



NETSCOUT Threat Intelligence Report
- Powered by ATLAS

DAWN OF THE TERRORBIT ERA

Findings from Second Half 2018

NETSCOUT®

TABLE OF CONTENTS

INTRODUCTION	1
Editor's Note	1
Executive Summary	2
ADVANCED THREATS	4
Overview	4
Nation-State Actor Highlights	5
CRIMEWARE	11
Overview	11
Crimeware Highlights	12
DDoS TRENDS	18
Overview	18
Year-to-Year Attack Volume Trends	20
Regional Attacks	21
Vertical Industry Attacks	22
DDoS Highlights	25
CONCLUSION	28
APPENDIX	29

EDITOR'S NOTE

HARDIK MODI *Senior Director, 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, while state-sponsored APT groups accelerate activity and traditional crimeware activity continues to proliferate.

We have actively monitored this space since 2007, when the company launched 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 correlates this and other data sets to provide automated data sharing and intelligence, facilitating usage by all internet users, business and private, giving them a broader perspective to better understand and react to the threats they face. ATLAS' reputation allows for collaboration or automated data 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 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 on ASERT are part of a group of experts that are referred to as 'super remediaters' and represent the best in information security practices and threat intelligence. ASERT provides operationally viable threat intelligence to thousands of network operator customers via automatic, in-band security feeds. The group contributes to dozens of operational security councils and is a founding member of the Red Sky Alliance, as well as being a member of the Cyber Threat Alliance. ASERT also has working relationships with hundreds of international CERTs.

By using ATLAS' internet-scale visibility in conjunction with more tactical holdings such as automated malware analysis pipelines, sinkholes, scanners, and 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, based on all our holdings and driven by analysis from our intelligence unit.

EXECUTIVE SUMMARY

LARGEST DDoS ATTACK
ON RECORD

1.7 TBPS

2H 2018 SAW THE
GLOBAL MAX DDoS ATTACK
SIZE INCREASE

▲ 19%

ONCE PLUGGED INTO THE
INTERNET IoT DEVICES ARE
ATTACKED WITHIN

5 MINUTES

AND TARGETED BY
SPECIFIC EXPLOITS IN

24 HOURS

When it comes to the global threat landscape, the second half of 2018 revealed the equivalent of attacks on steroids. NETSCOUT Threat Intelligence saw attackers bulk up existing tactics, rapidly evolve new performance enhancements, and apply smart business techniques to vastly accelerate attack growth rate.

IoT devices were attacked within five minutes of being plugged into the internet. Malware authors not only built more advanced devices, but also applied their learnings from IoT botnet manipulation to target new areas such as commodity Linux servers using malware like Mirai. Malicious actors, criminal organizations, and even individuals busily diversified malware tools and families, attack vectors, and distribution channels — all aimed at an expanding array of targets. Meanwhile, nation-state advanced persistent threat (APT) group activity ratcheted up in volume and targets. Here are a few highlights of the major trends that we observed.

COUNTDOWN TO ATTACK

Constant targets of DDoS malware, IoT devices are now under attack five minutes after being plugged in and targeted by specific exploits within 24 hours. IoT security is minimal to nonexistent on many devices, making this an increasingly dangerous and vulnerable sector as now everything from life-saving medical devices and equipment to home security systems and cars are IoT-equipped.

THE 'TERRORBIT ATTACK' AND BEYOND

February and March of 2018 marked the first reported terabit attacks. While the second half of 2018 didn't reveal new attacks at that volume, it is likely due to systemic changes to counter the Memcached vulnerability and the fact that other vectors didn't emerge. Overall attack numbers were up 26 percent, while those in the 100–400 Gbps range exploded, showing continued interest and maturity of tooling in this midrange. It's only a matter of time before new vulnerabilities drive attacks at the higher end again.

NATION-STATE INNOVATION

Activity from key nation-state actors such as China, Russia, Iran, and North Korea showed no sign of ebbing. New groups emerged, while known entities updated and evolved their tactics, techniques, and procedures (TTPs), combining custom tools with commodity crimeware to further extend their reach. We noted continued innovation from groups, such as the use of Chrome extensions to enable persistence in the STOLEN PENCIL campaign.

COMMERCIALIZATION OF CRIMEWARE

We saw a robust marketplace driven by well-stocked innovation pipelines from rapidly growing organizations. If this sounds like a business story, that's because it is. The cybercriminal underground operates much like a legitimate business on the right side of the law, with the huge proviso that cybercrime organizations cause billions of dollars in damage and negatively impact major enterprises and governments.

For instance, campaigns such as DanaBot use an affiliate model that distributes labor to specialists and moves away from the more inefficient method of managing the entire process in house. While this was popularized a few years ago with exploit kits like Angler, DanaBot has taken it to the next level by rapidly establishing its presence across the globe with 12 separate affiliates targeting financial institutions in many countries. Can a B-school case study write-up be far behind?

OVERALL THE NUMBER OF DDoS ATTACKS INCREASES

▲ 26%

YEAR OVER YEAR

DANABOT

CAMPAIGN HAS TAKEN CRIMEWARE TO THE NEXT LEVEL, ESTABLISHING ITS PRESENCE ACROSS THE GLOBE WITH

12 AFFILIATES

TARGETING FINANCIAL INSTITUTIONS

NETSCOUT'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.

ADVANCED THREAT.

The ATLAS Security and Engineering Research Team (ASERT) tracked approximately 35 APT groups around the globe in the latter half of 2018. These groups targeted verticals such as academia, government, and finance across the Middle East; the United States; Central and South America; and East and Southeast Asia. While the groups varied in sophistication, targeting, and TTPs, we saw the continued emergence of numerous groups on a worldwide basis.

NETSCOUT THREAT INTELLIGENCE

TRACKED APPROXIMATELY

35

APT GROUPS
IN 2H 2018

APT groups not only grew in number, but also in sophistication. Nation states continually added additional facets of cyber espionage to their toolkit, including new targeting methods. They used methods such as a unified extensible firmware interface (UEFI) rootkit known as LoJax and a browser plugin first utilized by a suspected North Korean group. In addition to uncovering previously unknown operations and researching new campaigns and methods, ASERT tracked dozens of APT groups and their activity across the internet using ATLAS®.

KEY FINDINGS INCLUDE

- New nation-state APT group activity was discovered at an accelerating rate, while known groups evolved and expanded their capabilities.
- The global diversity of APT operations resulted in a wide array of targeting that included academia, government, finance, and telecommunications industries.
- Analysis of APT malware samples in the ASERT holdings found combinations of custom tools and crimeware, as well as misuse of legitimate software such as LoJax.
- The numerous groups we tracked added additional capabilities to their arsenal, including a few observed zero-day attacks, the malicious use of legitimate bootkit software, and at least one instance of a browser plugin.

CHINA

Exfiltration of intellectual property via human and cyber means has been a fundamental component of China's modernization. It still is carried out by Chinese APT groups, despite the fact that China has the means to purchase any patents or companies that it desires.

The majority of what ASERT observed in 2H 2018 centered on geopolitical and strategic intelligence gathering, including a highly publicized hotel breach.



