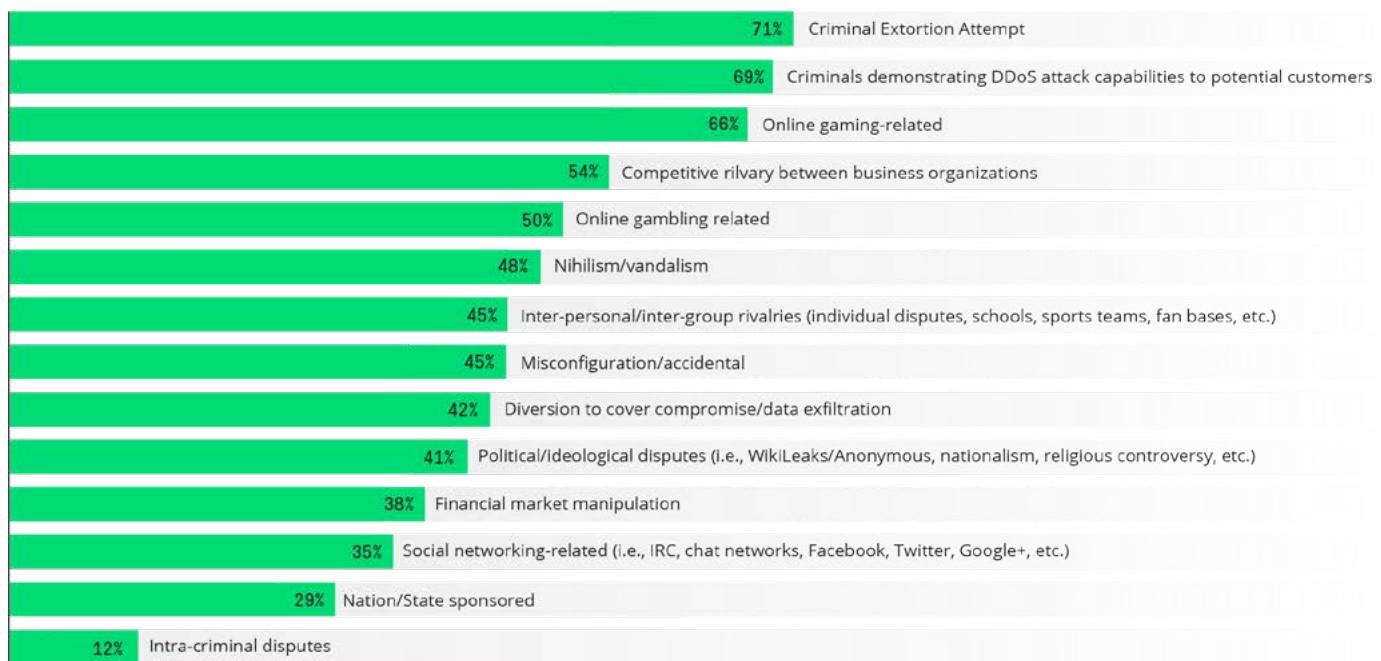


Figure 7: SP Attack Motivations

The People Problem

Finding qualified people continues to challenge service provider and enterprise security teams. The cybersecurity skills gap continues to be one of the most serious long-term issues facing network operators. It has been reported the gap is now four million open jobs!¹³

Nearly half of respondents blamed a lack of resources as an impediment to building a team, rising for the third consecutive year. Security practitioners are still in high demand and companies are spending to hire them, leading to churn throughout many organizations.

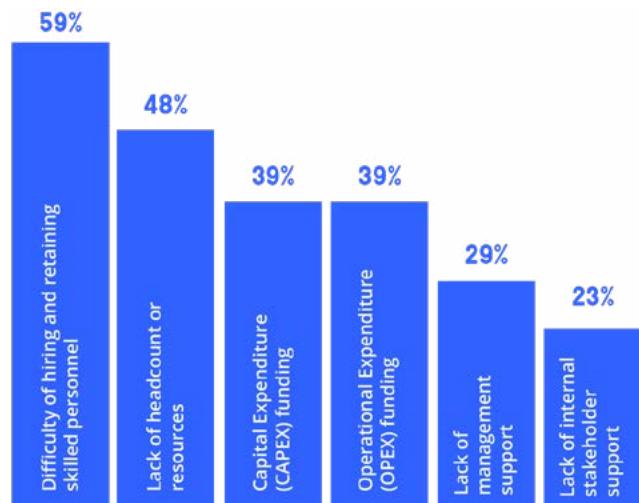


Figure 8: SP Operational Security Challenges

Interest Grows in Managed Security Services

The challenging hiring market has caused more enterprises to turn to service providers for security support, as more than half of service providers reported growing interest in DDoS managed services from customers. Cloud/hosting providers were the top vertical expressing interest, up from 5th place last year. As we predicted, this has led to an explosion in managed security services offerings.

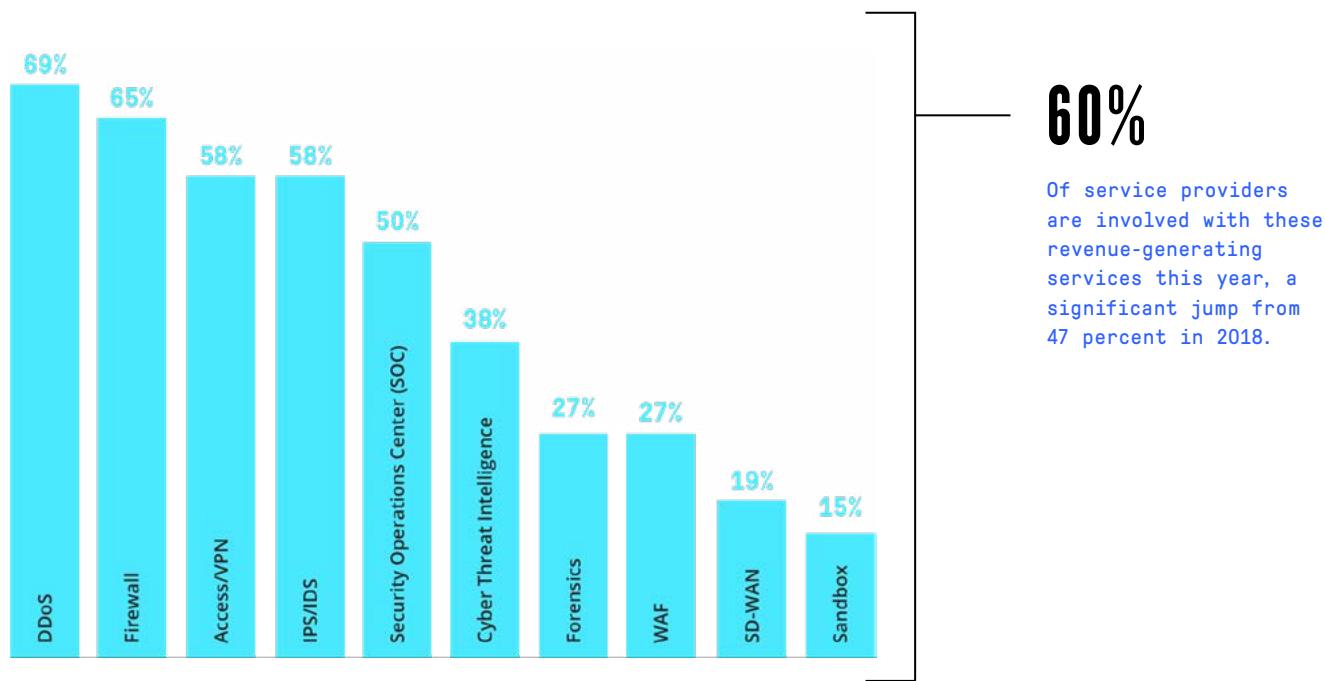


Figure 9: Managed Security Services

Service Provider SOCs

While enterprise teams reach out to service providers for outsourced support, service providers themselves are turning to third parties for some form of SOC capability, be it to fully outsource or augment existing teams with SOC capabilities. The people problem is so acute that even at companies where the network is the business, 42 percent either have no SOC at all, outsource completely, or use the hybrid model.

