NETSCOUT THREAT INTELLIGENCE REPORT

Powered by ATLAS

—

Findings from First Half 2018

NETSCOUT®

TABLE OF CONTENTS

LETTER FROM NETSCOUT THREAT INTELLIGENCE

HARDIK MODI *Senior Director, NETSCOUT Threat Intelligence*

—

The global cyber threat landscape continues to evolve, unleashing increasingly sophisticated and persistent attack techniques at internet scale.

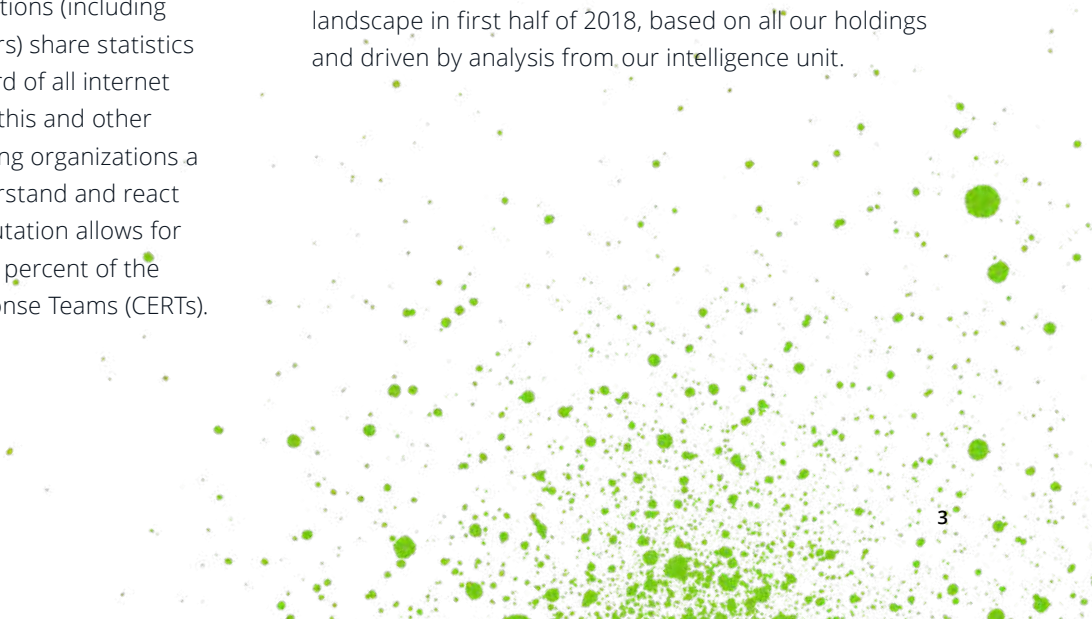
Today, attackers can release enormous terabit-per second-scale DDoS attacks. They routinely harness hundreds of thousands of Internet of Things (IoT) devices to launch attacks against specific targets that may be oceans and continents away. Further, state sponsored Advanced Persistent Threat (APT) groups representing a broad range of nation-states are seen as impactful, while traditional crimeware activity continues to proliferate.

NETSCOUT Arbor has actively monitored this space since 2007, when the company launched its Active Threat Level Analysis System (ATLAS®), which collects, analyzes, prioritizes, and disseminates data on emerging threats to enable the generation of actionable intelligence for consumption by people and systems alike.

Through telemetry on a massive scale, ATLAS delivers unparalleled visibility into the backbone networks at the core of the internet. Organizations (including 90 percent of Tier 1 service providers) share statistics representing approximately one-third of all internet traffic. NETSCOUT Arbor correlates this and other data sets to provide intelligence giving organizations a broader perspective to better understand and react to the threats they face. ATLAS' reputation allows for collaboration sharing with nearly 70 percent of the world's Computer Emergency Response Teams (CERTs).

ATLAS' internet-scale visibility is further enhanced by analysis from our ASERT (the ATLAS Security and Engineering Research Team). For more than a decade, ASERT's world-class security researchers and analysts have been building the tools and front-line database to analyze malware at internet scale. The security intelligence professionals within ASERT are part of a group of experts that are referred to as 'super remediators' and represent the best in information security practices and threat intelligence.

By using ATLAS' internet-scale visibility conjunction with more tactical holdings such as automated malware analysis pipelines, sinkholes, scanners, honeypots, and supplemented by open-source intelligence data sets and ASERT analysis, we can provide a unique view into the threat landscape, demonstrated by a steady stream of discoveries. This report represents our view of the threat landscape in first half of 2018, based on all our holdings and driven by analysis from our intelligence unit.



EXECUTIVE SUMMARY

2.8 MILLION

ATTACKS IN THE FIRST HALF OF 2018

SINCE MEMCACHED APPEARED, AVERAGE ATTACK SIZE HAS INCREASED

37%

INCREASE IN ATTACKS GREATER THAN 300 GBPS

7 ▶ **47**

IN 1H 2017 IN 1H 2018

DDoS attacks have never been more, innovative, dynamic or consequential.

The symbiotic nature of the digitally transformed world also adds vulnerability as malicious actors, nation states, criminal organizations, or even individuals can capitalize on the interdependencies that wind through our pervasively connected world.

Distributed Denial of Service (DDoS) attacks—where attackers seek to take down a website, application, or infrastructure by flooding it with requests—are a foundational element of much of this activity, and we saw about 2.8 million attacks in the first half of 2018. Moreover, the attack peak sizes have skyrocketed, as the Memcached-based attacks that started in Feb 2018 ushered in the terabit era of attacks. The size of attacks has increased to 47 attacks over 300 Gbps in the first half of 2018, compared with 7 in the same time period of 2017. DDoS attacks have never been more innovative, dynamic, or consequential, and there could be even more dangerous DDoS attacks on the horizon.

SO, WHAT CHANGED?

There has been increased innovation in DDoS attack tools and techniques. The availability of such improved tools has lowered the barrier of entry, making it easier for a broader spectrum of attackers to launch a DDoS attack. Attack targets have also diversified. It used to be that certain verticals were likely targets for a DDoS attack, with finance, gaming, and e-commerce atop the list. Today, any organization, for any real or perceived offense or affiliation, can become a target of a DDoS attack.

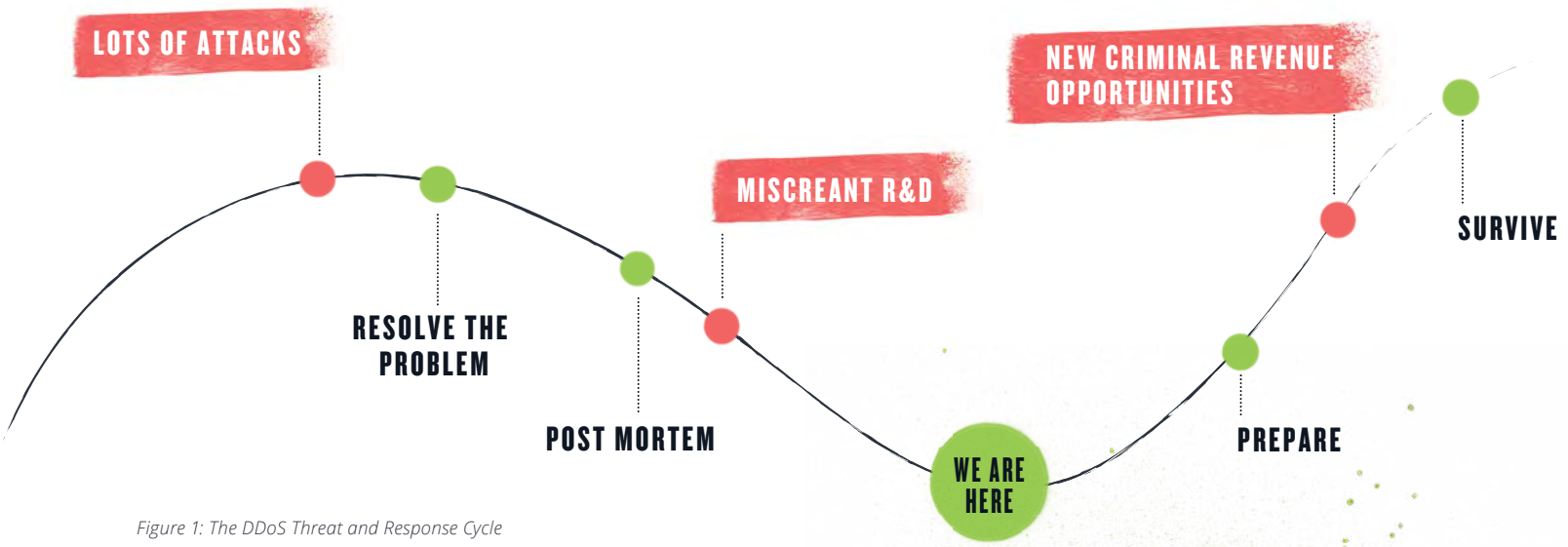


Figure 1: The DDoS Threat and Response Cycle

The scale of DDoS threats has also grown. Instead of targeted intrusions based on custom frameworks and crafted malware, DDoS activity now often involves hundreds of thousands—or even millions—of victims who largely serve to amplify the attack or end up as collateral damage, as indicated by the SSDP diffraction attacks that originated in 2015 and resurfaced this year.