Leviathan or TEMP.Periscope

Highly engaged in the South China Sea, this group is very interested in both military and commercial regional activity, targeting countries and organizations that monitor or transit the area. Maritime, defense, and logistics industries are commonly targeted along with in-region countries, including a recent attack targeting Cambodia.¹

Leviathan suspected of using a variety of tools such as Responder, NetBIOS Poisoning Tool, and exploitation methods like ETERNALBLUE. The use of these tools came only after they'd been made public, showcasing this group's preference to "live off the land".²

Stone Panda, APT10, or Menupass

Associated with the Ministry of State Security (MSS), this group targets managed service providers (MSPs) as a conduit to accessing sensitive information in a variety of industries, especially in Japan. They play a long game of careful reconnaissance followed by intrusion into service organizations in order to gain access to the actual target, which enables them to target entire supply chains and industries. ASERT observed a large spike in activity against logistics and government targets in July and August 2018, lending further credence to their long-game tactics.

Emissary Panda or Lucky Mouse

This group focuses heavily on diplomats and embassies and has targeted central Asian governments for at least most of 2018 by accessing a common data center. The group utilized that access to turn government websites into watering holes to lure additional victims. The diplomatic targeting is historically related to Central and Western Asia's political climate. Because of the nature of the group's TTPs, victims often range across verticals such as government, academia, and finance in addition to the primary targets of diplomats and embassies.

Emissary Panda spotted utilizing an in-memory C++ Trojan that listens for incoming connections from the C2 along with injecting C2 traffic into an RDP port.³ The group used a proxy tool, signed using a stolen certificate, to drop the trojan.



IRAN

From ASERT's perspective, Iranian APT groups appeared to continue on steadily, although changes in their targeting sometimes made them more or less visible.

They continued to develop and evolve their malware, heavily target their neighbors, and closely monitor Iranians (both in-country and out). They also targeted the usual sectors for intelligence value: aerospace, technology, and governments, among others.

Dark Hydrus

This APT group is a relative newcomer (first observed in the summer of 2018) that typically targets governments in the Middle East, but ASERT also observed financial institutions in Asia being targeted. ASERT found a significant overlap in the indicators of compromise (IoCs) in these verticals, suggesting that the same TTPs were used.

Dark Hydrus added a number of anti-analysis/anti-sandbox checks to a malware family called RogueRobin⁴. While anti-analysis checks are not new, the adversary included a large number of checks that include known sandbox names, RAM & CPU size/number, and instructions to look for known analysis tools like Wireshark and SysInternals.





Charming Kitten or NEWSCASTER

This group is known to target and masquerade as legitimate companies. ASERT noted an explosion in this group's infrastructure, with the usual themes: mimicry of legitimate software as well as doppelgängers of legitimate companies. In this mix, ASERT observed doppelgänger domains for aerospace, industrial vehicles, and technology companies, as well as for some non-profit entities in Saudi Arabia.

Charming Kitten ASERT's research led us to discover a legacy C2 pointing to an active or re-activated Cobalt-Strike server.

Chafer

A third Iranian group ASERT tracked predominantly targets the airline industry with both commodity and custom malware. Specific targets include companies that support the airline industry, such as technology and telecom companies, engineering consultants, and even administrative support contractors. While public reporting noted this group's activity in the Middle East, ASERT also observed activity in the United States, Southeast Asia, and South America.

OilRig, APT34 or Helix Kitten

This group continues to evolve its capabilities as noted in a September 2018 blog post ASERT published highlighting changes to BONDUPDATER, a PowerShell-based Trojan that now obfuscates the data prior to exfiltration. ASERT managed to capture live command-and-control (C2) communications from this group and reverse engineer the communication protocols the malware used.⁵ We primarily observed the group actively targeting government and technology industries.

Oilrig continues to evolve a custom PowerShell DNS tunnel, BONDUPDATER, a backdoor tool ([2017-2018](#)). Analysis of the protocol can be found on the ASERT blog [here](#).





RUSSIA

Russian APT operations largely target government or government-affiliated networks.

Specifically in the following areas:

- Geopolitical workings of its neighboring states
- Western, NATO, and democratic encroachment in Eastern Europe and the military campaign in Syria
- Russian annexation of the Crimea in Ukraine
- Espionage operations against major players of interest

ASERT also tracked some disinformation domains of known Russian origin, which tend to rise and fall as current events and priorities change. Russia stands accused of meddling in the elections of up to 27 countries over the past decade. Bloomberg reports that European Union officials are already bracing for Russian cyberattacks and disinformation campaigns ahead of the spring 2019 elections of its member states.

.....

Fancy Bear is using multiple languages to write the same tools. Zebrocy, a downloader and backdoor tool, has been seen writing in Delphi, C#, VB.NET, Go.⁶

Cannon, a custom email-based C2 channel leveraged by the group, is written in both C# and Delphi.⁷

Fancy Bear's double agent LoJax UEFI writing module was found in the wild by ESET researchers.⁸

Fancy Bear, APT28, or Sednit

This APT group employed legitimate UEFI rootkit software to establish a backdoor on victim machines. The malicious files, originally classified as "unwanted software" by anti-virus vendors, avoided detection by minimally tweaking the software to phone home to the attacker C2 servers without changing any functionality within the software itself. Notably, systems compromised by LoJax could also be monitored in real time by the group. The nature of the hijacked software allowed the geo-location of the infected machine.

This type of targeting serves the purpose of potentially finding and following high-value targets and gaining access to potentially sensitive materials on compromised computers. ASERT tracked the infrastructure using custom fingerprints and identified live, active attacker controlled C2 servers. We found this group heavily targeting government entities around the world. In October, the U.S. Department of Justice issued indictments against members of this group, claiming that: "...beginning in or around December 2014 and continuing until at least May 2018, the conspiracy conducted persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government."

VIETNAM

First seen in 2012, Vietnamese APT operators have flown below the radar until recently. Vietnam currently has at least three APT groups, two of which are rarely seen operating beyond Vietnam's neighbors.

Targeting activity suggests espionage motivations and the desire to gain insight into strategic foreign relations. Tension in the South China Sea drives a substantial portion of the espionage activity, particularly around the Spratly Islands. China, Taiwan, Malaysia, Philippines, and Vietnam all occupy some portion of the islands and lay claim to the area.

Ocean Lotus or APT32

The most visible and well-known of the Vietnamese APT groups, Ocean Lotus updates TTPs frequently and uses increasingly sophisticated tradecraft and customized malware. Analyzing a number of the group's malware samples and phishing campaigns, ASERT found that they often showcased themes designed to target foreign governments of Southeast Asia, dissidents, journalists, and anyone with business or strategic interests in Vietnam. Most interesting, however, was that ASERT saw substantial internal activity where Vietnamese victim machines attempted to phone home to a known C2 infrastructure owned by Ocean Lotus, suggesting the group also focuses on internal targeting.

PoisonVine, APT-C-01, or PoisonIvy Group

Active for years, this group specializes in conducting cyber espionage campaigns against key national Chinese agencies, including defense, government, science, technology, academic, and maritime. The group primarily focuses on the military industry, Chinese strategic relations, cross-strait issues with Taiwan and China, and ocean-related fields. ASERT observed additional activity targeting government, academic, finance, and non-profit sectors.