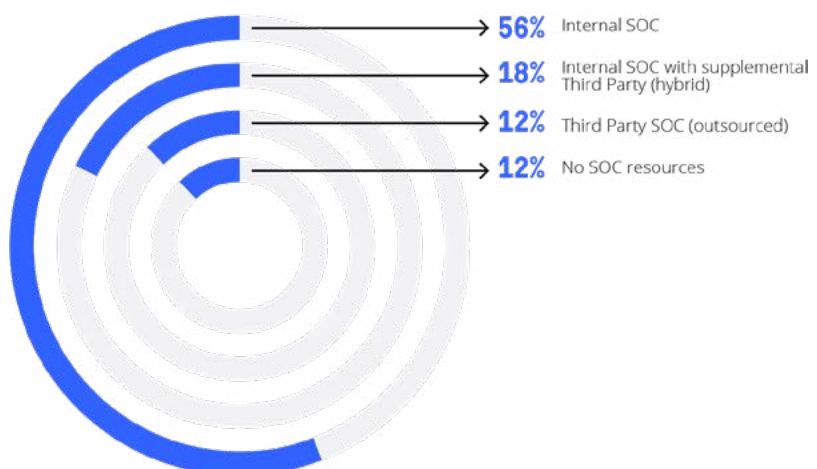


Figure 10: SP SOC Team Resources

ENTERPRISE

Enterprise Threats and Concerns

Just like service providers, enterprise security teams must defend increasingly complex, distributed multi-cloud environments. However, enterprises work with fewer people and resources, often within sectors with strict regulatory requirements. As a result, they are less concerned with types of attacks, and more concerned with self-protection. One of the biggest threats faced by enterprise network operators last year was Accidental Data Loss, and it remains the number-one concern for 2020. It is surely no coincidence that this is top of mind in light of new regulations such as GDPR and CCPA. After that, ransomware, malicious insiders, and DDoS attacks remain top priorities.

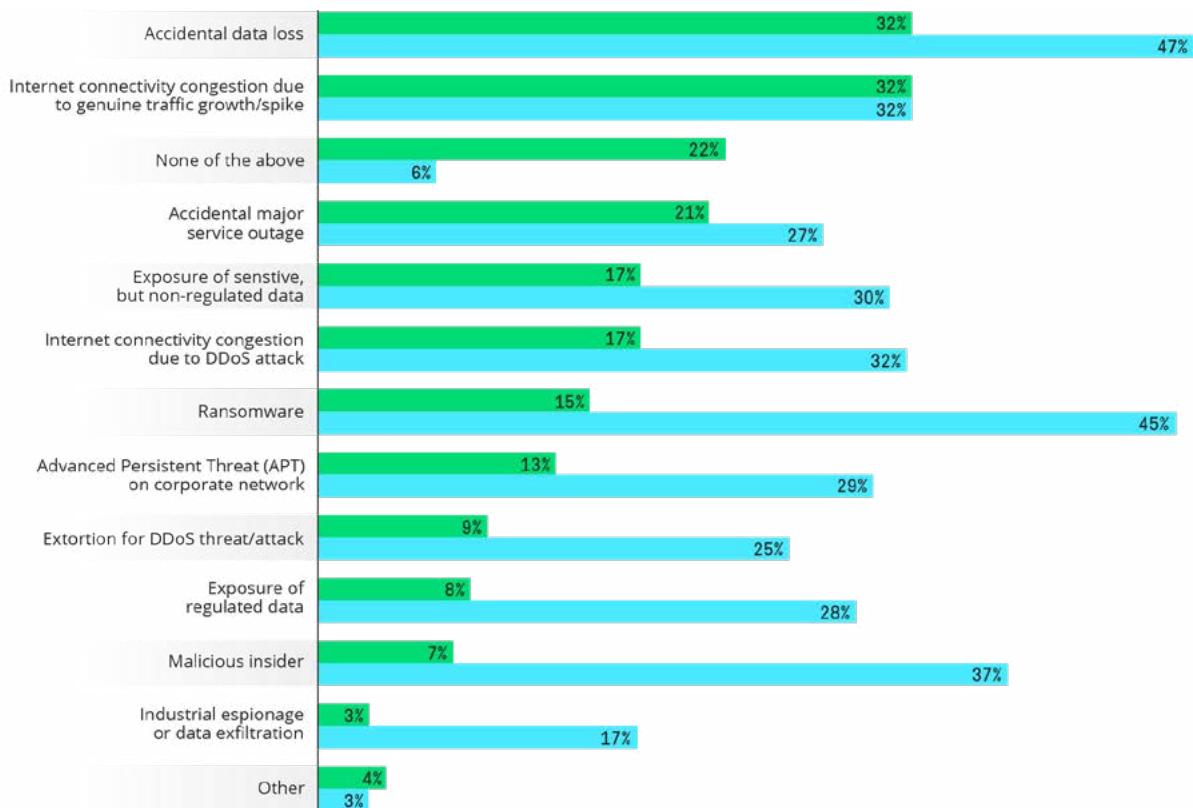


Figure 11: Enterprise Threats vs. Concerns

● Threat ● Concern

Top Services Targeted by Application Layer Attacks

While enterprise IT teams were struggling with cloud migration and application access, underground criminals were busy developing new attack tools of all types and using them as part of DDoS-for-hire services. Just as enterprise IT environments started sprawling across multiple cloud partners, attackers were ready with powerful new tools with a new target: layer 7 applications.

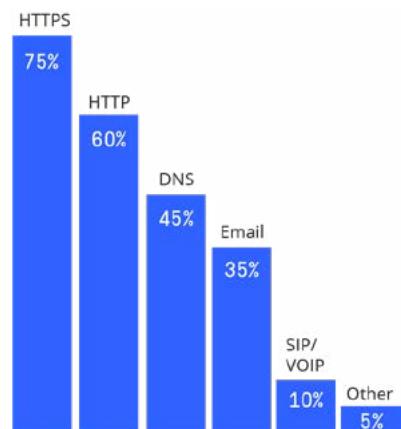


Figure 12: Top Services Targeted by Application Layer Attacks

Cloud, Customers Are Top Targets

Attacker focus on cloud-based service was also reflected in enterprise DDoS attack targets, where they took 3rd and 4th place. Top targets were equally concerning: Two thirds of enterprises indicated DDoS attacks targeted customer-facing services and applications, while just over half saw attacks targeting their infrastructure. In either case, these attacks directly affect the organization's ability to service customers, thus impacting revenue and profitability.

IoT

IoT devices have ushered in a new era of convenience and efficiency for businesses and consumers—while dramatically increasing the attack surface and risk profile of all organizations, including the [internet itself](#)¹⁴. IoT device manufacturers are focused on go-to-market strategies, not security. As a result, devices are being delivered with poor to non-existent security, for which patches are rarely made available. Once again, this year the WISR shows the impact this expanded threat surface is having on security defenses and the people behind them.

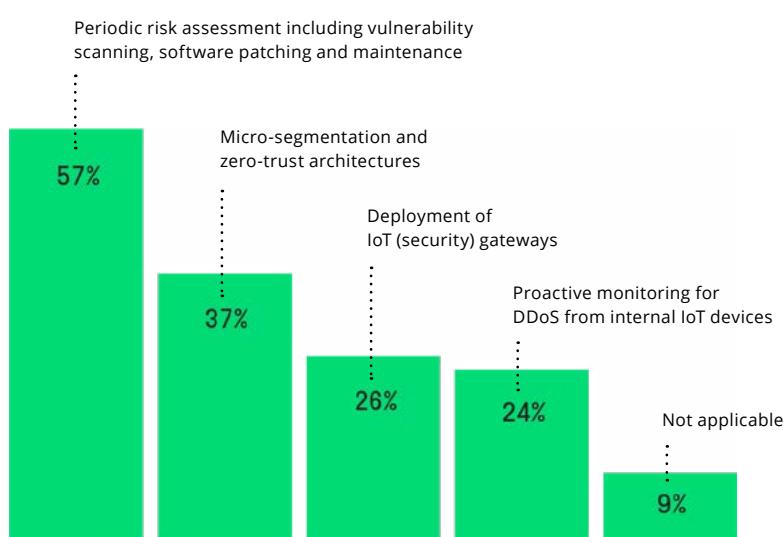
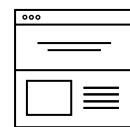
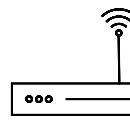


Figure 14: Enterprise IoT Security



66.7%

Customer-facing services and applications



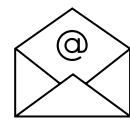
52.4%

Infrastructure (router, firewall)



14.3%

Third-party data center or cloud service



9.5%

SAAS services (VPN, email, transaction processing)

Figure 13: Enterprise DDoS Targets

The threats and challenges facing security teams are likely to be very similar next year. Attackers will continue to innovate and exploit. Finding quality people and staffing teams will continue to be a challenge.