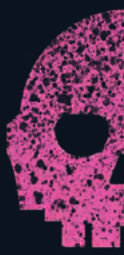
While DDoS threats have enormous size and scale, activity from cyber criminals and nation-state espionage groups pose threats as well. Over the past 18 months, internet worms, supply chain attacks, and customer premises equipment (CPE)/IoT compromises have opened up internet-scale threat activity. Nation-state APT groups continue to develop globally, used as another means of state-craft and often targeting governments and institutions of geo-strategic relevance. Of particular interest to us are the observations of internet-scale activity in the strategic sphere, where campaigns such as NotPetya, CCleaner, VPNFilter, etc., involved broad proliferation across the internet, even as the ultimate targets were highly selective. These are distinct from the targeted attacks enterprises have become accustomed to dealing with over time, which often involve direct spear-phishing and limited scope to avoid detection and maintain presence. In this respect, targeted campaigns can now be backed by internet-scale intrusions.

As threats grow across the landscape, NETSCOUT Arbor's unique position protecting enterprise networks and the internet through our service provider customers gives us wide visibility into this dynamic and ever-changing environment. By drawing on that comprehensive view in conjunction with analysis from NETSCOUT Threat Intelligence, we have created a representative view of the threat landscape based on all our holdings and driven by extensive research and analysis.

NETSCOUT Threat Intelligence has created a representative view of the threat landscape based on all our holdings and driven by extensive research and analysis.

DDoS ATTACK TRENDS

The DDoS landscape is driven by a range of actors, from malware authors to opportunistic entities offering services for hire. They are a busy group, constantly developing new technologies and enabling new services while utilizing known vulnerabilities, pre-existing botnets, and well-understood attack techniques.



This leads to a somewhat cyclical rate of incidence, but that does not mean the underlying dynamics aren't changing. DDoS attackers are persistent and innovative, and they constantly evolve their technology. Sometimes they add new malware modules onto existing technology, as in the case of Mirai. Other times, a new vulnerability is spotted or rapidly utilized that opens up an entirely new line of attack, as in the massive Memcached attacks this year. Inclusion of 0-day and use-after-free vulnerabilities increase the efficacy of DDoS attacks and propagation, fueling the spread of botnets that serve future attacks.

All of this adds up to an overall rising line of risk over time. So, while there is currently a relative lull when it comes to the use of new attack vectors, attack vectors are under development, as our ASERT team monitors and identifies these groups conducting live field tests of malware under development. The IoT Reaper campaign that was live for two weeks in October 2017 is one example.[1] Meanwhile, the attackers continue evolving existing malware. For example, Mirai continues to beget variants, many with new capabilities, including exposing intrusion capabilities. This builds on our previous findings presented at DEF CON 25 on Windows variants of Mirai, which could extend the botnet inside the enterprise to be used for internal propagation and disruption or internal DDoS, which none of us are prepared for.[2,3]

Like any cybersecurity sector, dealing with DDoS is like trying to battle the many-headed Hydra of Greek mythology, as adding a new module or piece of malware is akin to adding another head to the beast. Even worse, the old heads never fully go away. Look at SSDP, for example: This is a well-worn protocol for reflection/amplification abuse that does not belong on the internet. And yet, we continue to see deployments. Vulnerable SSDP deployments are being exploited to launch attacks that fool naïve defense techniques. Further, we have demonstrated that there's a broad class of devices whose implementations can be exploited to achieve an intrusion.

Then there's Memcached, which was used to launch the largest DDoS attack to date, a 1.7 Tbps DDoS attack disclosed by NETSCOUT Arbor in March of 2018. This attack vector was weaponized by the Booter/Stresser community mere days after its emergence in the public domain and is a major factor in the surge of large DDoS attack sizes since.

FROM FIRST HALF 2017 TO FIRST HALF 2018...

GLOBAL MAX DDOS ATTACK SIZE INCREASED

▲ 174%

GLOBAL FREQUENCY DECLINED

▼ 13%

FIRST HALF 2018 DDoS ATTACK TRENDS

Comparing first half (January to June) 2017 to 2018, we saw a drop in attack frequency accompanied by a dramatic increase in attack size and scale. However, while the first half of 2018 saw fewer attacks than the same time period of 2017, it doesn't mean that DDoS attacks are abating. The max attack size has leaped up with a small drop in frequency of attacks. While smaller DDoS attack sizes still predominate, there has a significant increase in the size of attacks greater than 300 Gbps in 1H 2018.

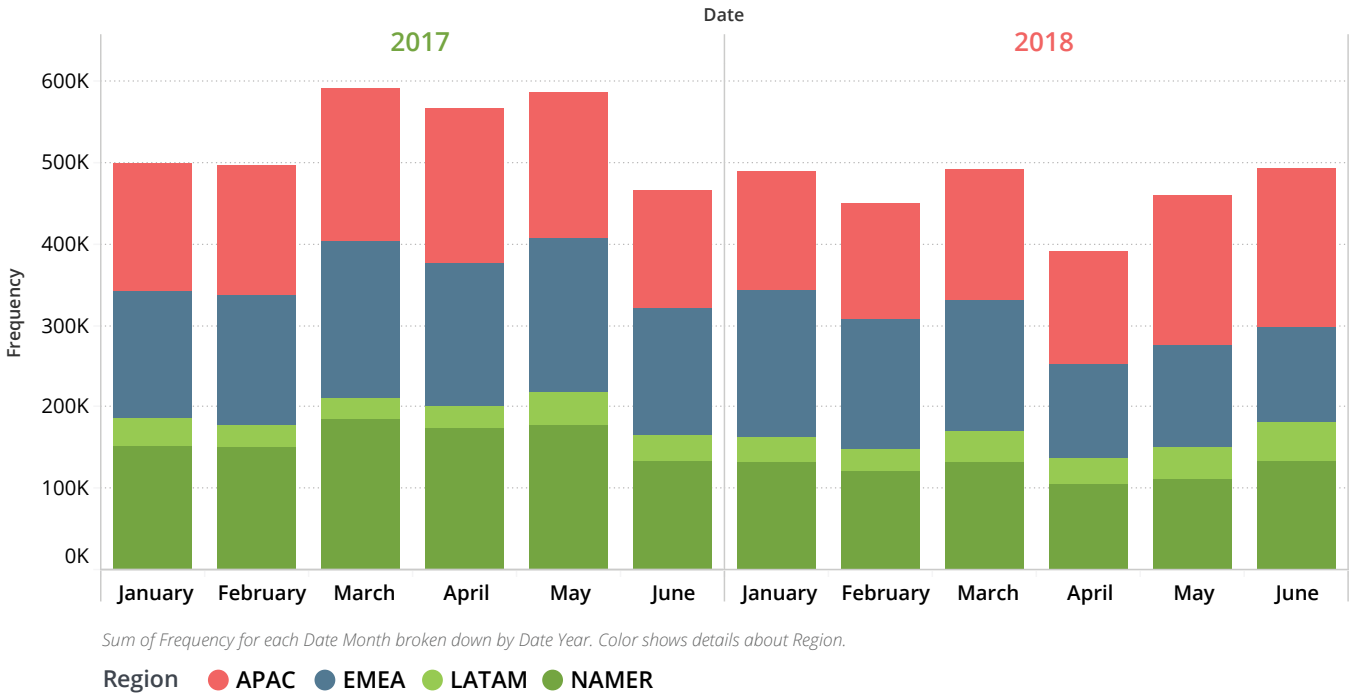


Figure 2: Global DDoS Attack 1H 2017 and 1H 2018 Frequency

REGIONAL ATTACKS

That same trend—which is an increase in the size of attacks with a dip in frequency—played out fairly consistently across regions, as Latin America was the only region to report increased attack frequency, and even that rise was relatively small (see figure 2). All the other regions showed a decrease in attack frequency accompanied by an increase in max attack size. For example, the Asia Pacific region experienced a disproportionally large number of attacks in comparison with other regions. Looking specifically at China, we saw that attacks over 500 Gbps increased from zero in 1H 2017 to 17 in 1H 2018—a particularly large growth rate. However, North America was the site of the 1.7 Tbps attack, the largest DDoS attack recorded to date.