PoisonVine utilizes RATs that can detect the presence of anti-virus based upon how the AV simulates the windows API call 'GetClientRect'.⁹



DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

While primarily motivated by intelligence gathering and intellectual property theft, North Korean APT groups are also known for destruction and fundraising to support the regime, which is rather rare among APT groups.

STOLEN PENCIL Campaign

As reported in a December 2018 blog post, ASERT discovered a campaign of probable DPRK-origin targeting universities.¹⁰ ASERT saw massive credential theft across four universities, where all of the compromised targets were in the mechanical engineering field and focused on biomedical research. One victim was a member of a Pacific-region policy non-profit. ASERT research uncovered a far-reaching campaign resulting in ongoing collaboration with industry professionals around the world.

DPRK utilized a browser plugin in the STOLEN PENCIL campaign, going so far as to leave reviews on the plugin from compromised accounts in a likely effort to establish legitimacy.

CRIMEWARE

Financially motivated threat actors rely on crimeware: malware intended to loot the victim's bank account or steal victim data to exploit for money. For crimeware actors, the key word is more: more groups, more attack monetization, more businesslike methods, and certainly more — and better — tools. We are seeing new attacks from additional groups, often using increasingly sophisticated and persistent malware coupled with innovative techniques that target an expanded set of targets.

KEY FINDINGS INCLUDE

- Once plugged in to the internet, IoT devices are attacked within five minutes and targeted by specific exploits within 24 hours.
- Actors grew ever more sophisticated and efficient at monetizing malicious attacks using modular, persistent crimeware that provides a better ROI than a simple smash-and-grab method.
- Crime campaigns like DanaBot increased distribution efficiency and cut labor costs by using an affiliate model that encourages specialization among threat actors and substantially increases the pool of potential victims across the world.
- The overall lifetime of crimeware infections sometimes lasts years, long after an infrastructure goes offline.
- Several strains of IoT malware showed a marked increase in design sophistication.
- Cyber threat actors learned from IoT malware, pivoting to add Linux servers to their targets.



DANABOT'S AFFILIATE
MODEL FUELED GLOBAL
PROLIFERATION IN ONLY

8 MONTHS

.....
ONCE PLUGGED INTO THE
INTERNET, IoT DEVICES
ARE ATTACKED WITHIN

5 MINUTES

CRIMEWARE HIGHLIGHTS

Crimeware actors primarily deliver malicious code via weaponized emails containing either booby-trapped documents or classic social engineering.

In late 2018, we saw a growing array of crimeware morph into modularized frameworks, adding functionality to increase the monetization of infection beyond a simple smash-and-grab. Common modules include spam delivery, password theft, or cryptocurrency mining. Much like the old story of the camel with its head in the tent, that first successful incursion into a victim's machine is only the initial step. More often than not, cyber adversaries use the original foothold as an avenue to leverage many different malware payloads to further infect and exploit their victims.

Crimeware families wax and wane in popularity as features become available and infrastructure changes hands in underground marketplaces (Figure 1). Among the hundreds of malware families tracked by ASERT, we observed spikes in families like IcedID, often delivered by Emotet, and DanaBot, a modular malware framework first discovered in May 2018.¹¹ Simultaneously, we observed a significant decrease in established families like Panda Banker, an offshoot of the classic Zeus malware family.

Sample Intake by Month

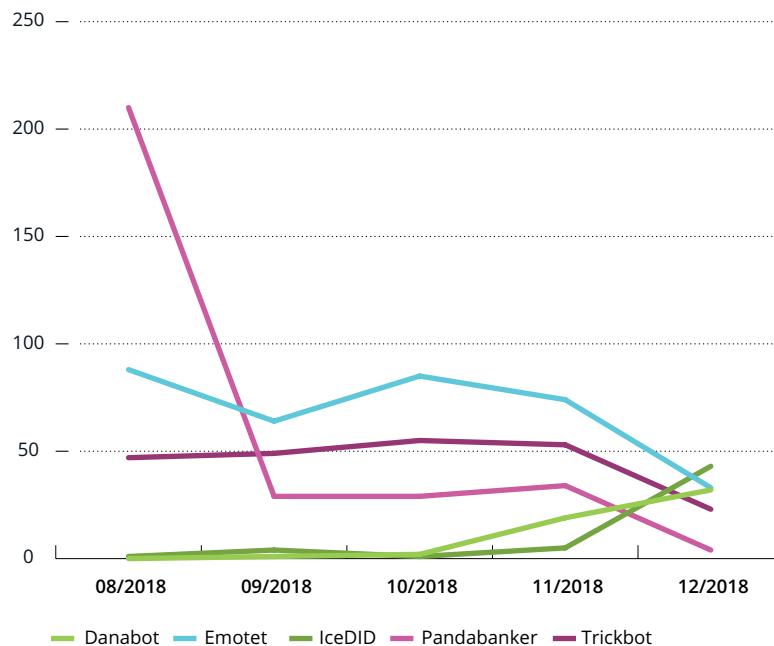
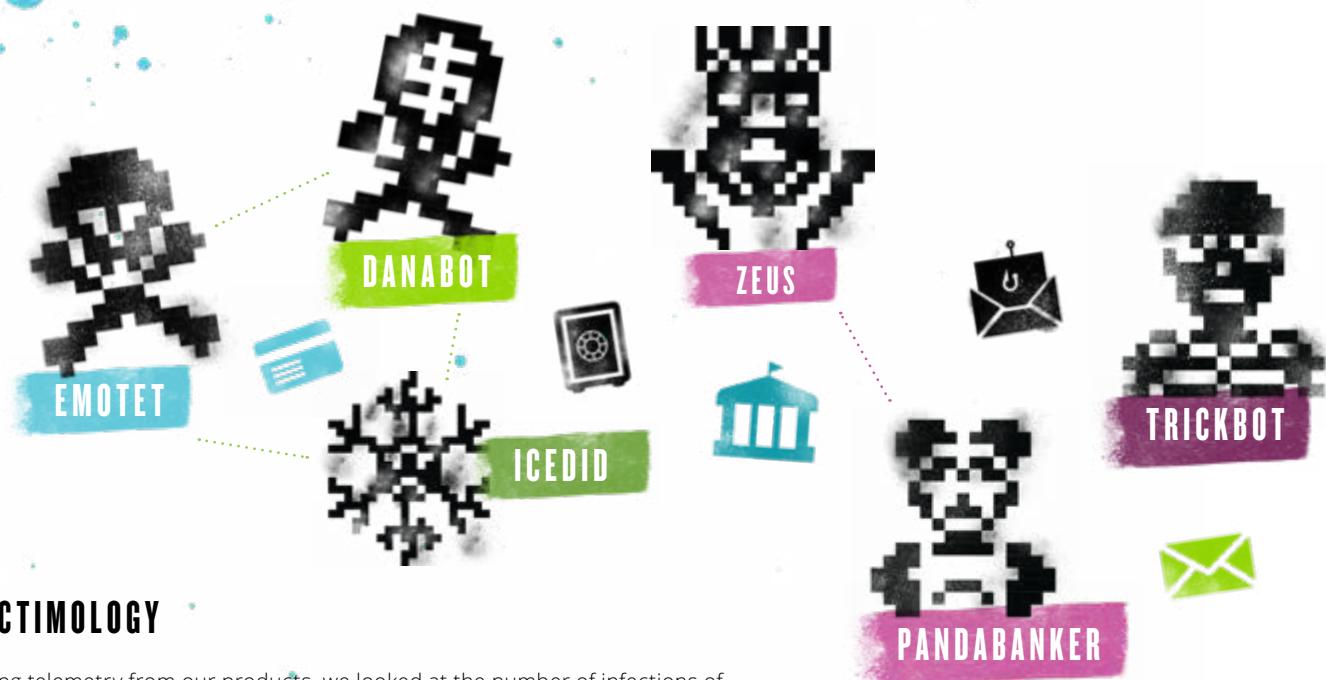