With all that said, it does not mean that your specific organization cannot dramatically improve its security and risk posture in the coming year. There are so many things that can be done, from the very basics, like patching, to more advanced activities like deploying visibility without borders or practicing incident response drills.

Together, we're building a connected world. The complexity of it all, especially networks, mean that there will always be challenges. We hope that you find the information useful in protecting your business in the coming year.



IoT MALWARE

KEY FINDINGS

1

IoT: Botmaster's Dreams Come True

Botmasters eagerly await the 20.4 billion devices forecast to connect to the internet in 2020. This indefatigable group can choose from an ever-growing selection of malware strains that target a growing array of system architectures.

2

One Strain to Rule Them All

Mirai continued to dominate into the second half of 2019, with tens of thousands of unique versions of the malware circulating in the wild. Mirai-based variants increased by 57 percent from 2018, with nearly 103,000 unique samples seen in 2H 2019.

3

Honeypots Overflow

ASERT honeypots saw a 51 percent increase in the use of default/hardcoded administrative credentials and an 87 percent increase in the number of exploit attempts during the latter half of 2019.

▲ 87%

Increase in
exploit attempts

20.4B

Devices forecast to connect to the internet in 2020

▲ 57%

Increase in Mirai-based Variants from 2018

NOW SERVING

20400000001 DEVICES

Who knew smart doorbells and lightbulbs were on Santa's list? Nearly 60 percent of Americans were forecast to buy a smart home gadget during the holidays, and that's only one sector of the market.⁵

Everything from smart watches to tablets, thermostats, and even smart toys invaded homes around the world during the second half of 2019—a drop in the bucket compared with the millions of commercial devices that go online daily.

These devices range from educational to mission-critical, but to malicious botnet operators, they represent rich fodder for expanding their botnets. These botnets not only provide attackers with the means to steal user data, but they also allow the attackers to establish a launching platform for devastating DDoS attacks.

During the second half of 2019, we continued to see significant increases in IoT-based malware, largely made up of Mirai variants. Our partner ReversingLabs highlights the number of unique Mirai samples ingested over the course of the past year. (Figure 15) The graph in Figure 15 shows the continued increases of unique Mirai variants from 2017 to 2019. We also observed the uptick in Mirai variants via our IoT honeypot network.

Looking at the samples found in the wild for the past few years, it is evident that the trend is likely to continue (Figure 15).

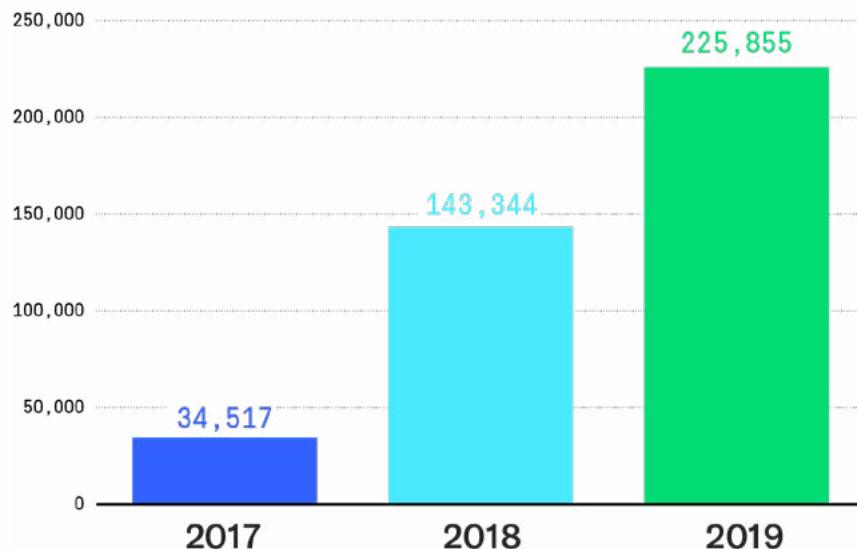


Figure 15: Mirai Sample Count

Of these Mirai variants, there is a broad dispersion of targeted system architectures as well. The following ReversingLabs data (Figure 16) shows a breakdown of the total count for Mirai samples and the operating system they targeted in 2019.

Architecture	Sample Count
ARM	67,165
MIPS	38,431
Intel 80386	26,180
PowerPC or Cisco 4500	19,723
SPARC	13,816
Motorola m68k	11,761
Renesas SH	11,702
ARC Core Tangent-A5	243
Xilinx MicroBlaze 32-bit RISC	82
ARM aarch64	82
Altera Nios II	43
Tensilica Xtensa	35
OpenRISC	33
unknown arch 0xc3 version 1 (SYSV)	23
UCB RISC-V	5
Version 1 (SYSV)	1

Figure 16: Mirai Samples and the Operating Systems They Targeted in 2019

Brute-forcing

▲ 51%

since the start of 2019

It is common knowledge that Mirai predominantly uses brute-forcing as the preferred method for compromising IoT devices, but we continue to see both brute-forcing and exploitation attempts increase (approximately 51 percent and 87 percent, respectively) since the start of 2019 (Figure 17). Because of their success, many of the same credential combinations and exploits from the first half of 2019 were also observed in the second half of the year.

Exploitation attempts

▲ 87%

since the start of 2019

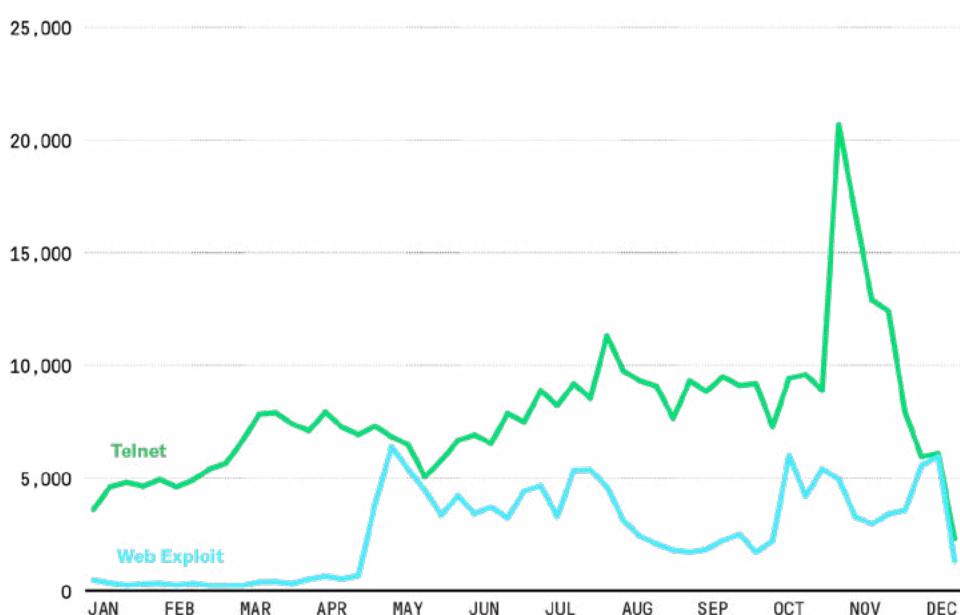


Figure 17: Telnet vs. Web Exploits for 2019

Figure 18 shows the top 10 Telnet usernames and passwords observed by our honeypot network for 2019.