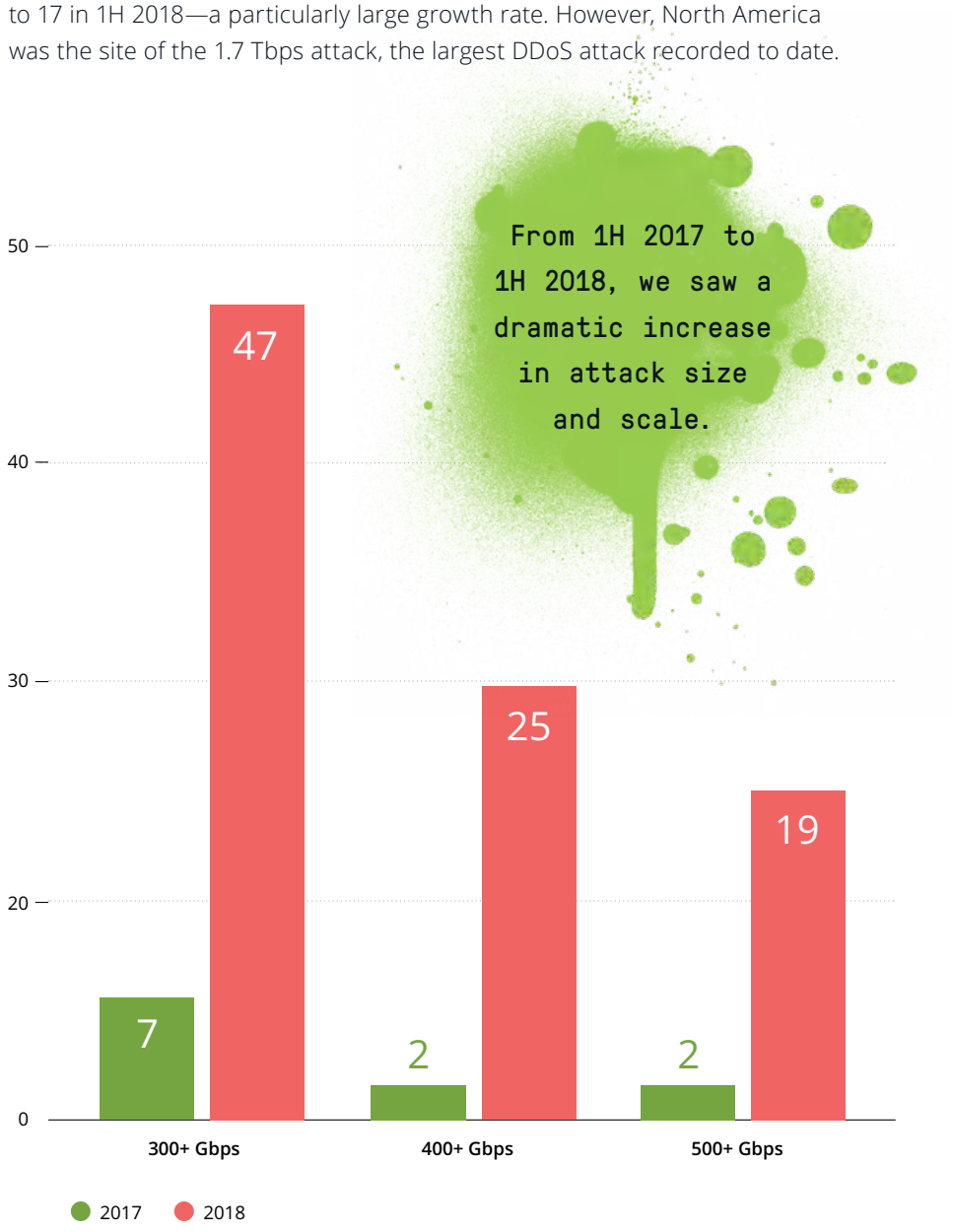


Figure 3: Global growth in large attacks 1H 2017 vs. 1H 2018

GLOBAL

INCREASE IN ATTACKS GREATER THAN 300 GBPS

7 ▶ 47

ATTACKS IN 1H 2017 — ATTACKS IN 1H 2018

ASIA PACIFIC

INCREASE IN ATTACKS GREATER THAN 300 GBPS

5 ▶ 35

ATTACKS IN 1H 2017 — ATTACKS IN 1H 2018

CHINA

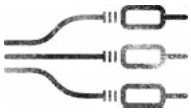
INCREASE IN ATTACKS GREATER THAN 500 GBPS

0 ▶ 17

ATTACKS IN 2017 — ATTACKS IN 2018

VERTICAL INDUSTRY ATTACKS

We analyzed attack data sorted by North American Industry Classification System (NAICS) codes, which groups companies into 22 broad categories that contain multiple large sub sectors. Comparing 1H 2017 data with 1H 2018 data for the top ten most-targeted sectors revealed some insights year over year.



WIRED TELECOMMUNICATIONS CARRIER

MAX ATTACK SIZE

339.5 GBPS IN 1H 2017 ▶ **1.7 TBPS** IN 1H 2018

For both years, the top four sub-vertical sectors remained the same, and all hailed from the Information category:

Wired Telecommunications Carriers

Data Processing, Hosting, and Related Services

Telecommunications including Satellite and Cable

Wireless Telecommunications Carriers

It's not surprising to find that telecommunications providers observe the overwhelming majority of attacks, as do data hosting services including many cloud providers. This is inherent to their role as connectivity providers. Attacks where such providers are seen as the target are either focused on their subscribers, both residential and business, as well as the infrastructure maintained for operations.

What did change are the size and frequency of attacks. Wired telecommunications carriers topped the list both years when it came to frequency of attacks. In 2017, the group sustained approximately 996,000 attacks, with a maximum attack size of 339.5 Gbps. However, 2018 told a different tale: the frequency of attacks dropped to approximately 793,000, while the maximum attack ballooned to a record 1.7 Tbps. The same holds true across the entire top four, with the exception of Data Processing, Hosting, and Related Services, which saw a slight dip in both areas.

The list also shows some shifts in popular targets. The sub-vertical sector Custom Computer Programming Services—which includes system integrators and consulting houses—dropped from sixth to tenth place year over year. And in 2017, Educational Services—an NAIC category that contains colleges and universities—appeared in eighth place, while dropping four spots to 11 in 2018. Meanwhile, 2018 showed increased attention to ecommerce, as Electronic Shopping and Mail-Order Houses took over at eighth place. This broadening and shifting of targets may be seen as evidence that the target spectrum is expanding beyond traditional targeted sectors.

Most interesting of all, however, was the appearance of the sub-vertical International Affairs in the 7th spot. Part of the Public Administration category, this sector contains information for attacks on targets such as consulates, embassies, the International Monetary Fund, the State Department, and the United Nations. This aligns with the use of DDoS against targets by government as well as those ideologically opposed to the interests represented by these institutions.

TOP VERTICALS TARGETED BY DDoS ATTACKS

	2017	# OF ATTACKS	MAX ATTACK	CATEGORY	2018	# OF ATTACKS	MAX ATTACK	CATEGORY
1	WIRED TELECOMMUNICATIONS CARRIERS	996,495	339.5 Gbps	Information	WIRED TELECOMMUNICATIONS CARRIERS	793,377	1.7 Tbps	Information
2	TELECOMMUNICATIONS	492,367	622.3 Gbps	Information	TELECOMMUNICATIONS	491,314	302.0 Gbps	Information
3	DATA PROCESSING, HOSTING & RELATED SERVICES	340,679	367.0 Gbps	Information	DATA PROCESSING, HOSTING & RELATED SERVICES	316,395	316.9 Gbps	Information
4	WIRELESS TELECOMMUNICATIONS CARRIERS	219,249	102.3 Gbps	Information	WIRELESS TELECOMMUNICATIONS CARRIERS	157,388	327.5 Gbps	Information
5	CUSTOMER COMPUTER PROGRAMMING SERVICES	62,181	451.7 Gbps	Professional, Scientific, and Technical Services	SOFTWARE PUBLISHERS	44,724	170.6 Gbps	Information
6	SOFTWARE PUBLISHERS	59,839	151.5 Gbps	Information	INTERNATIONAL AFFAIRS	40,711	34.3 Gbps	Public Administration
7	EDUCATIONAL SERVICES	58,604	28.3 Gbps	Educational Services	ELECTRONIC SHOPPING & MAIL-ORDER HOUSES	39,493	170.6 Gbps	Retail Trade
8	ELECTRONIC SHOPPING & MAIL-ORDER HOUSES	56,754	93.5 Gbps	Retail Trade	NON-TRADITIONAL TELECOMMUNICATIONS	39,004	600.0 Gbps	Information
9	COMPUTER & ELECTRONIC PRODUCT MANUFACTURING	46,894	56.8 Gbps	Manufacturing	CUSTOMER COMPUTER PROGRAMMING SERVICES	31,837	170.6 Gbps	Professional, Scientific, and Technical Services
10	OTHER COMPUTER RELATED SERVICES	36,737	36.2 Gbps	Professional, Scientific, and Technical Services	EDUCATIONAL SERVICES	27,164	96.8 Gbps	Educational Services