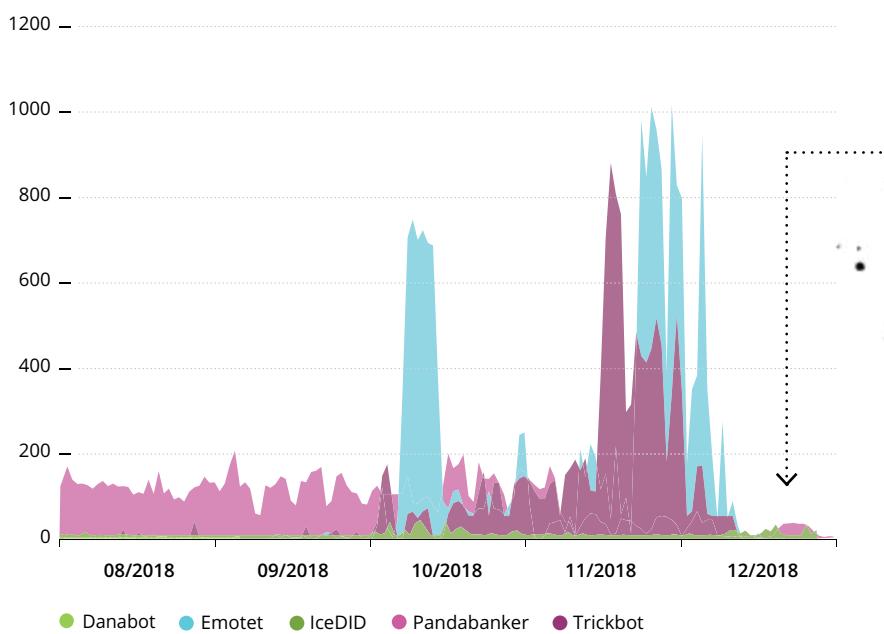
Figure 1: Sample Intake by Month



VICTIMOLOGY

- Using telemetry from our products, we looked at the number of infections of common crimeware families during the last half of 2018. Victim geography is widespread, as crime actors typically aim for broad dispersion in order to get maximum effect.
- Zeus-derived bankers like Panda Bot remained ever-present, but bankers and downloaders like TrickBot and Emotet took center stage in the fall of 2018. Leading up to the middle of December, the noticeable drop-off in attacks likely represents computers going offline for the holiday season.

Infections by Day



The noticeable drop-off in attacks likely represents computers going offline for the holiday season.

Figure 2: Infections by Day



Affiliate ID	Targeted Countries	First Seen
3	Austria, Italy	9/6/2018
4	Australia	9/24/2018
8	Canada, US	9/11/2018
9	Austria, Germany, Italy, Poland, US	9/15/2018
12	Australia	9/26/2018
13	Germany	9/29/2018
15	Poland, US	11/21/2018

CRIMEWARE GOES TO B-SCHOOL

As shown in a December blog post, the DanaBot crimeware family exemplifies the criminal underground's increasing tendency to operate like a regular business. For crimeware operators to make money, they need to distribute their malware as widely as possible, maintain a C2 infrastructure, and cash out by converting banking credentials to hard cash. Each of these requires a separate skill set, creating an opportunity for threat actors to provide specialized services to the underground.

While the DanaBot authors maintain the centralized C2 infrastructure, they outsource the distribution of the malware to third-party affiliates. The affiliate model works using a tokenization method that allows the owners to maintain oversight on the botnet. The affiliates handle malware installation and cashing out, accepting the bulk of the risk themselves.

This affiliate model promotes a much broader reach of potential victims. With the distribution of labor, threat actors no longer need to single-handedly target bank accounts in multiple countries. By outsourcing installation of the malware via affiliates, DanaBot gained a global foothold in the latter half of 2018 (Figure 3).