1	guest/12345	106,950
2	root/xc3511	106,636
3	admin/admin	84,921
4	root/vizxv	78,756
5	root/root	71,419
6	support/support	69,720
7	root/admin	68,795
8	root/	67,760
9	guest/guest	68,817
10	root/Zte521	65,925

Figure 18: Top 10 Telnet Username and Password Combinations

Why do we still see these combos being used three years later?

There are two major reasons: they still work, and people are lazy.

- 1 Purging hard-coded administrative credentials requires a firmware update, a manual process that often daunts the typical owner of a DVR or an IP-based camera. Not surprisingly, consumers rarely go through the firmware upgrading process. In addition, we need to take into account shelf-life syndrome, in which devices become vulnerable while waiting to be purchased. Logically speaking, you can't apply updates to a product sitting on a shelf. Small wonder that these old combos still yield results.
- 2 Malware authors widely reuse code from the original Mirai source code, which was publicly leaked in September of 2016. Rather than starting from scratch, they leave the original credential combos and just append newly discovered credential combos to the password spray attacks used by Mirai. This is evident by the upward trend in the use of brute force password attacks observed in our honeypot network (Figure 17).

From late November through early December, we saw an unusual surge of login attempts. A quarter of the login attempts during this spike used the credentials of "root/xc3511." The majority of those connections originated from Brazil and China, likely indicating a push to expand already-established botnets.

Figure 18 should not surprise anyone, since these are the usual suspects when it comes to IoT username and password combos. We routinely see "root/xc38511" and "root/vizxw" hit our top 10 list. These combos are commonly found hardcoded on numerous DVR and IP-based cameras, and were included with the original Mirai botnet back in 2016.

Top 5 Credentials by Origin Country

CHINA

BRAZIL

TAIWAN

EGYPT

RUSSIA

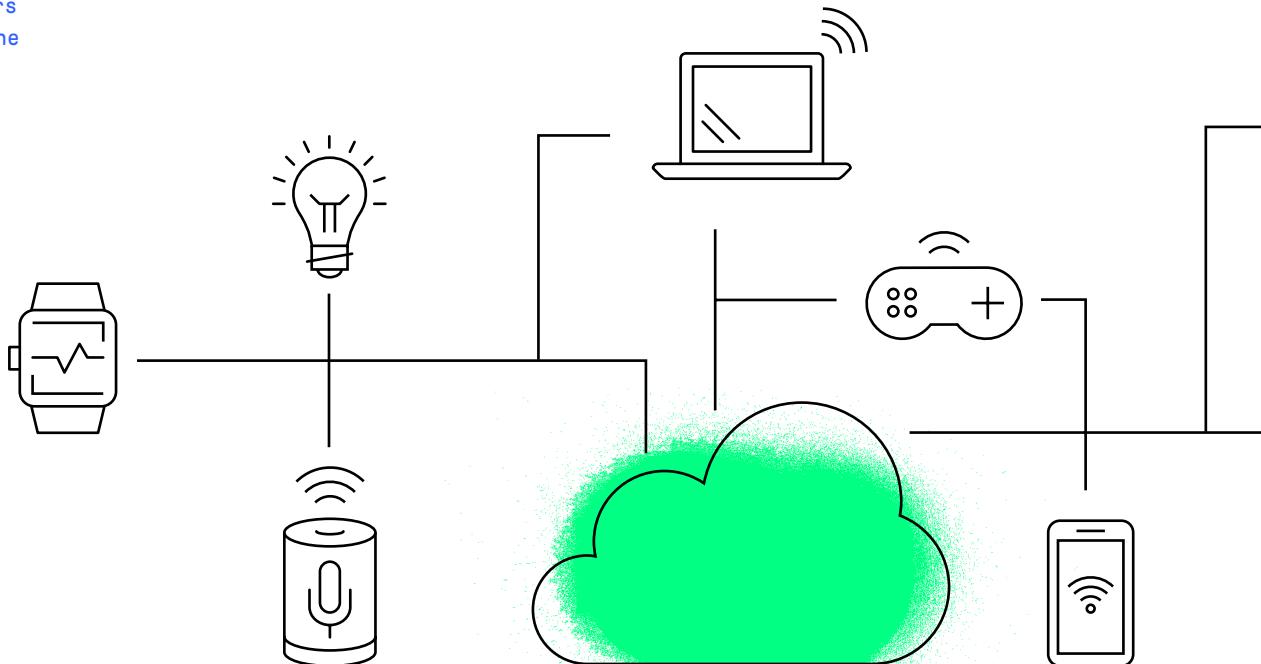
Compared to the second half of 2018, we see the same top five countries using the same top five credential combos, confirming the fact that it ain't broke, so attackers wisely stick to the same techniques.

Exploit Name	EDB-ID	Top Countries
Huawei Router HG532 Arbitrary Command Execution	43414	China Taiwan
Realtek SDK Miniigd UPnP SOAP Command Execution	37169	China Japan
Hadoop YARN ResourceManager Command Execution	45025	China United States
D-Link DSL OS Command Injection	44760	Egypt Italy
Linksys E-series Remote Code Execution	31683	China Italy

Figure 19: Top 5 IoT Exploits Attempts 2H 2019

Focusing on the second half of 2019 and breaking down the top five credential combos based on origin country, we find China, Brazil, Taiwan, Egypt, and Russia round off our top five countries. Compared with the second half of 2018, we see the same top five countries using the same top five credential combos, confirming the fact that it ain't broke, so attackers wisely stick to the same techniques.

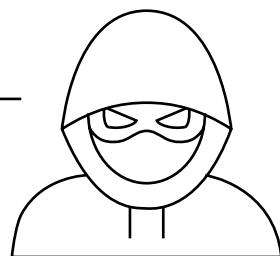
During the same time period we also saw a 51 percent increase in unique attempts that used default or hard-coded administrative credentials to deliver a Mirai variant. To augment the use of hard-coded administrative credentials, malware authors continue to leverage exploits to increase their bot numbers. In one such case, a recent version of ECHOBOT surfaced that now contains 71 exploits at its disposal. In our honeypot, we saw an 87 percent increase in the number of exploit attempts during the second half of 2019 (Figure 17). The top five IoT vulnerabilities are shown in Figure 19.



As we move into 2020, IoT malware numbers will continue to rise and their capabilities to expand, much as we've seen with ECHOBOT. Organizations and countries are beginning to fight back with standards such as OWASP Internet of Things Project⁶ and European Telecommunications Standards Institute specification TSS 103 645, as well as laws such as California's Senate Bill 327, which bans the use of default passwords in consumer IoT devices beginning in 2020.

But while these protections lead IoT security in the right direction, they do not apply to millions of legacy IoT devices. Moreover, several of the requirements are open to interpretation. With that in mind, we expect to see a continued rise in new exploits, older exploits, and hard-coded credentials used to grow IoT botnets in 2020. Mirai and its variants will retain dominance in the IoT malware landscape, although a handful of unique non-Mirai-based IoT malware will gain ground. Organizations must remain vigilant as the attack surface expands with more and more IoT devices entering the workplace.

Consumers must understand the very real threat posed by vulnerable devices and take proactive measures to ensure their home is protected against intrusions that would unknowingly make them complicit in DDoS attacks around the globe.



Top Exploits and Vulnerabilities

Figure 20 breaks down the percentages of exploits attempted per country for the top five vulnerabilities in the latter half of 2019.