DDoS HIGHLIGHTS

MASS TARGETED INTRUSIONS

2 MILLION

DEVICES ON THE INTERNET THAT RESPOND TO SSDP

1.2 MILLION

CAN BE ABUSED FOR SSDP DIFFRACTION ATTACKS

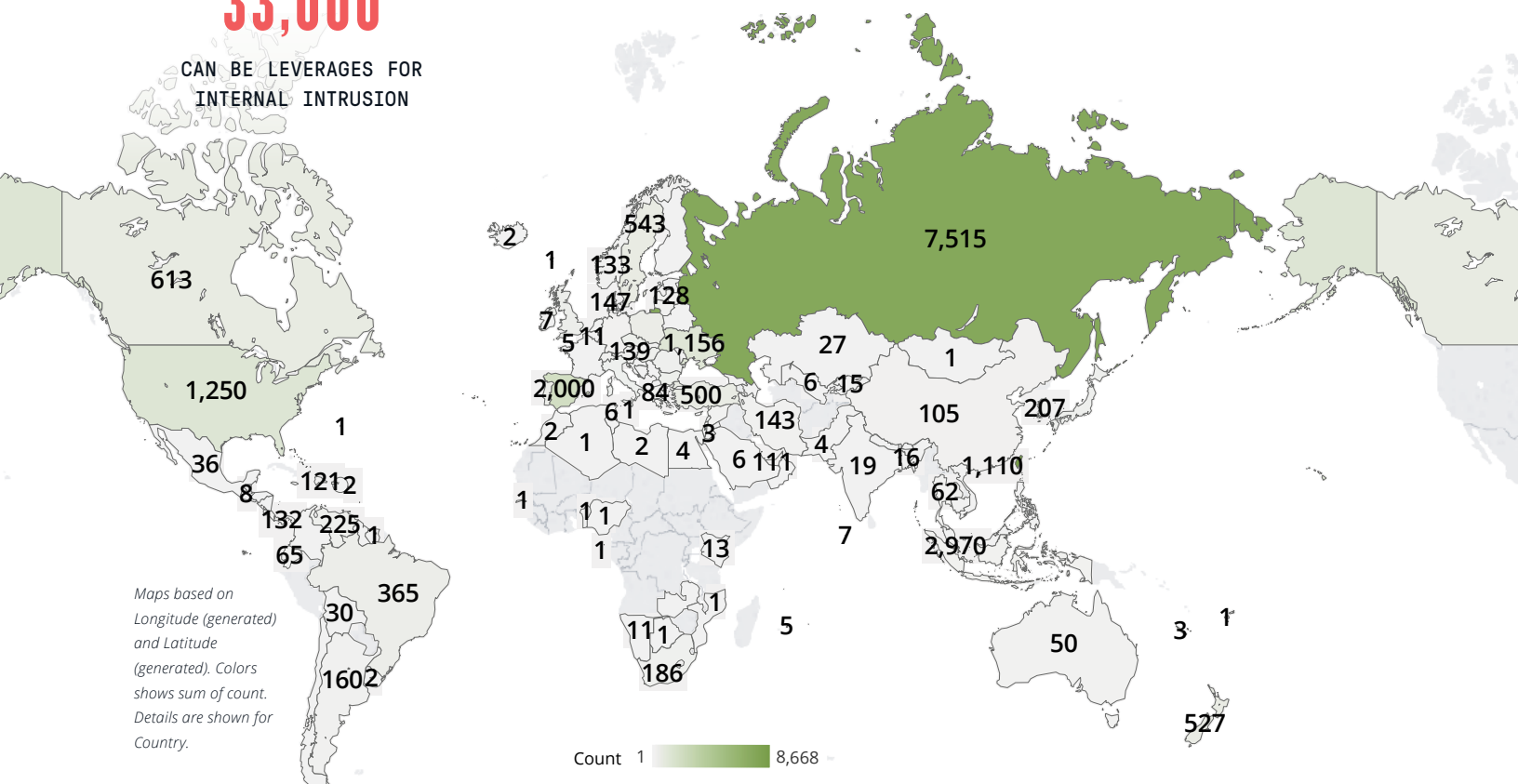
33,000

CAN BE LEVERAGES FOR INTERNAL INTRUSION

SSDP

Simple Service Discovery Protocol (SSDP) has been used for reflection/amplification attacks for many years. (In 2015, Arbor identified attacks utilizing SSDP traffic from ephemeral source ports.) However, it gained newfound attention in 2018 amid claims that this existing tool represented a new type of DDoS campaign with potentially millions of vulnerable devices. As NETSCOUT Threat Intelligence demonstrated, this is incorrect.[4] Of the total internet population of approximately 2,000,000 abusable SSDP reflectors/amplifiers, there are only about 33,000—or 1.65 percent—that could potentially be manipulated in this manner. The SSDP country chart shows how devices with vulnerable SSDP implementations are distributed globally (see Figure 4 below).

However, our team uncovered a new class of SSDP abuse where naive devices will respond to SSDP reflection/amplification attacks with a non-standard port.[5] The resulting flood of UDP packets has ephemeral source and destination ports, making mitigation more difficult—an SSDP diffraction attack. This behavior appears to stem from broad re-use in CPE devices of the open source library libupnp. Evidence from prior DDoS events suggest that attackers are aware of this behavior and may choose a pool of these misbehaving victims based on the efficacy of their attack. Mitigating these attacks requires inspecting packet content to filter the flood of SSDP replies and non-initial fragments.



Maps based on Longitude (generated) and Latitude (generated). Colors shows sum of count. Details are shown for Country.

Figure 4: SSDP Vulnerable Implementations by Country, May 2018

MEMCACHED

The Memcached attack campaign used vulnerabilities in misconfigured Memcached servers to launch enormous DDoS attacks, a process that took very little time from initial reports to the first attack tool being made available. Indeed, NETSCOUT Arbor confirmed a 1.7 Tbps reflection/amplification attack on March 5th, a record event.[6] Of 17,000 servers cited on a public list as vulnerable to this type of attack on March 5, only 550 servers remained at risk by the end of June 2018 (see Figures 5 and 6 below). This shows that the internet community has either fixed 96.8 percent of these servers or blocked them from the internet, which is commendable. On the other hand, 3.2 percent of those remain vulnerable and can be used to launch attacks, according to public list of data used in this analysis. Moreover, attackers can readily use pliable hosting companies to deploy their own vulnerable servers worldwide and use them to launch an attack. The reality is, once a DDoS type is invented, it never really goes away.