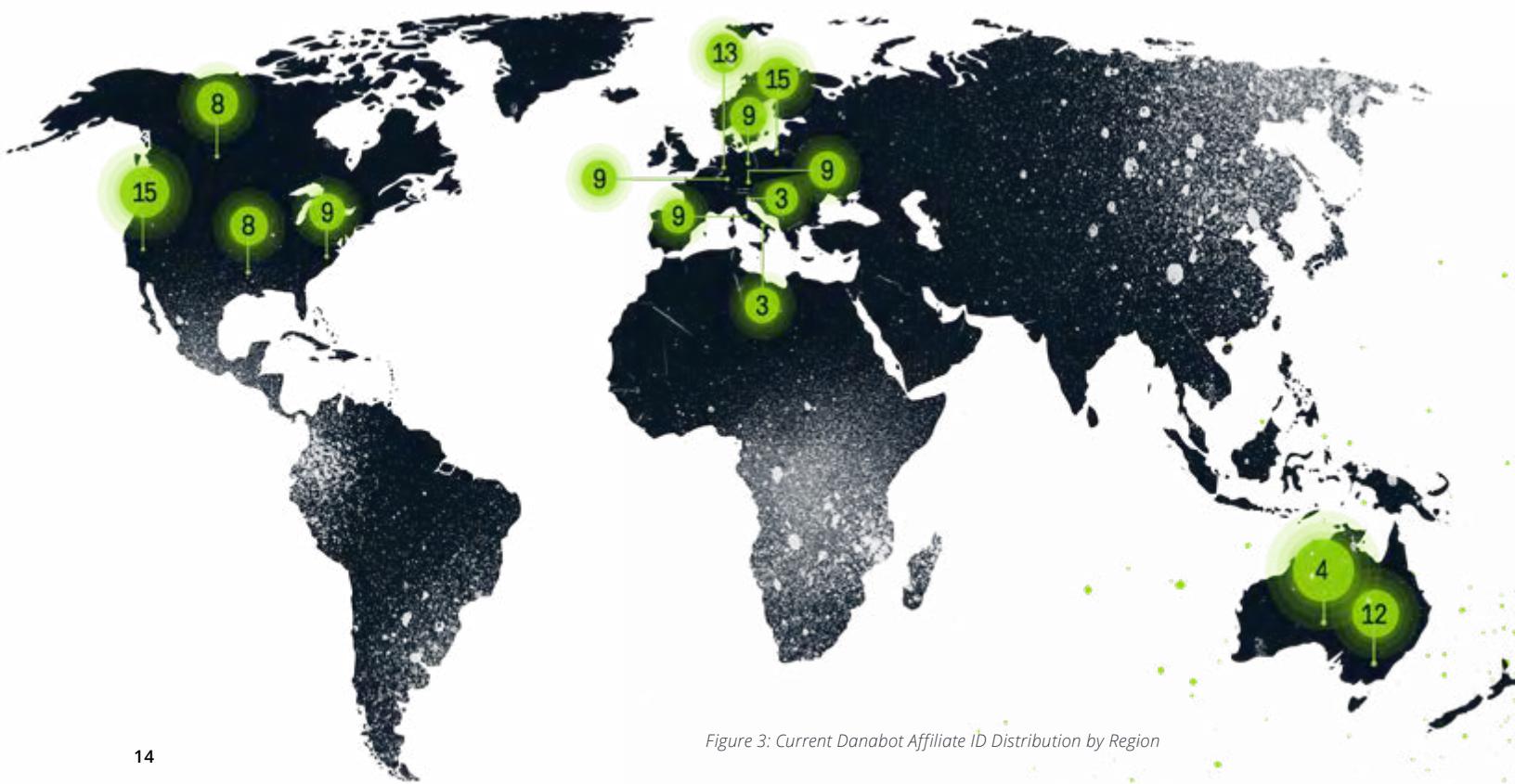


Figure 3: Current Danabot Affiliate ID Distribution by Region

Neverquest Infections by Day

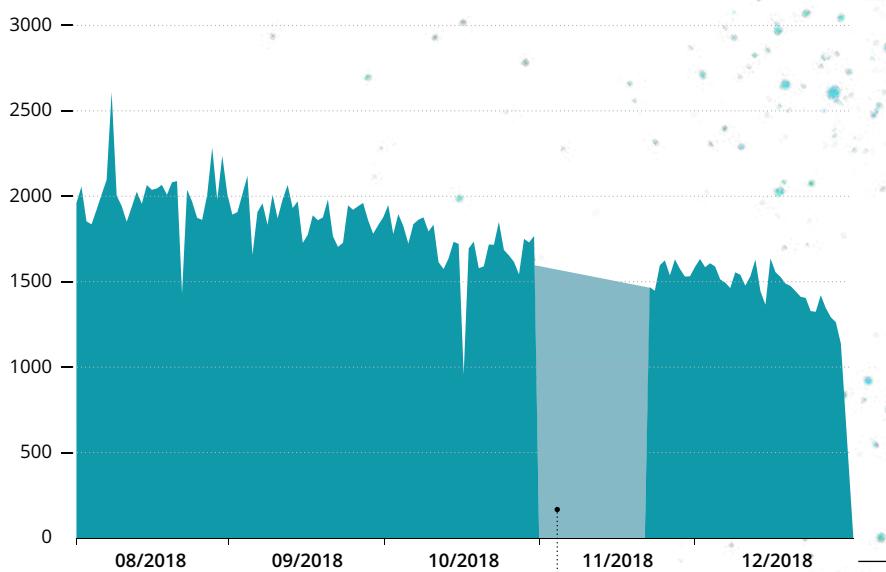


Figure 4: Neverquest Infections by Day

Estimated count due to gap in collection

If this many infections remain almost two years after being shut down, we can expect the malware we see today to remain an ongoing problem for security teams well into the future.

CRIMEWARE: NO EXPIRATION DATE

Malware infections tend to fester long past their official expiration dates. For example, the Neverquest banking Trojan officially ended in 2017 when authorities shut down this once-thriving criminal enterprise. And yet, it's still out there. A malware sinkhole ASERT maintains continues to see almost 2,000 daily check-ins to Neverquest C2 sites that we registered prior to Neverquest's demise (Figure 4). As remediation or forced attrition eliminates the threat from victim machines, over time the number of infections has declined.

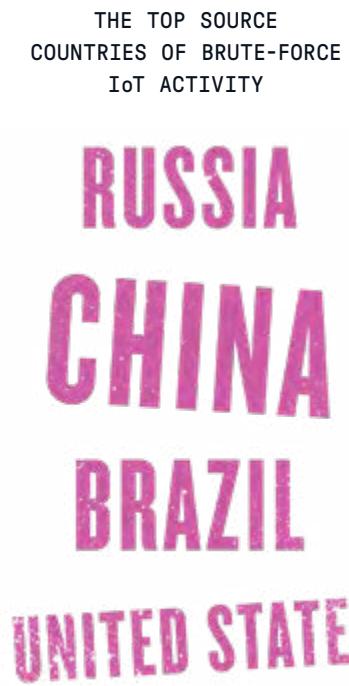
The longevity of these malware infections requires security defenders to remain vigilant long after the apparent threat subsides. Though we've yet to uncover adversaries registering expired domains to capitalize on ongoing infections, it is possible that attackers have leveraged this tactic, gaining easy access to sensitive data.



BANKING TROJAN

NEVERQUEST

WAS SHUT DOWN BY
AUTHORITIES IN 2017,
BUT MALWARE INFECTION
STILL LINGERS



IoT

IoT devices are constant targets of DDoS malware. They can sit for months in a warehouse or on a store shelf, waiting to be brought home and plugged into a network. Once they are plugged in, our research shows IoT devices will be targeted with a brute-force attack of common backdoor usernames and passwords within five minutes. Within hours, they will be subject to common exploits.¹²

We use our global network of IoT honeypots to monitor brute-force and exploit activity. Brute-forcing happens when IoT malware continuously attacks random targets via the antiquated Telnet protocol, running through lists of common factory-default usernames and passwords until they succeed and can deliver the malware to the victim device. The top source countries of brute-force IoT activity are Russia, China, Brazil, and the United States.

As highlighted in an October 2018 blog post, we've compiled a list of the most common username and password combinations used by IoT malware (Figure 6). While there is some regional affinity, the list is composed exclusively of hardcoded credentials for many common classes of IoT devices, such as web-enabled cameras and home routers.¹³

Mirai remains the king of IoT malware. Since the authors of Mirai released the source code in late 2016, threat actors tweaked the infection mechanisms by adding new usernames/passwords and exploits, as well as DDoS attack techniques.