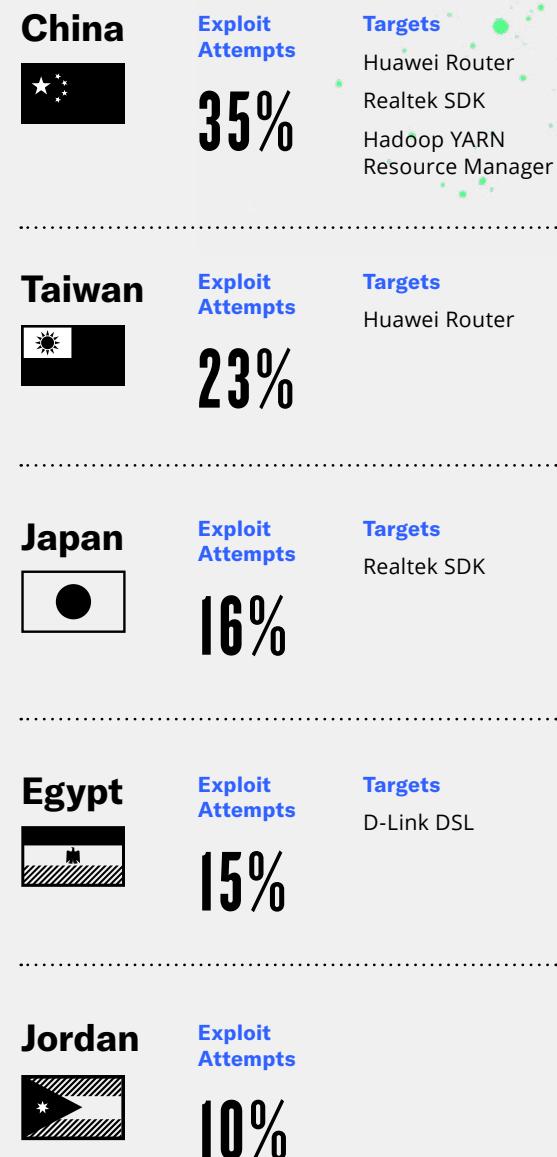


Figure 20: Top 5 Exploits and Vulnerabilities per Country

ADVANCED THREAT

WEAPONIZING MOBILITY

KEY FINDINGS

1 Tracking Dissent

APT adversaries increasingly include mobile malware as part of their toolkit, using it to infiltrate international targets as well as to monitor internal dissidents and protesters.

2 Mobile Malware: There's an App for That

APT groups that lack the domain knowledge and expertise to build their own malware need not despair: there are commercially available mobile malware solutions capable of monitoring targets.

3 Breathtaking Vulnerability

Only about half of mobile device users take any steps to protect their device, making it shockingly simple for APT groups deploy and use mobile malware.

Zero-day exploits, PowerShell scripts, highly customized malware, and deceptive social engineering techniques are just a few methods nations and state actors use to gain a foothold into target systems and networks.

However, many find that mobile malware adds an entirely new dimension to their toolbox. While not new, mobile malware essentially gives APT groups a window into the mind of the user. Mobile devices often contain invaluable personal and professional communications, sensitive documents, and other accesses into privileged environments. They can provide a glimpse into where a user has been and track current movements. In fact, mobile devices are increasingly the only computers that some people have, and yet only about half will take steps to protect them.⁷

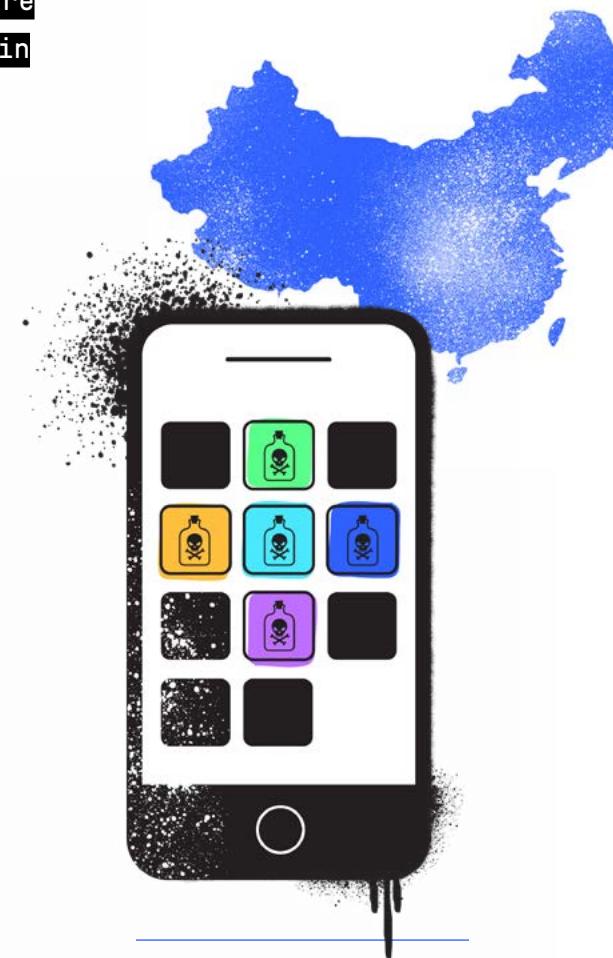
While APT groups target mobile devices for a variety of reasons, this report focuses on the motive ASERT observed the most in the past year: human rights abuse.

Targeting dissidents, journalists, activists, and expatriates to monitor activity and counter claims that threaten the governments are common targets for APT groups. While this targeting occurs worldwide, no one relies on the tactic more than authoritarian governments, often against their own people.

CHINA

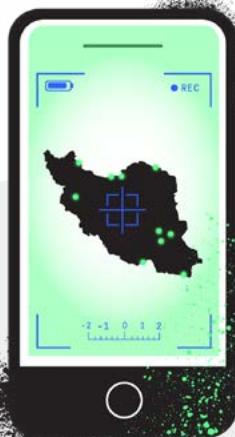
China uses APT groups to target the “Five Poisons”: The Muslim Uyghur population; Tibetan independence movement; Taiwanese independence movement; the Falun Gong religion; and Chinese democracy advocates, which includes the unrest in the city of Hong Kong.

These “poisons” are considered a threat to the homogenous culture, Marxist ideology, and the Chinese Communist Party’s legitimacy and control. Multiple organizations such as the Human Rights Watch⁸ and Amnesty International⁹ published documentation on the population-monitoring spyware, as have many infosec companies. POISONCARP¹⁰ was a one-click mobile exploit used against the Tibetan population. CallerSpy, another mobile malware threat, targeted the Uyghur population¹¹. Fake apps have appeared on the smart phones of Hong Kong protesters for years and recently, the Great DDoS Cannon surfaced again in an effort to thwart protest coordination.¹²



While often targeting the population directly, targeting of these “Poisons” often also includes investigative journalists, expatriate activists, human rights organizations, lawyers, and non-profits. Targeting poor, minority populations is not predicated on the assumption that those populations personally own mobile devices.

IRAN



Continual surveillance of the Iranian population and expatriates, especially during Iran's current internal unrest, showcases Iran's use of mobile monitoring tools.

The Iranian regime (both government and religious authorities) attempts to limit the influence of Western culture, Sunni or minority religions, and thoughts of democratic ideals. For example, recent published research highlighted how a group called Domestic Kitten built Android malware for an Iranian surveillance program¹³. This malware almost exclusively existed on Iranian phones, but could also be found on the phones of groups that threaten the stability of the Iranian regime. Often, mobile malware masquerades as a legitimate app or malware authors embed it in a repackaged app, such as GolfSpy,¹⁴ which they then advertise on social media for download. Similar APT surveillance malware called MobonoGram 2019 even made its way into the Google Play store for a period of time¹⁵. Leaked documents reportedly from Iran's Ministry of Intelligence appear to confirm both capability and intent, noting the existence of dedicated mobile malware teams, with the expressed purpose of tracking Iranians at home and abroad.¹⁶ When all else fails, Iran will simply block the entire internet.¹⁷

VIETNAM



Vietnam has a long history of using malware for surveillance of journalists, activists, and non-profits, with victims both outside and inside Vietnam's borders.¹⁸

ASERT analysis of recent campaigns found that a substantial number of victims reside inside Vietnam. The authoritarian Communist Party of Vietnam completely restricts the rights and accesses of its own people, with severe consequences for dissent.¹⁹ Internationally criticized cybersecurity laws that went into effect in 2019 both dismantle privacy and further repress the country's own people.