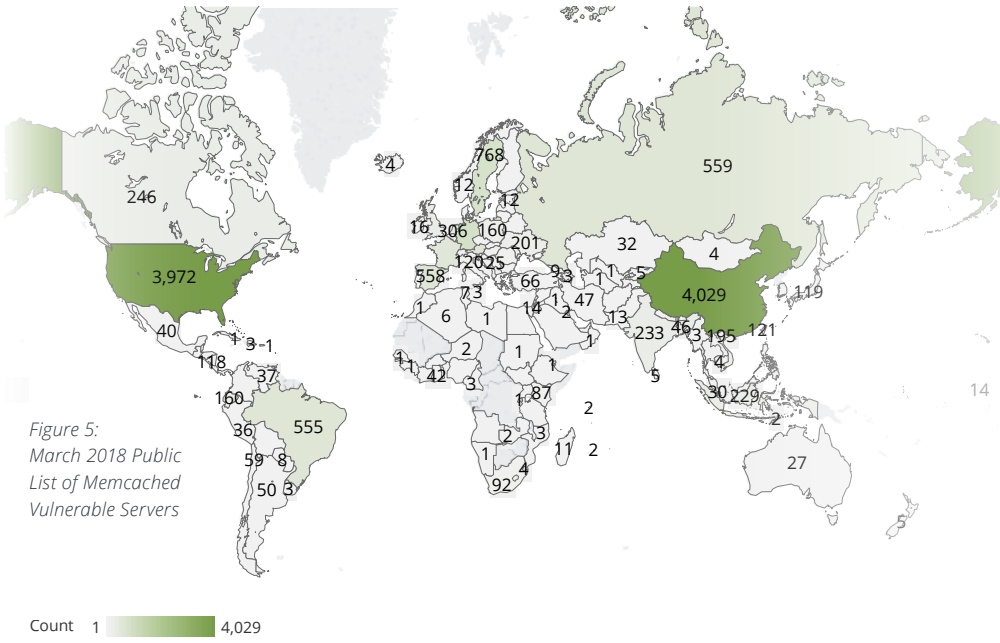


Figure 5: March 2018 Public List of Memcached Vulnerable Servers

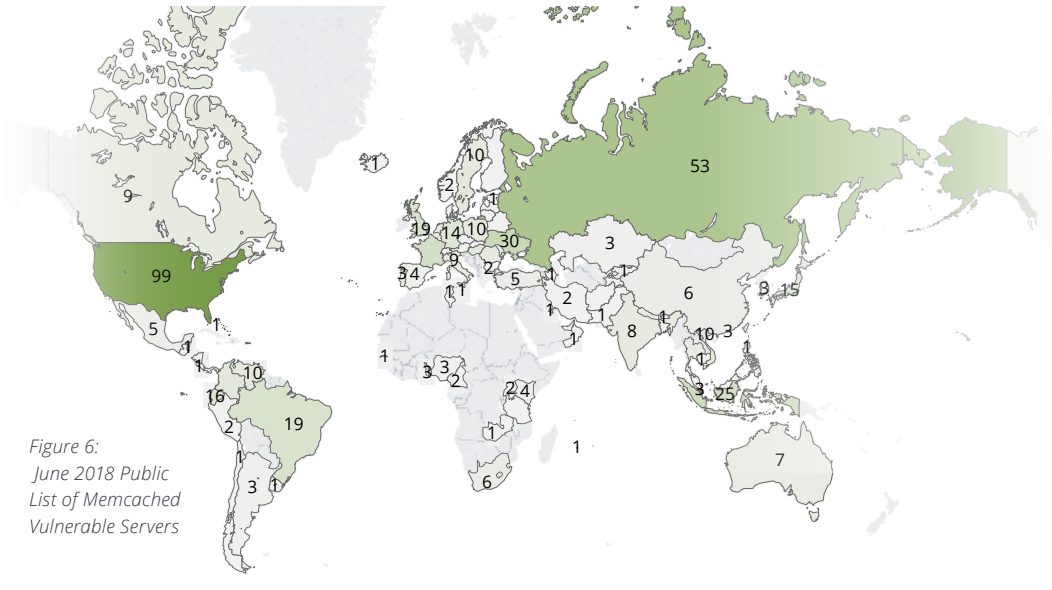


Figure 6: June 2018 Public List of Memcached Vulnerable Servers

LARGEST DDoS ATTACK RECORDED TO DATE

RECORDED BY NETSCOUT ARBOR

1.7 TBPS

ON MARCH 5, 2018

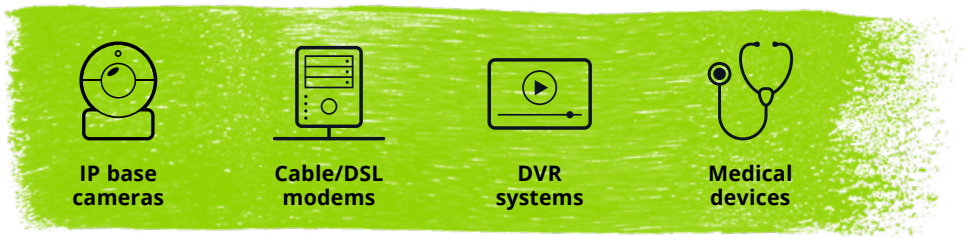
VULNERABLE SERVERS

17,000 ▸ 550

AT RISK IN MARCH 2018 — AT RISK BY JUNE 2018

IoT BOTNETS

IoT covers a wide range of devices, including (but not limited to):



CONNECTED DEVICES

VULNERABLE TO IOT BOTNETS

27 BILLION

IN 2017

▼

125 BILLION

BY 2030

Any embedded device that runs an operating system and has networking ability (send/receive data over a network) can be considered an IoT device. IoT devices quickly go to market and have low costs. These factors tend to increase the possibility that such devices will exhibit the most basic types of vulnerabilities, such as hard code/default credentials, buffer overflows, and command injection.

Most consumer IoT devices contain these types of vulnerabilities, which are further exacerbated by the fact that consumers rarely contemplate the security aspect, or perhaps do not understand the necessity of applying regular security updates and patches. With nearly 27 billion connected devices in 2017 expected to grow to 125 billion by 2030,[7] they make an extremely attractive target for malware authors.

As the explosion of IoT devices continues unabated, we expect to see corresponding increases in IoT botnets. Malware authors will continue to leverage IoT-based malware in automated fashion, quickly increasing the botnet size through worm-like spreading, network proxy functionality, and automated exploitation of vulnerabilities in internet-facing devices. It is important for organizations to apply proper patching, updates, and DDoS mitigation strategies to defend their organizations.

MIRAI

Mirai, seen as revolutionary for malware that targets IoT devices, has wrought destruction around the globe and popularized IoT-based malware. Mirai was first utilized by attackers to launch multiple high-profile, high-impact DDoS attacks against various internet properties and services in 2016.

On September 30, 2016, the source code for Mirai was published. Since then, IoT botnet authors have used it as a framework to build Mirai variants such as Satori, JenX, OMG, Wicked, and IoTrojan.[8] Satori leveraged remote code injection exploits to enhance the Mirai code, while JenX removed several features from the code and instead relies on external tools for scanning and exploitation.

OMG was also added to the Mirai legacy. OMG adds a novel feature in the form of an HTTP and SOCKS proxy. This proxy feature allows the infected IoT device to act as a pivot point, which gives the bot author the flexibility to launch additional scans for new vulnerabilities or additional attacks without having to update the original binary. Depending on the type of IoT device and how it is connected, the bot author can pivot to private networks that are connected to the infected IoT device.

Wicked joined the legion of minions in May of 2018. Wicked's flair is the ability to target Netgear routers and CCTV-DVR devices that are vulnerable to remote code execution (RCE) flaws. Within the RCE exploit, Wicked includes instructions to download and execute a copy of the Owari bot.

The latest minion to hit the scene is IoTrojan. The author of IoTrojan appears to have been involved with the Wicked and Owari botnets. IoTrojan exploits CVE-2017-17215, a remote code execution vulnerability in Huawei HG532 routers. IoTrojan includes the same DDoS functionality as its minion brothers. Often, the scanning and exploitation of devices can be automated, resulting in any susceptible devices becoming part of the botnet.

MIRAI

SOURCE CODE PUBLISHED

9.30.2016

FIVE VARIANTS

DEVELOPED BY
IoT BOTNET AUTHORS

OMG

WICKED

JEN X

SATORI

IoTROJAN

ADVANCED THREAT TRENDS

Espionage and crimeware activity continues to grow, as actors in this space develop and unleash increasingly sophisticated attacks worldwide, causing billions of dollars in damage and impacting major brand names and governments.

As predicted by many, state-sponsored activity has developed to the point where campaigns and frameworks are discovered regularly for a broad tier of nations. Our findings include campaigns attributed to Iran, North Korea, Vietnam, and India, beyond the actors commonly associated with China and Russia.

The campaigns target a wide variety of sources, from governments and industries to academic institutions. Goals range from increasing geopolitical unrest to intellectual property theft. They often use supply chains as a conduit, a tactic that allows them to attack their main target via the intertwined relationships of partners and suppliers. Between August and September 2017, for example, espionage actors compromised CCleaner, a popular tool used to clean computers and increase performance. Security research discovered the software included malware distributed to over two million users. Last June's "NotPetya" attack used a similar strategy, as the actors (widely attributed to Russian military) planted a backdoor in a popular Ukrainian accounting software package. The malware mainly targeted the Ukraine, where more than 80 businesses were affected, but it also proliferated across France, Germany, Italy, Poland, the United Kingdom, Russia, and the United States.