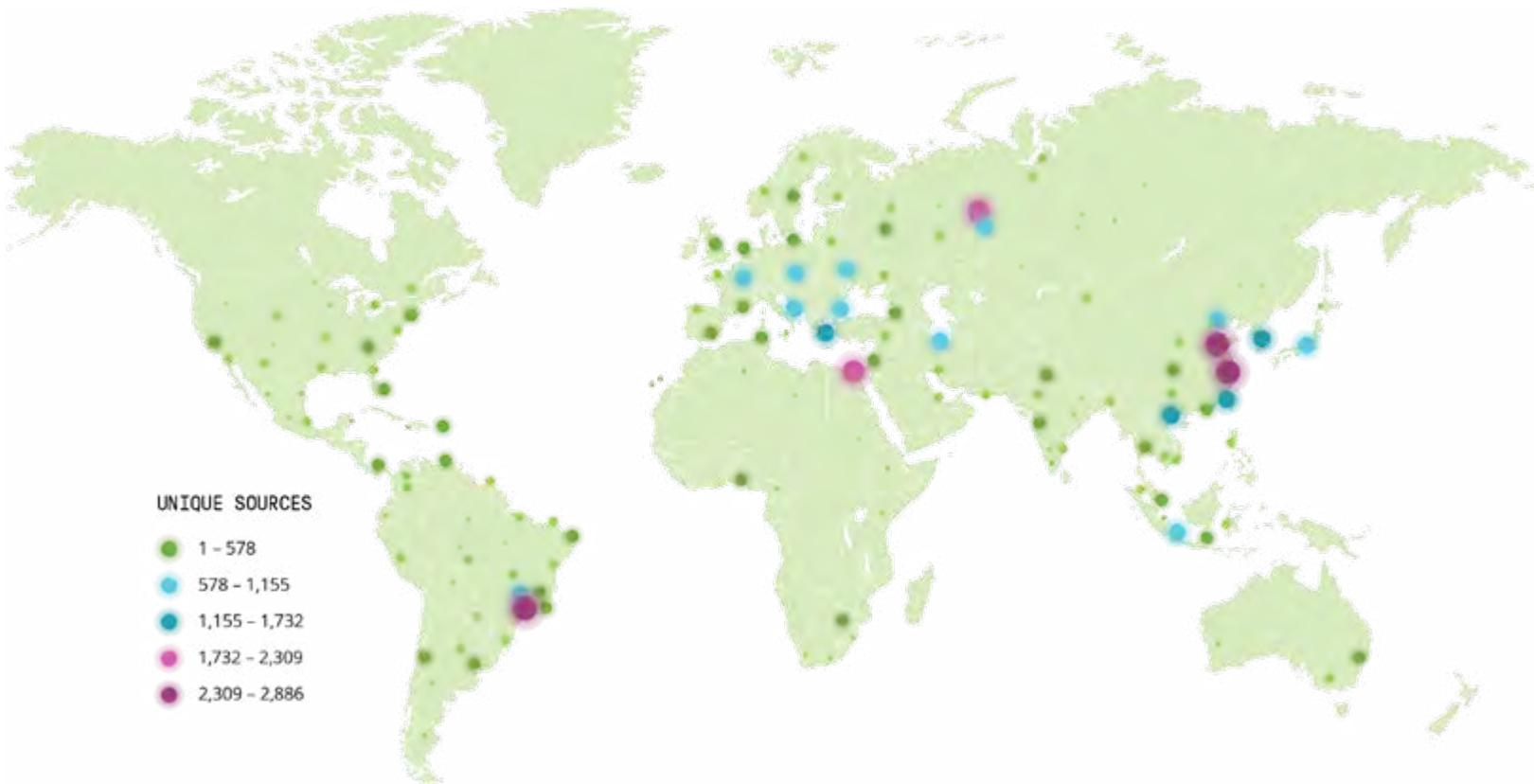


Figure 5: Brute-Force IoT Activity by Country

Common Username and Password Combinations

user_pass: Descending	Count
root/xc3511	198,171
support/support	159,661
root/123456	152,959
vstarcam2015/201	147,134
e8ehomeasb/e8ehomeasb	134,808
admin/admin	36,881
guest/12345	30,089
root/vizxv	25,783
root/admin	23,800
admin/1234	21,027

Figure 6: Common Username and Password Combinations



REMAINS THE KING
OF IoT MALWARE



ARE TWO NEW BREEDS
OF ADVANCED IoT BOTS

IoT MALWARE TRENDS

There are two trends in IoT malware we've seen in the latter half of 2018. First, there are several particularly interesting tactics hidden within the onslaught of Mirai variants. Earlier in the year, we saw an advanced threat actor use a malware named VPNFilter to target specific home routers. It was delivered in multiple stages with a modularized payload, a level of sophistication not seen before in IoT malware.

We also observed Torii, which like VPNFilter, is a part of a new breed of advanced IoT bots that deviate from using Mirai as its framework. Instead, Torii leverages a dropper to install and establish persistence, an unusual technique for IoT bots. Torii uses its own encryption scheme to communicate with its C2 and uses TCP port 443 as an evasion tactic. While most IoT botnets ship with pre-canned DDoS attacks, Torii focuses on data exfiltration. Torii is also built to be modular in nature, as it contains the ability to download files and execute remote commands.

Secondly, threat actors are learning from their experience with IoT malware to target known vulnerabilities on Linux servers in the data center. For instance, the Hadoop YARN vulnerability was initially used to deliver DemonBot, a DDoS malware, to IoT devices. Soon after, threat actors used the vulnerability to install Mirai on Linux servers, blurring the line between IoT and server malware.

DDoS TRENDS

FROM SECOND HALF 2017
TO SECOND HALF 2018...

GLOBAL ATTACK
NUMBERS INCREASED

▲ 26%

GLOBAL MAX DDoS
ATTACK SIZE INCREASED

▲ 19%

LARGEST DDoS
ATTACK ON RECORD

1.7 TBPS

MITIGATED BY NETSCOUT
IN MARCH 2018

EXPLOSIVE GROWTH IN THE
100–400 GBPS
ATTACK RANGE

A foundational element of the threat landscape, the DDoS sector continues to reflect the indefatigable efforts of a busy and ever-more organized community of bad actors. The latter half of 2018 saw everything from state actors trying to influence geopolitical processes to an increasingly businesslike DDoS service-for-hire community.

In turn, that has led to a skyrocketing diversification of attack avenues, methods, and techniques, wiping away traditional expectations around both DDoS attack mechanisms and defense practices. Gone are the days where a single bot offered a simplistic DDoS attack type. In today's DDoS threat landscape, attackers increasingly add diversification into their bots, allowing for a wide variation of attacks and protocols to take down networks.

KEY FINDINGS

- Attack numbers were up 26 percent while attacks in the 100–200 Gbps, 200–300 Gbps, and 300–400 Gbps exploded, up 169 percent, 2,500 percent, and 3,600 percent, respectively.
- Capitalism is alive and well in the DDoS attack economy, which is growing ever more sophisticated and efficient at monetizing malicious attacks.
- There was an increasing accessibility of attack vectors that were once the province of sophisticated attackers, such as the large increase in carpet-bombing DDoS attacks observed in 2018.¹⁴ A new variant of the reflection-type attacks, carpet-bomb attacks take aim at entire subnets or CIDR blocks rather than focusing on specific target IPs. Due to the rapid weaponization of new attack types and inclusion into Booter/Stresser services, these attacks are now becoming more prevalent.
- Western governments and authorities are collaborating with private sector security experts in law enforcement action against DDoS infrastructure. ASERT supported the investigation into the MedusaHTTP botnet, which ultimately led to an indictment of the malware author by the US Department of Justice.