Vietnam's malware is unique in that the country developed desktop and mobile versions alongside one another, with the intent to use both simultaneously.²⁰ In its recent campaign, OPERATION OCEANMOBILE, researchers found multiple fake Android apps that were really surveillance malware.²¹ The apps were sent to specific, targeted individuals via phishing, and were also available in the official Google Play store, complete with business back stories, privacy policies, and even a GitHub repository.

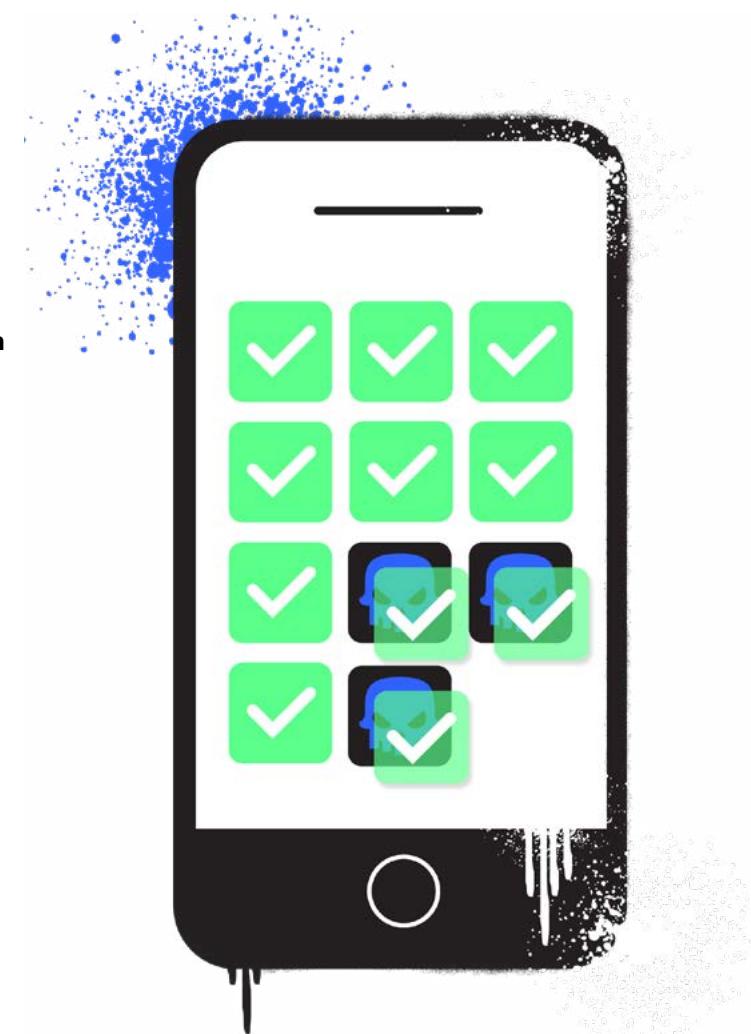
MOBILE ESPIONAGE FOR HIRE

Not every nation has the time or expertise to build mobile surveillance malware from scratch—but don't worry, there's an app for that. There are several malware purveyors willing to pretend that what they sell will be used only for law enforcement purposes. Luckily, one group executed its surveillance campaign with terrible OPSEC,²² giving us a window into the world of commercial mobile malware.

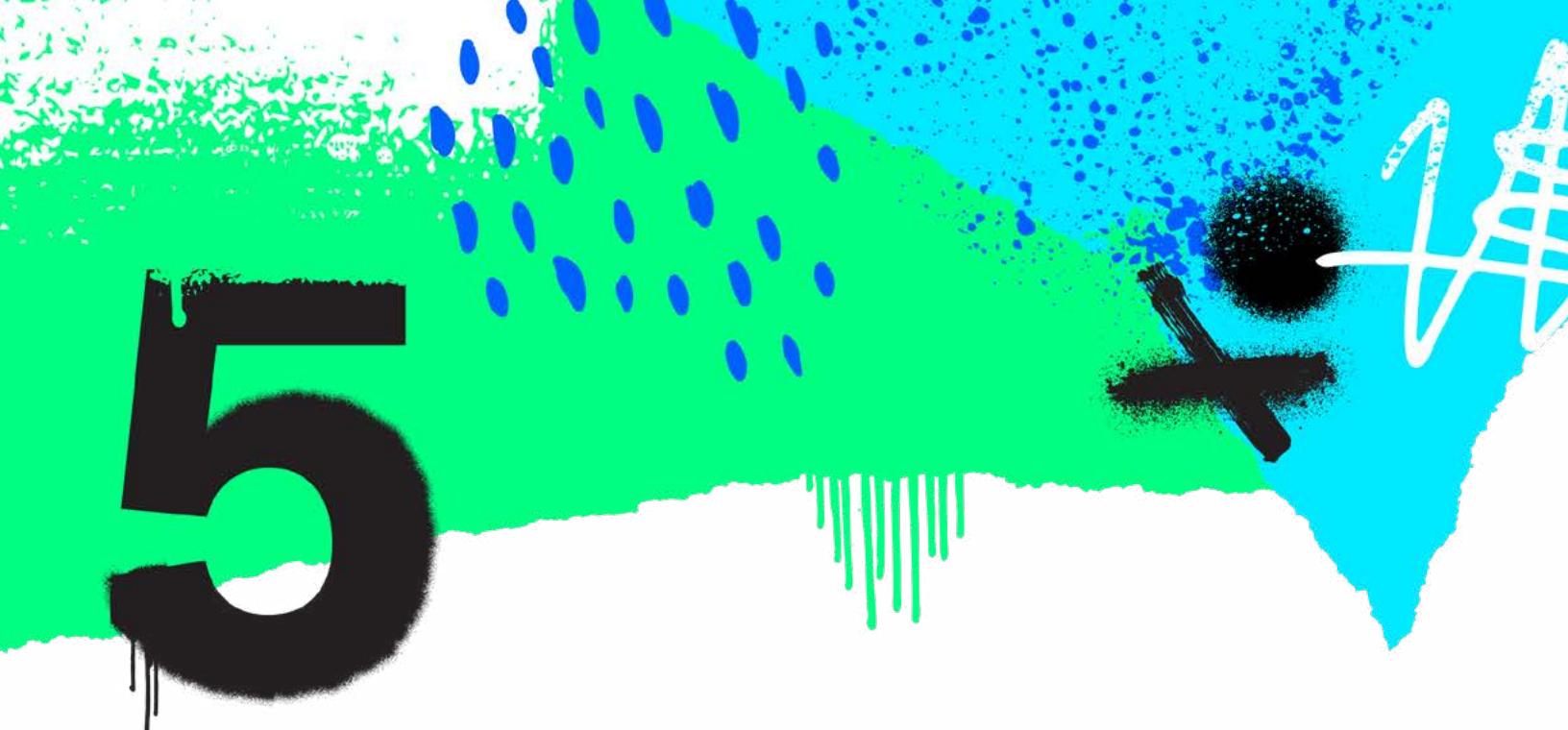
Appearing benign, the FinFisher/FinSpy mobile app has a history of targeting individuals in the March for Justice movement in Turkey²³, as well as others across the globe.²⁴ Updated versions are more advanced with support for iOS in addition to Android.²⁵ Pegasus is another mobile monitoring malware that, once installed, can access calls, messages, emails, and files, and even operate the microphone and camera. Evidence points to this malware targeting dissidents²⁶ in the Middle East²⁷ and elsewhere. Related, the newer Chrysaor²⁸ is an Android spyware tool that can track the victims' location.

Mobile malware is quickly evolving from a supplemental role supporting desktop malware to a stand-alone solution often capable of obtaining information in real time. While we chose to focus on human rights targeting, the use of mobile malware for intelligence espionage, intellectual property theft, and financial crimes appears to accelerate at similar rates. Regardless of the type of organization, ignoring the risks posed by mobile devices leaves security professionals in a blind spot, with potentially disastrous consequences.

Mobile malware is quickly evolving from a supplemental role supporting desktop malware to a stand-alone solution often capable of obtaining information in real time.