Another avenue espionage actors use involves masquerading as legitimate software, unbeknownst to the end user. Arguably, this technique could fall under supply chain attacks, but attackers do not need to use the supply chain distribution of legitimate businesses for proliferation. Such was the case with the recent discovery of the double-agent malware in the Absolute LoJack recovery software for laptops attack associated with Fancy Bear. The attackers replaced the command and control domain to one of their own. The software, which often comes preinstalled on laptops, would then beacon back to attacker-controlled servers rather than the servers intended to allow for remote recovery of stolen laptops. This effectively gave the actors remote access to the compromised computers.

Meanwhile, the crimeware arena continues to expand and weaponize, as traditional malware adds worm modules, allowing the malicious software to spread faster and more easily. Many crimeware operations, including banking malware and ransomware, have also added modules or secondary downloads that allow actors to mine cryptocurrency such as Bitcoin or Monero. The move from ransomware to cryptocurrency mining lowers the threshold for detection and law enforcement attention, insulating the attackers against concentrated takedown efforts and reprisal. Due to the increasing sophistication and ability to more rapidly infect systems, many campaigns can more easily and directly affect millions of consumers and impact enterprises, government organizations, and other organizations globally.

Such activity is often found via research and monitoring from security teams such as ASERT, which discovered the Absolute Lojack theft recovery software hijack and Kardon Loader malware, among others.

Over the course of the year, the ASERT team has monitored and identified dozens of espionage and crimeware groups and activities. In particular, the team finds the following threat groups of interest due to recent trends, unique tactics, or geo-political ramifications

The campaigns target a wide variety of sources, from governments and industries to academia. Goals range from increasing geopolitical unrest to intellectual property theft.

OILRIG

OilRig is an active and organized Iranian APT threat group that has targeted specific government, industry, academic, and financial institutions for strategic purposes since at least 2015.

It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. While this group can quickly utilize newly discovered vulnerabilities (such as CVE-2017-0199 and CVE-2017-11882), they primarily rely on social engineering to compromise victims. They are known for extensive research, continuous development, and evasion testing for their customized toolset. Additionally, they employ custom DNS tunneling protocols for command and control (C2) and exfiltration of credentials and files.

- ASERT researchers observed this group targeting financial, high technology, and government verticals.
- OilRig this year was seen for the first time using an IIS ISAPI filter,[9] dynamic-link-libraries often used to modify and enhance functionality provided by IIS such as URLs, for a C2, which is an uncommon technique for this group.

Profile

COUNTRY OF ORIGIN

Iran

PRIMARY TARGETS

Government
Industry
Academic
Financial

KNOWN TECHNIQUES

Anti-virus Evasion, Webshells, Backdoors, DNS Tunneling, Credential Dumping, Native System Applications, FTP Data Exfiltration, Supply Chain

FANCY BEAR

Also known as APT28, Fancy Bear is an APT group working out of Russia. Likely operating since the mid-2000s, this group is the most well-known and the most visible of the Russian APT groups and has been attributed to the Russian government.

Their cyber attacks usually focus on current geopolitical issues and Industrial Control System (ICS)/critical infrastructure, which they target with destructive malware. They are widely suspected of interfering in elections in multiple countries, including the United States and France, and are believed to be responsible for cyber attacks on targets such as the International Olympic Committee, NATO, and the Democratic National Committee. This year, the ASERT team associated Fancy Bear with malware in Absolute LoJack's recovery software for laptops.[10] Absolute LoJack, formerly known as Computrace, is a legitimate laptop recovery solution used by a number of companies to protect their assets should they be stolen. The software makes an excellent double agent due to appearing as legitimate software while natively allowing remote code execution

Profile

COUNTRY OF ORIGIN

Russia

PRIMARY TARGETS

International Olympic Committee

Elections

NATO

Democratic National Committee

KNOWN TECHNIQUES

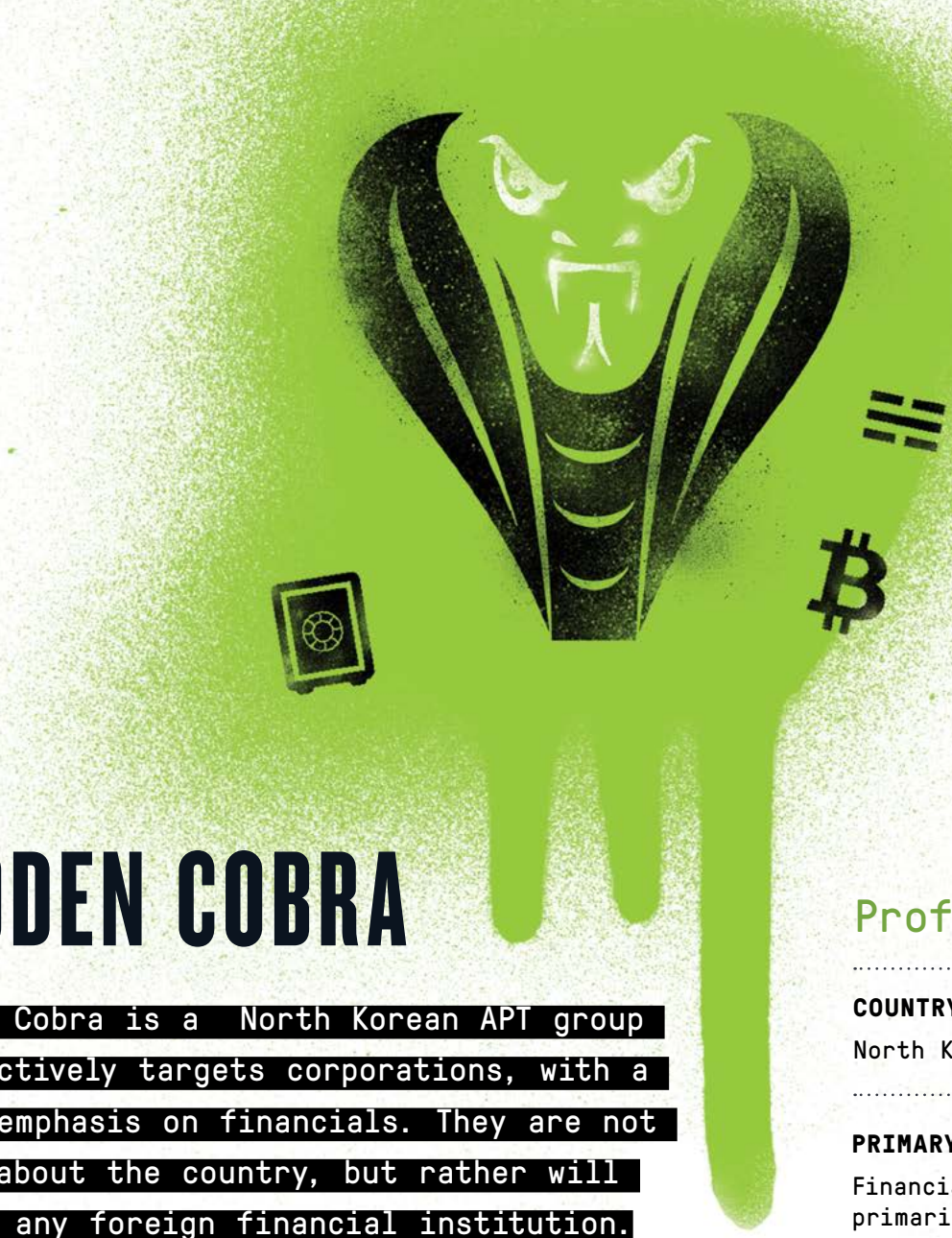
Bootkit, Credential Dumping, Screen Captures, COM Hijacking, Privilege Escalation, Lateral Movement Vulnerabilities, timestomping, Removable Media Propagation, Keylogging, Access Token Manipulation, Legitimate Software Hijack

Although the initial intrusion vector for this activity remains unknown, Fancy Bear often utilizes phishing email to deliver payloads.

- ASERT researchers identified agents containing C2 domains likely associated with Fancy Bear operations. Proof of concepts in using this software as a backdoor or intrusion vector date back to 2014, and its continued use suggest attackers could have used it in long-running operations.
- Initially, the software agents containing rogue C2 had low anti-virus (AV) detection, which increased the probability of infection and subsequent successful C2 communication.
- The distribution mechanism for the malicious software remains unknown. However, Fancy Bear commonly uses phishing to deliver malware payloads, as seen with Seduploader in late 2017.
- Throughout the previous year, ASERT observed Fancy Bear activity targeting finance and government verticals.

Fancy Bear activity also included the use of VPNFilter malware based on findings from other public research. ASERT analysts independently verified many of the claims about the malware capabilities.