VERTICAL INDUSTRIES

- There was a significant increase in DDoS attacks related to wireless telecommunications, satellite telecommunications, data processing, data hosting, television broadcasting, libraries, and archives.
- We also saw a greater than 10,000 percent increase in the size of DDoS attacks targeting marketing research and public opinion polling. This is consistent with residual telemetry we've seen in which DDoS attacks coincide with geopolitical events.
- In the second half of 2018, we observed a significant increase in DDoS attacks against colleges, universities, professional schools, and educational services of between 115 percent to 525 percent, with a max attack size of 113 Gbps.
- There was also a massive increase in attacks targeted at the scheduled passenger air transportation sector in the latter part of 2018. The size of attacks increased by more than 15,000 percent, bringing the max attack size to 245 Gbps.
- The max DDoS attack size increased more than 1,000 percent for targets such as specialized design services, various computer-related and programming services, and advertising and related services.

In today's DDoS threat landscape, attackers increasingly add diversification into their bots, allowing a wide variation of attacks and protocols to take down networks.

DDoS ATTACK TRENDS

Although the number of DDoS attacks increased year over year by about 26 percent, the dominant story continued to be about attack size.

The second half of 2018 saw a continuation of the overall trend toward larger attacks. The global max DDoS attack size grew by 19 percent in the second half of 2018 as the era of internet-scale attacks continued to gain traction.

In this potent new strategy, threat actors launched strategic campaigns that compromised and used a vast array of devices related solely by internet connectivity.

While we continued to see a steady uptick in attacks greater than 400 Gbps in the second half of 2018, it was accompanied by an explosion of attacks at the lower end of the large attack range. (The small big attacks, so to speak.) The number of overall attacks in the 100–200 Gbps range increased by 169 percent; meanwhile, attacks in the 200–300 Gbps and 300–400 Gbps range grew by an astounding 2,500 percent and 3,600 percent, respectively.

In our estimation, the increases across such a wide range likely reflect the continued monetization of the threat landscape. As DDoS-for-hire grows in accessibility and affordability, we expect Booter/Stresser services to further proliferate and diversify. While these tools are not necessarily new, the ease of access, quick iteration of new attack types, and a broader range of international customers will result in lots of amateur cybercriminals getting hold of destructive malware. And it will result in a wider array of organizations being targeted for any number of reasons. Law-enforcement action against such services and their users, as we've seen recently, are the main counterbalance to their otherwise inexorable rise.

Global DDoS Attack 2H 2017 and 2H 2018 Number of Attacks by Region

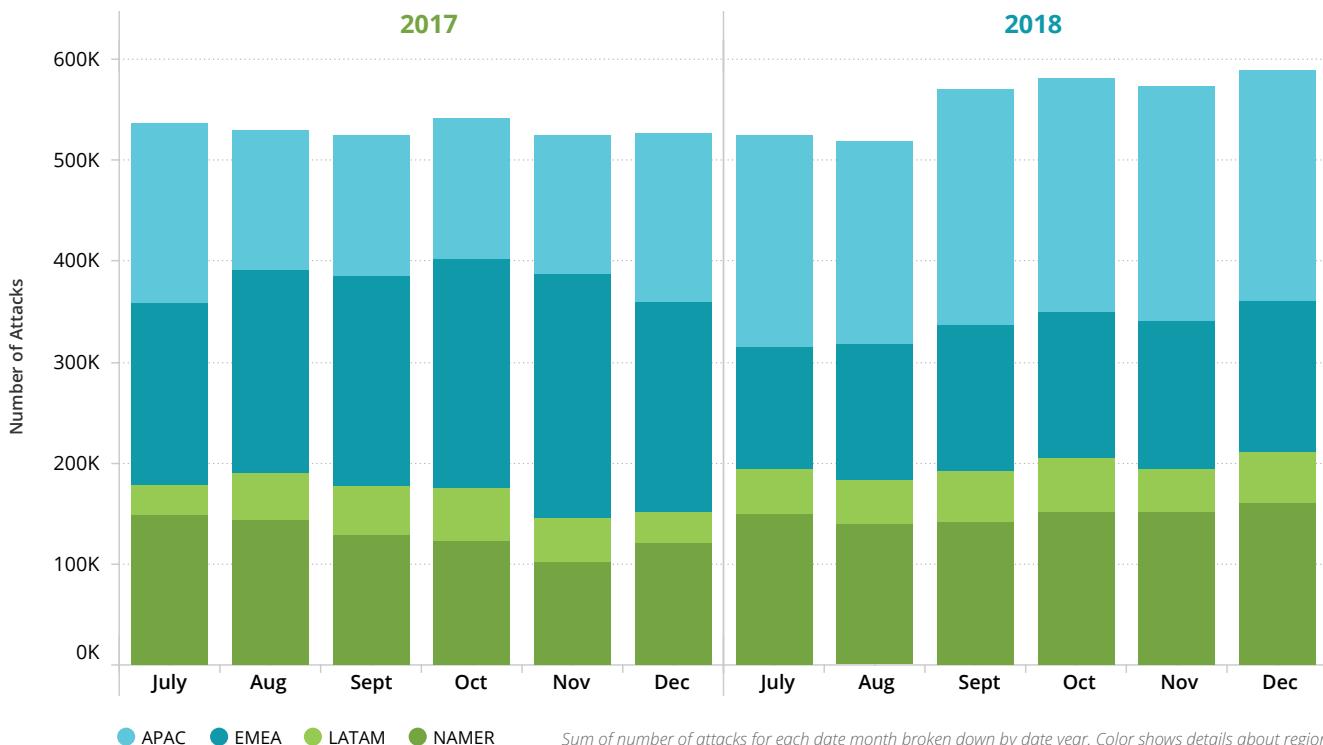


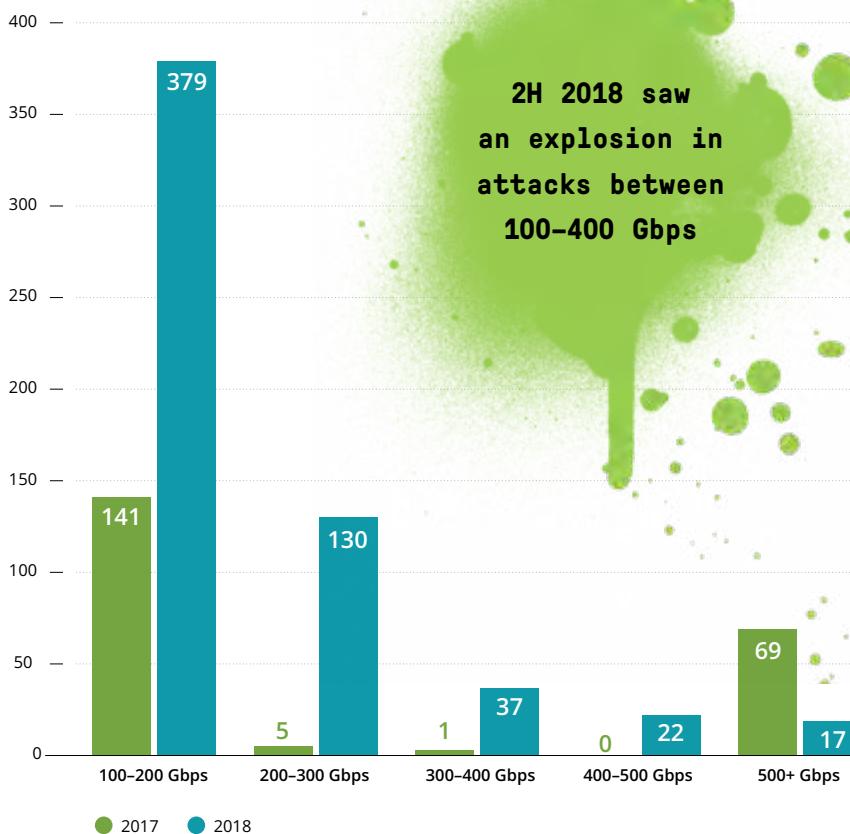
Figure 7: Global DDoS Attack 2H 2017 and 2H 2018 Number of Attacks by Region

REGIONAL ATTACKS

In the second half of 2018, We saw a significant increase in attack numbers across regions, with the exception of EMEA, where attack numbers fell by a third.