5



KEY FINDINGS

1

Defend at the Source

ASERT data shows that blocking threats closer to the origination of an infection vector prevents follow-on infections and secondary payloads.

2

More Samples = More Victims

Emotet saw a significant increase not only in the number of samples circulating in the wild, but also in the number of victims impacted.

3

Black Hats Never Rest

Attackers innovate and evade detection via constant tweaks and updates to Emotet—a strategy that earns them the ultimate prize of more victims.

CRIMEWARE

DEEP DIVE: EMOTET

How profitable is cybercrime? If it were a country, cybercrime would have the 13th highest GDP in the world, with large multi-national operations earning more than US\$1 billion annually.²⁹

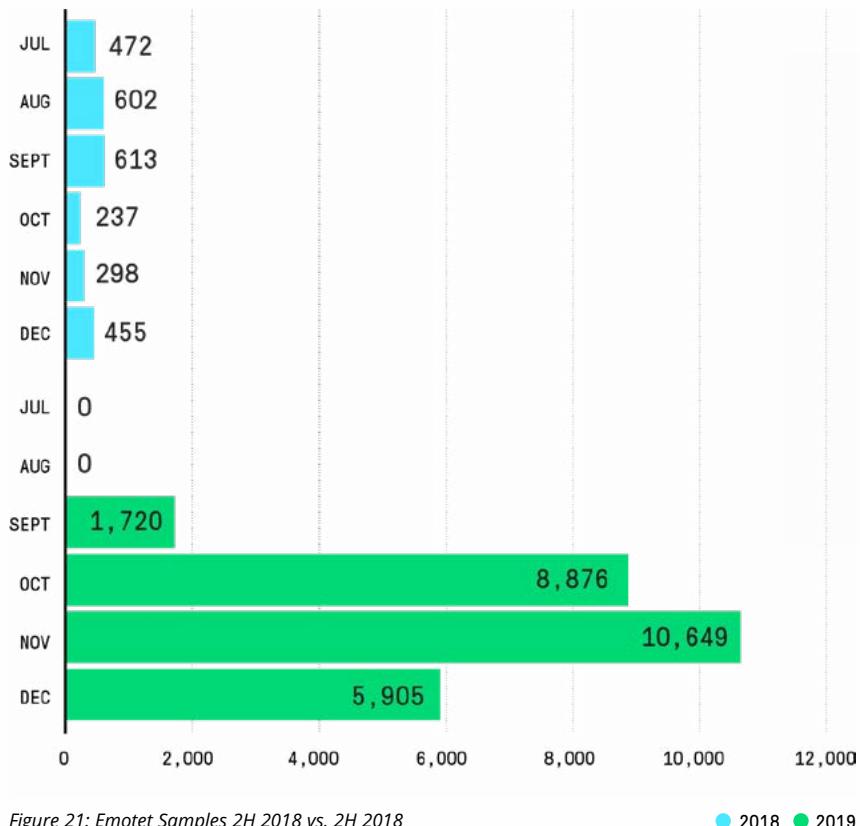
This gives cybercriminals plenty of motivation to release a constant onslaught of spam distribution, phishing, global botnets, ransomware, and many other forms of malicious malware. These threats loom over not just the business world, but nearly every household in the world.

How do you protect yourself? Start as close to the source as possible. While we see a lot of spam messages, our primary focus has been on downloaders and installers such as Emotet, Andromeda, and Pony—three of the more notorious download families. Once upon a time, Upatre also fell into that same category, but largely it delivers pharma messages rather than more insidious threats like Trickbot or a dozen different varieties of ransomware.

EMOTET

A closer look at one of those downloaders—Emotet—has uncovered useful metrics from the second half of 2019 that showcase observed activity and the trends we see in the threat landscape.

After a brief four-month hiatus, September saw Emotet surge back into action with a vengeance. Comparing the monthly binaries year over year, September 2019 saw an increase that rivaled almost all the samples we saw combined for the second half of 2018 (Figure 21). The drastic increase in unique compiled binaries aligns to the increase in alerts we saw from our sensors. Throughout the second half of 2019, we observed approximately 300,000 notifications of Emotet command and control (C2) traffic, about 100,000 more victim alerts than were seen during the same time period in 2018. This doesn't indicate unique infections, but rather persistent communications spanning variable time frames. Of the 300,000 alerts, we saw over 1,000 unique IP addresses communicating to these C2 servers.



Throughout the second half of 2019, we observed approximately 300,000 notifications of Emotet command and control (C2) traffic, about 100,000 more victim alerts than were seen during the same time period in 2018.

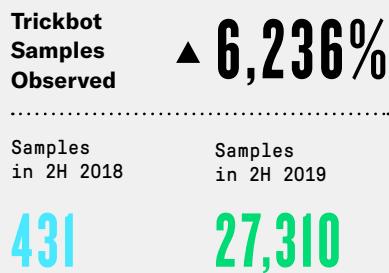


Emotet Samples Observed	▲ 913%
Samples in 2H 2018	2,681
Samples in 2H 2019	27,150



TRICKBOT

Tracking TrickBot, a second-stage payload associated with Emotet³⁰, yields data that illustrates why we tend to focus more on the downloaders themselves. The goal is to prevent follow-on infections, such as Emotet downloading TrickBot. The data shows that while we saw an equal number of TrickBot samples, there were significantly fewer infections based on alerts from our customer base:



In this same time period, we observed approximately 50,000 alerts for TrickBot C2s against our customers. This is a significant decrease compared with the more than 300,000 alerts seen with Emotet. (It should be noted that alerts do not necessarily annotate uniquely, because one infection can generate many alerts.)

The following charts displays the geographic dispersion of both victims and attacker-controlled C2 infrastructure for Emotet over the second half of 2019.

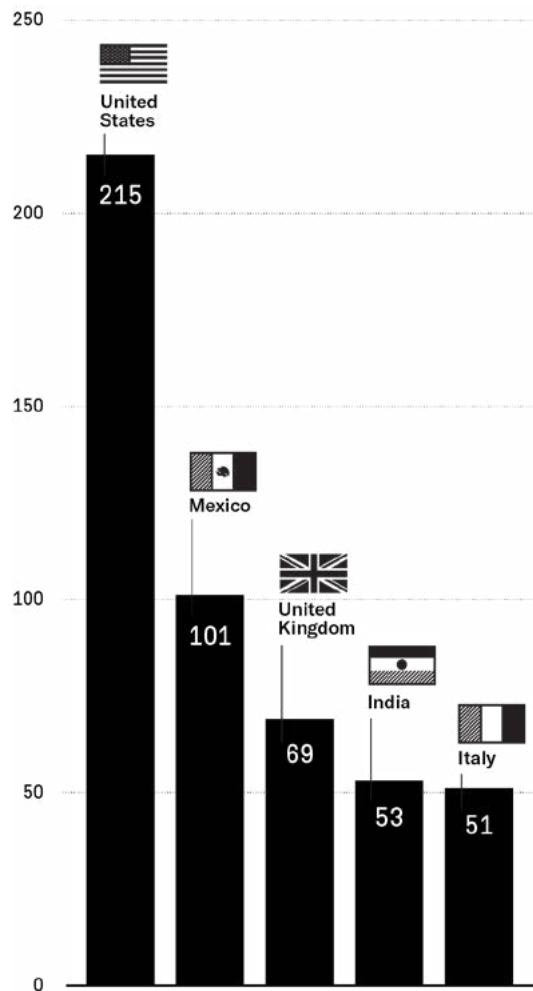


Figure 22: Top Victims by Country

These alerts are spread out over three campaigns, or what are now being called epochs. Each epoch follows a set time for updates and C2 infrastructure, as well as unique RSA keys used in communications.

As part of our analysis of these campaigns, we tracked the number of unique compiled binaries. Clearly, adversaries significantly ramped up operations, since the number of samples skyrocketed between September 2019 and November 2019. In fact, a [Spamhaus report³¹](#) shows a sharp increase in email distribution for Emotet, which coincides with the marked increase we observed for Epoch 2.