- VPNFilter malware is a multi-stage, modular platform with versatile capabilities to support both intelligence gathering and destructive capabilities, as identified by public security research.[11] Based on publicly available research, some secondary payloads also provide destructive capabilities to the malware.
- First detected in May, VPNFilter is estimated to have hijacked half a million IoT devices such as routers and network-attached storage (NAS) devices.
- The known devices affected by VPNFilter include Linksys, MikroTik, Netgear, TP-Link, ASUS, D-Link, Huawei, Ubiquiti, UPVEL, and ZTE networking equipment in the small and home office space, as well at QNAP NAS devices.



HIDDEN COBRA

Hidden Cobra is a North Korean APT group that actively targets corporations, with a heavy emphasis on financials. They are not picky about the country, but rather will target any foreign financial institution.

They have also been seen targeting cryptocurrency exchanges. South Korea and the US are its primary targets when not focusing on the financial sector. For example, many researchers attribute the Sony hack to this group. They are known for being destructive to cover up their tracks. Tools and capabilities used by Hidden Cobra include DDoS botnets, keyloggers, remote access Trojans (RATs), and wiper malware. Recent activity includes:

- Targeting financial organizations in Turkey with a variant of the group's Bankshot malware implant.[12] The attack involved financial organizations controlled by the Turkish government, as well as three other large Turkish financial institutions.
- Phishing attacks that target financial tech and cryptocurrencies, along with their surrounding exchange system. Hidden Cobra is believed to have successfully infiltrated and stolen funds from numerous exchanges.[13]
- Suspected in attacks against Central and South American banks.

Profile

COUNTRY OF ORIGIN

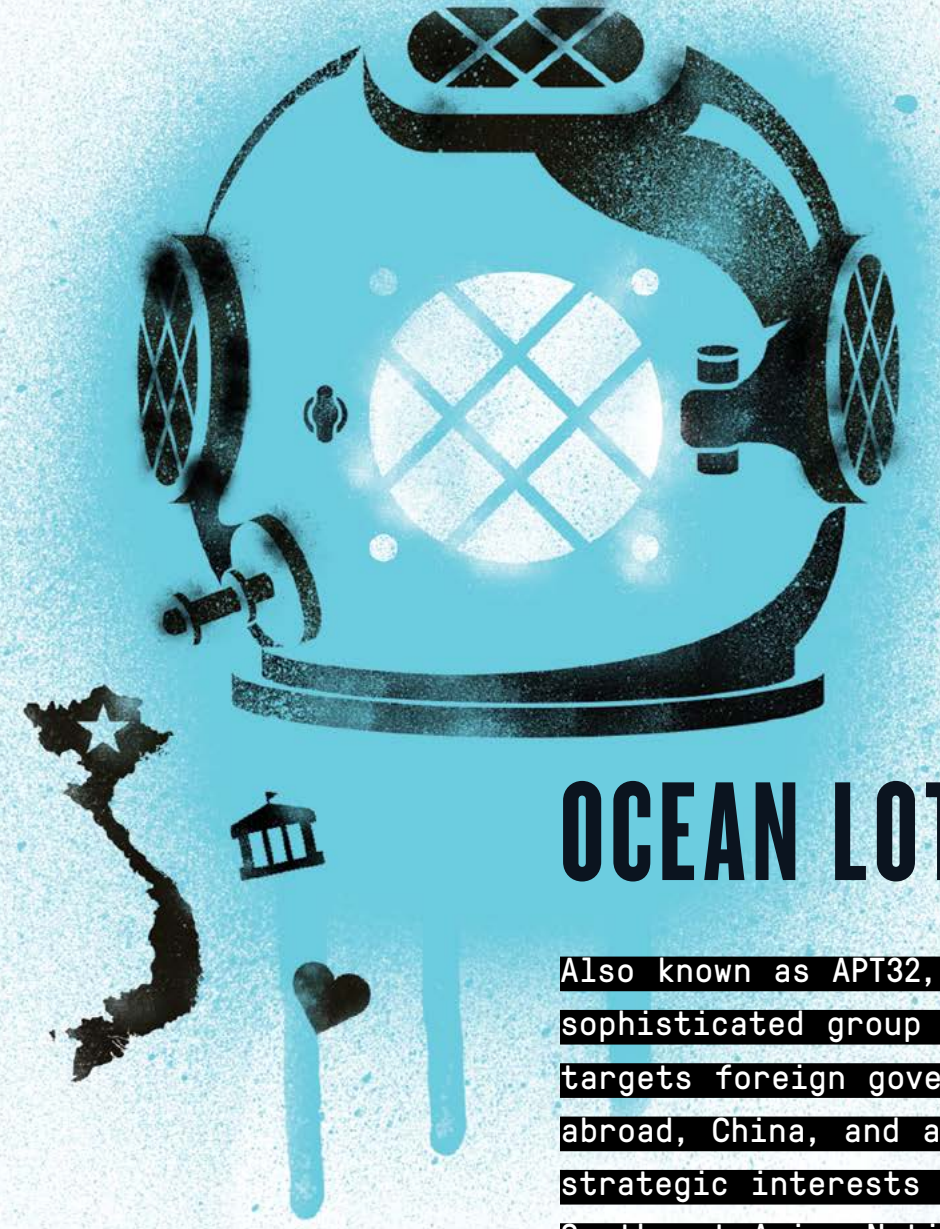
North Korea

PRIMARY TARGETS

Financial Institutions primarily in South Korea and U.S.

KNOWN TECHNIQUES

DDoS Botnet, Disabling Security Products, Brute Force Lateral Movement, SMTP Data Exfiltration, Bootkit, Access Token Manipulation, Remote Access Trojan, Keylogger, Destructive Malware, Custom C2 Protocol, Timestomping, Persistent Shortcuts



OCEAN LOTUS

Also known as APT32, Ocean Lotus is a sophisticated group from Vietnam that historically targets foreign governments - especially near-abroad, China, and anyone with business or strategic interests in Vietnam, the Association of Southeast Asian Nations (ASEAN), media, and human rights civil society organizations, even those within their own country.

Profile

COUNTRY OF ORIGIN

Vietnam

PRIMARY TARGETS

Foreign Government

KNOWN TECHNIQUES

Cobalt Strike Framework, Powershell scripting, Timestomping, Privilege Escalation, Supply Chain, Webshells

Active since at least 2012, Ocean Lotus uses a full suite of custom malware often combined with commercial products and has exploits for both Windows and Macintosh systems. Targeting also appears to be very surgical rather than widespread.

Theft has included intellectual property, confidential strategic business information, and intelligence information. Recent discoveries of threat activity include:

- Recent sample seen utilizing control panel (CPL) files, following an apparent trend of some in the APT community away from executables. CPL files launch in a similar manner as executables.
- The group frequently updates their backdoors, infrastructure, and infection vectors.
- The ASERT team observed Ocean Lotus activity targeting government and finance sectors over the past year.

DONOT TEAM

NETSCOUT Threat Intelligence's research into the EHDevel malware toolkit led to the discovery of a new modular malware framework attributed to the Donot Team.[14]

We assess that this new framework picks up where EHDlevel left off, focusing on targets in South Asia. The framework discovered by the ASERT team uses a new modular malware dubbed the "yty" framework. While the infrastructure is similar to that used by existing publicly known APT groups, there are enough differences that we can't say definitively if this activity fits the methods of those groups.

- ASERT discovered a new modular malware framework dubbed 'yty' that focuses on file collection, screenshots, and keylogging. While we believe this framework and its components are new, it shares many tactics, techniques, procedures, and indicators of compromise with the EHDevel malware framework.
- We believe the Donot Team, the threat actors who created EHDevel, also created the yty framework.
- In a likely effort to disguise the malware and its operations, the authors coded several references into the malware for football—it is unclear whether they mean American football or soccer. The theme may allow the network traffic to fly under the radar.
- ASERT also identified activity associated with the Donot Team targeting government, retail, finance, and technology verticals over the previous year.

Profile

COUNTRY OF ORIGIN

Unknown

PRIMARY TARGETS

Government

Retail

Finance

Technology

KNOWN TECHNIQUES

Modular Malware Framework, Screenshots, Keylogging, File Exfiltration, Sandbox Detection, System Profiling

CRIMEWARE HIGHLIGHTS

The crimeware sector remains robust and shows signals of spreading beyond its traditional attack methods.

According to Verizon's 2018 Data Breach Investigations Report, email-driven campaigns targeting financials, such as Emotet and Trickbot, continue to claim the lion's share of activity (about 90 percent.) Web attacks comprise about six percent of the pie, while direct attacks make up the rest. However, there are some notable changes in methods designed to accelerate proliferation. Inspired by 2017 worm events such as WannaCry, major crimeware groups added worm modules to malware, essentially adding a self-propagation method that allows the malware to spread faster and more easily.