250

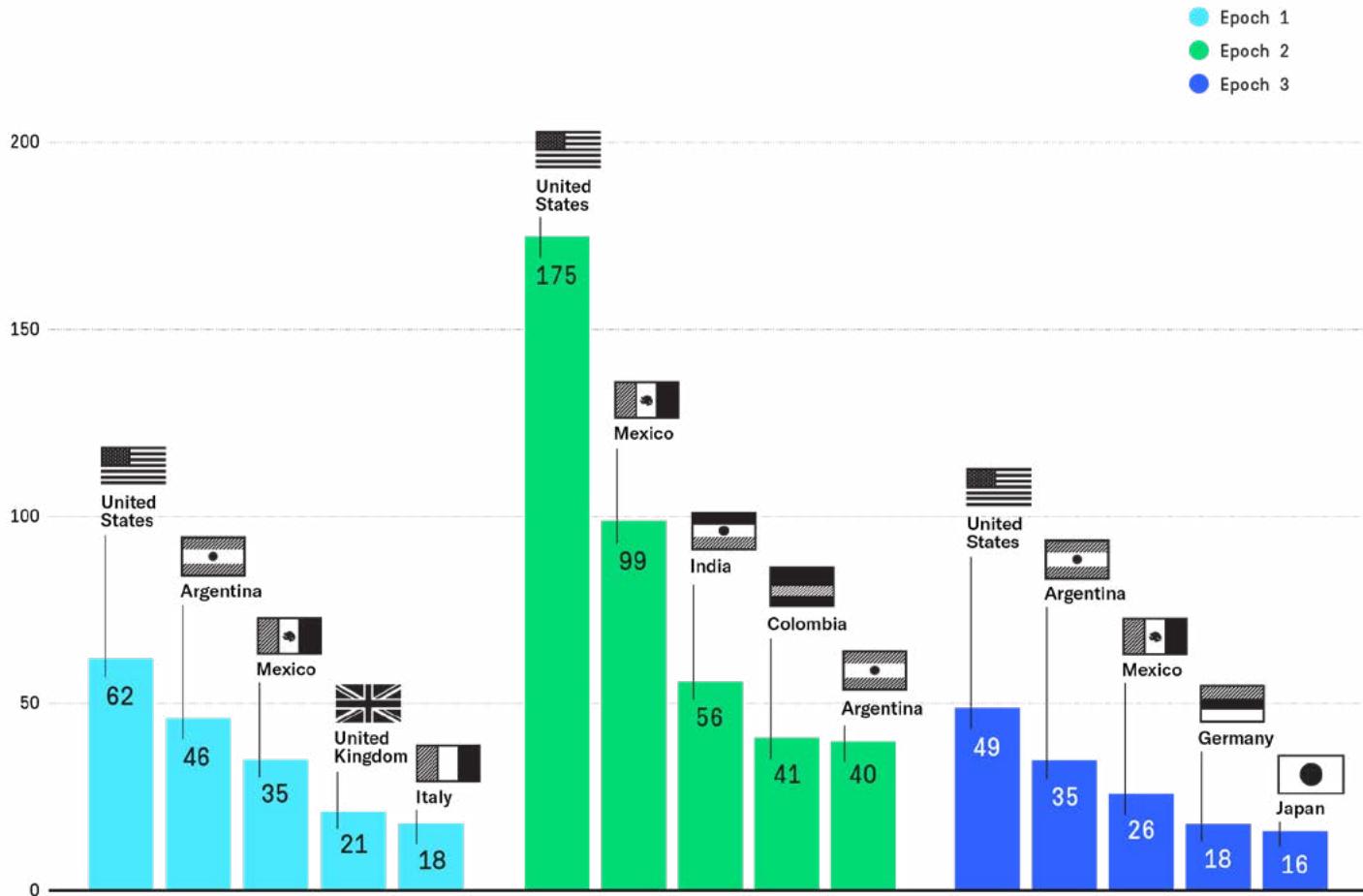


Figure 23: Top Attackers in Epoch 1-3 by Country

Activity observed firsthand, as well as that of the community, highlights the need to continue tracking these downloaders to ensure that we block threats before they reach their final stage, such as TrickBot or some flavor of ransomware. Ideally, one would focus on spam messaging as a first course of action, but should that fail, targeting the initial state of the infection and where the attackers gain a foothold, should be step two. Downloaders play an important role in the attack lifecycle for crimeware and remain a critical target for defenders to mitigate.

CONCLUSION

The overall threat landscape only knows one direction: up. Cybercrime is a multi-billion-dollar business, while nation-state groups proliferate globally and with increasing impact.

Meanwhile, cyber attackers always seem one step ahead of the game, targeting not only enterprises and service providers, but also their customers. Key digital transformation technology such as cloud services and mobile networks and devices have become prime targets. Sadly, the ongoing deluge of vulnerable IoT devices brings tears of joy to botmasters wielding an ever-growing selection of malware strains. These adversaries are smart and motivated, and we can count on them to continually discover and weaponize new vectors or add techniques onto existing ones.

But that does not mean that your specific organization cannot dramatically improve its security and risk posture in the coming year. There are so many things that can be done—from the very basics, such as patching, to taking the time to understand your own network architecture and traffic flows during peace time. Things like regular attack mitigation drills or using automated DDoS detection and mitigation tools can help you quickly respond and defend against DDoS attacks.

Together, we're building a connected, amazing world. The growing global complexity of it all means that there will always be challenges. The ASERT team continues to monitor the threat landscape and report on new discoveries, from malware under development to the increasingly sophisticated tools and techniques used. We hope that you find the information useful in protecting your business over the coming year.

APPENDIX

¹ verizon.com/about/our-company/5g/internet-things-will-thrive-5g-technology

² digitaltrends.com/gaming/world-of-warcraft-classic-ddos-attacker-arrested/

³ infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops/

⁴ netscout.com/blog/mirais-botnet-tsunami

⁵ businessnewsdaily.com/15315-holiday-tech-spending.html

⁶ owasp.org/www-project-internet-of-things/

⁷ media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083912/4114_B2C_Report_2017_WEB.pdf

⁸ hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

⁹ amnesty.org/en/press-releases/2019/04/state-sponsored-cyber-attack-hong-kong/

¹⁰ citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/

¹¹ blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-distributed-through-callerspy-mounts-initial-phase-of-a-targeted-attack/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29

¹² bleepingcomputer.com/news/security/the-great-cannon-ddos-tool-used-against-hong-kong-protestors-forum/

¹³ virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Kayal-Finkelstein.pdf

¹⁴ blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

¹⁵ symantec.com/blogs/threat-intelligence/unofficial-telegram-app-malicious-sites

¹⁶ clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf

¹⁷ theregister.co.uk/2019/11/19/iran_kills_internet/

¹⁸ welivesecurity.com/2014/01/20/vietnamese-malware-single-post-enough-to-trigger-spyware-attacks-against-u-s-bloggers-eff-claims/

¹⁹ hrw.org/world-report/2019/country-chapters/vietnam

²⁰ antiy.net/p/analysis-of-the-attack-of-mobile-devices-by-oceanlotus/

²¹ blackberry.com/uk/en/forms/enterprise/mobile-malware-report

²² cyberscoop.com/mobile-zero-days-lookout-shmoocn-2019-android-barracuda-ios-stonefish/

²³ accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf

²⁴ citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

²⁵ securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/

²⁶ citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

²⁷ amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/

²⁸ blog.checkpoint.com/2017/04/06/latest-findings-chrysaor-pegasus-android-even-stealthy/

²⁹ [darkreading.com/vulnerabilities---threats/cybercrime-economy-generates-\\$15-trillion-a-year/d/d-id/1331613](http://darkreading.com/vulnerabilities---threats/cybercrime-economy-generates-$15-trillion-a-year/d/d-id/1331613)

³⁰ threatpost.com/un-weathers-emotet-trickbot-malware/151894/

³¹ spamhaus.org/news/article/791/estimating-emotets-size-and-reach

ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate, and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability, and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

© 2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. All other brands and product names and registered and unregistered trademarks are the sole property of their respective owners.