In addition to new worm module development, we also saw an increased focus on cryptocurrency mining in malware. It seems that attackers see this method as a less risky and more profitable alternative to ransomware, since the latter has the unfortunate side effect of drawing attention from law enforcement agencies.

Meanwhile, new platforms such as Kardon Loader are emerging, and well-known ones such as Panda Banker are being directed at new targets. Even in the face of take-downs and arrests of key individuals, botnets like Dridex continue to remain relevant. It all adds up to reveal a sector that's constantly reinventing technology and methods to expand its footprint and improve attack efficacy.

ASERT researchers found the following to be particularly emblematic of these overall trends.

EMOTET

Emotet has historically been recognized as a modular malware framework capable of banking theft, spamming, and credential theft.

In more recent versions, attackers moved away from banking modules in favor of adding a cryptocurrency miner for Monero and a worm module for self-propagation. This continued expansion of capabilities allows Emotet to thrive and become more dangerous, as exemplified by the February 2018 attack on Allentown, PA,[15] which shut down several financial and public safety operations and cost the city an estimated US $1 million. This new wave of Emotet trojan infections spreads via phishing emails and downloads additional modules, such as a worm module for automatic propagation.

- Emotet added a Monero coin-mining module.
- Following the public disclosure of Eternal Blue exploits, Emotet added a "worm" module for automatic propagation using the exploits.

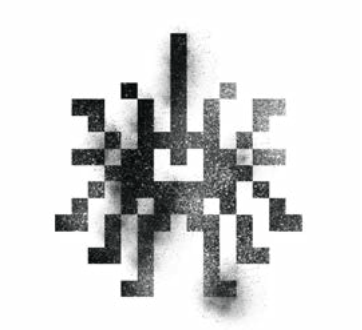
TRICKBOT

First discovered in 2016, Trickbot is a banking Trojan that targets the customers of major banks.

Trickbot uses webinjects and redirects to steal from its victims. Trickbot spreads via phishing campaigns that direct users to fraudulent websites masquerading as legitimate operations. Although many of the spam campaigns distribute widely, the targets in Trickbot webinjects have a higher proportionality in the United States and United Kingdom. In addition to these main targets, the attackers included targets for dozens of additional countries (Canada, Sweden, Australia, and more).

Trickbot remains in constant development and has recently demonstrated some new capabilities:

- Trickbot now utilizes an exploit CVE- 2018-8174 for infection.[16]
- Trickbot also received a Monero coin mining module.
- Addition of a worm module for automatic propagation in wake of the EternalBlue/EternalRomance public disclosures.
- Recent versions of Trickbot saw rapid growth in the number of targeted entities.[17]



KARDON LOADER

ASERT researchers discovered KardonLoader[18] being advertised on underground forums.

Advertised as a paid open beta product, Kardon Loader is a malware downloader with functionality that allows customers to open their own botshop, which grants the purchaser the ability to rebuild the bot and sell access to others. Offered by an actor with the user name Yattaze, this product had been available since late April. The actor offers the sale of the malware as a stand-alone build with charges for each additional rebuild, or the ability to set up a botshop in which case any customer can establish their own operation and further sell access to a new customer base.

Malware authors and distributors leverage downloader malware and botshops to build malware distribution networks. Malware distribution networks are commonly used by cyber criminals to create botnets to distribute additional payloads such as credential theft malware, ransomware, banking Trojans, and others. These distribution networks are often run by third-party operators and offered as a service in underground market.

NETSCOUT Threat Intelligence actively collects indicators associated with this malware family to provide protection for our NETSCOUT Arbor customers.

- NETSCOUT Threat Intelligence researchers discovered Kardon Loader advertised on underground forums.
- Kardon Loader features functionality allowing customers to open their own botshop, which grants the purchaser the ability to rebuild the bot and sell access to others.
- Kardon Loader was in early stages of development, offered as a public beta at the time of discovery.
- It incorporates numerous anti- analysis checks to discourage analysis.
- After a member of the underground community informed the actor of researcher interest on Kardon Loader, the actor stopped actively advertising the malware and stopped posting in threads related to it. However, the actor is still active on underground forums, so it is likely he or she will publish malware in the future.

PANDA BANKER

Based on the Zeus malware family, Panda Banker uses a technique known as "man in the browser" along with web injects to steal user credentials, account numbers, and ultimately money from victim banking accounts.

This banking malware, first seen in the wild in the beginning of 2016, has seen consistent, incremental development since its appearance. Panda Banker is sold as a kit on underground forums, resulting in multiple users of the malware.

Cybercrime threat actors tend to focus their campaigns on particular countries, usually dependent on their ability to convert stolen credentials and account details from those locations into real money. Over the years, we've seen Panda Banker campaigns focus on financial institutions in Italy, Canada, Australia, Germany, the United States, and the United Kingdom.

Recently, Panda Banker expanded to target Japan.[19]

- A threat actor using the well-known banking malware Panda Banker started targeting financial institutions in Japan.
- Based on ASERT research, this is the first time that we have seen Panda Banker injects targeting Japanese organizations.
- It is likely a new campaign or actor started using Panda Banker, since in addition to the previously unseen Japanese targeting, ASERT has not seen any indicator of compromise (IOC) overlaps with previous Panda Banker campaigns.
- The sample used in this campaign was the first sample we observed in the wild to use the newest version of Panda Banker, version 2.6.6.

CONCLUSION

The accelerating internet-scale threat paradigm changes the frontiers for where and how attacks can be launched, observed and interdicted.

The complexion of the threat landscape is moving more rapidly, expanding footprint and changing tactics. Methods that are commonplace in the DDoS threat tool kit have sprung to crimeware and espionage. The increase in the use of auto propagation methods; especially worms and mass malware distribution are seen in the use of CCleaner, VPNFilter, WannaCry and NotPetya programs. The array of state actors will continue to grow, and we will see new groups emerge from regions that have not previously been associated with significant activity.

The hunger for exploitation of new vectors will also continue, as we have seen in the immense DDoS attack impact created by Memcached earlier this year. The use of the well known network protocol vector, SSDP, is now being leveraged for internal intrusion. In addition, the use of legitimate software programs by espionage groups and the addition of secondary tactics such as adding crypto currency mining by crime ware actors as we have seen in the case of Emotet and Trickbot. This creates new pressure for heightened awareness and scrutiny of defenses for security and IT teams within organizations across all verticals.

This accelerating internet-scale threat paradigm changes the frontiers for where and how attacks can be launched, observed and interdicted. Global threats will require new global interventions, involving enterprises, service providers, governments and consumers.

The ASERT team will continue to monitor the threat landscape and report on new groups and malware under development, as well as updated techniques. Although it is difficult to be fully prepared for any incoming threat, regular consumption and application of threat intelligence is an important preparatory safeguard, as doing so provides insight to inform both strategic direction and areas to address technically.

APPENDIX

[1] asert.arbornetworks.com/reaper-madness/

[2] media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/Steinthor%20Bjarnason%20and%20Jason%20Jones/

[3] www.youtube.com/watch?v=qMQwENS30pg

[4] asert.arbornetworks.com/the-importance-of-being-accurate-ssdp-diffraction-attacks-udp-refraction-attacks-and-upnp-nat-bypass/

[5] asert.arbornetworks.com/a-new-twist-in-ssdp-attacks/

[6] asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/

[7] news.ihsmarkit.com/press-release/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says

[8] asert.arbornetworks.com/omg-mirai-minions-are-wicked/

[9] www.nyotron.com/nyotron-discovers-next-generation-oilrig-attacks/

[10] asert.arbornetworks.com/lojack-becomes-a-double-agent/

[11] www.us-cert.gov/ncas/current-activity/2018/05/23/VPNFilter-Destructive-Malware

[12] www.us-cert.gov/ncas/current-activity/2017/12/21/North-Korean-Malicious-Cyber-Activity

[13] securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

[14] asert.arbornetworks.com/donot-team-leverages-new-modular-malware-framework-south-asia/

[15] www.us-cert.gov/ncas/alerts/TA18-201A

[16] myonlinesecurity.co.uk/fake-hmrc-important-outstanding-amount-delivers-trickbot-via-cve-2018-8174/

[17] www.f5.com/labs/articles/threat-intelligence/trickbot-rapidly-expands-its-targets-in-august-shifting-focus-to-us-banks-and-credit-card-companies

[18] asert.arbornetworks.com/kardon-loader-looks-for-beta-testers/

[19] asert.arbornetworks.com/panda-banker-zeros-in-on-japanese-targets/

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.

SECTR_1H2018_EN-1801