Once again, the APAC region showed disproportionate growth, as the number of attacks nearly doubled. In comparison, Latin America and North America saw an increase of 15 percent and 16 percent, respectively.

EMEA saw a 364 percent increase in attacks between 100–300 Gbps. Asia Pacific and North America also saw significant increases of attacks in that range. APAC again came under heavy fire when it came to large attacks, experiencing 37 attacks over 400 Gbps, as compared with two in EMEA and none in Latin America and North America.



GLOBAL

INCREASE IN ATTACKS
100-200 GBPS

141 ► 379
ATTACKS IN 2H 2017 ATTACKS IN 2H 2018

▲ 169%
GROWTH

INCREASE IN ATTACKS
200-300 GBPS

5 ► 130
ATTACKS IN 2H 2017 ATTACKS IN 2H 2018

▲ 2,500%
GROWTH

ASIA PACIFIC

INCREASE IN ATTACKS
GREATER THAN 300 GBPS

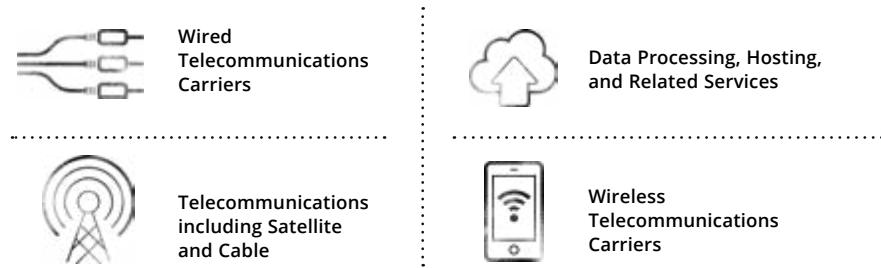
0 ► 70
ATTACKS IN 2H 2017 ATTACKS IN 2H 2018

Figure 8: Global Growth in Large Attacks 2H 2017 vs. 2H 2018

VERTICAL INDUSTRY ATTACKS

We analyzed attack data by North American Industry Classification System (NAICS) codes, which groups companies into 22 broad categories that contain multiple large sub-vertical sectors. Comparing second-half data from 2017 to 2018 for the top ten most-targeted sectors, we found significant shifts in targets and an overall growth in attack size and numbers.

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



It's not surprising to find that telecommunications providers observed the overwhelming majority of attacks, as did data hosting services (which includes cloud providers). This is inherent to their role as connectivity providers, with attacks focused on their residential and business subscribers as well as their operational infrastructures.

However, there were some variations year over year that illustrated the ongoing increase in attack size, as well as a rising line of attack numbers for a diverse range of vertical sectors.

The top two most attacked targets all experienced significant increases in attack numbers, while the max attack size decreased for Wired Telecommunications Carriers and Telecommunications by 10 percent and 19 percent, respectively. Meanwhile, Data Processing, Hosting, and Related Services (including cloud providers) saw an 83 percent increase in the number of attacks year over year, as well as a 198 percent increase in max attack size. With cloud service providers hosting an increasingly large amount of valuable data, this makes sense. On the other hand, wireless telecommunications carriers actually saw a decrease of 29 percent in attack numbers.

The sub-vertical sector Custom Computer Programming Services — which includes system integrators and consulting houses — saw a 198 percent increase in attack numbers. Meanwhile, its max size attack of 186.2 Gbps was 1,043 percent larger than in 2017.

PASSENGER AIR TRANSPORTATION



The ASERT team continued to observe significant interest from malicious actors in the International Affairs sub-vertical, which jumped up five spots year over year. Attack numbers for this group grew 186 percent. This sector includes consulates, embassies, the International Monetary Fund, the State Department, and the United Nations. We see the growth in this sector as illustrative of increased activity from actors with politically motivated agendas, including nation-state groups and governments.



INTERNATIONAL AFFAIRS

ATTACK NUMBERS

▲ 186%

ATTACK GROWTH OUTSIDE OF THE TOP TEN TARGETS



Cloud Service Providers

Data Processing, Hosting, and Related Services—aka cloud service providers—occurred in 2H 2018, with an 83 percent increase in the overall number of attacks and a 365 percent increase in max attack size.

MAX ATTACK SIZE ▲ 365%



Market Research and Public Opinion Polling

2H 2018 saw a greater than 10,000 percent increase in the size of DDoS attacks targeted at marketing research, and public opinion polling. This is consistent with residual telemetry we've seen in which DDoS attacks coincide with geo-political events.

MAX ATTACK SIZE ▲ 10,000%



Gambling Industry

The gambling industry saw a 2,200 percent increase in DDoS attack size in 2H 2018, with a max attack size of 8 Gbps as opposed to 344 Mbps in 2H 2017.

MAX ATTACK SIZE ▲ 2,200%



Design Services

Max DDoS attack size increased 1,600 percent targeting specialized design services, various computer related and programming services, and advertising and related services.

MAX ATTACK SIZE ▲ 1,600%



Civil Engineering

Heavy and civil engineering services saw a nearly 2,000 percent increase in DDoS attack size.

MAX ATTACK SIZE ▲ 2,000%



Hospitals and Doctors Offices

Attacks against hospitals and physicians' offices increased between 300 percent to 1,400 percent with max attack sizes between 122 Gbps and 137 Gbps.

MAX ATTACK SIZE ▲ 1,400%

TOP VERTICALS TARGETED BY DDoS ATTACKS

2H 2017

1



WIRED TELECOMMUNICATIONS CARRIERS

# OF ATTACKS	MAX ATTACK	CATEGORY
742,886	386.4 Gbps	Information

2



TELECOMMUNICATIONS

# OF ATTACKS	MAX ATTACK	CATEGORY
421,556	250.1 Gbps	Information

3



DATA PROCESSING, HOSTING + RELATED SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
239,866	83.6 Gbps	Information

4



WIRELESS TELECOMMUNICATIONS CARRIERS

# OF ATTACKS	MAX ATTACK	CATEGORY
193,463	104.7 Gbps	Information

5



OTHER TELECOMMUNICATIONS

# OF ATTACKS	MAX ATTACK	CATEGORY
19,053	115.8 Gbps	Information

6



EDUCATIONAL SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
14,686	18.1 Gbps	Educational Services

7



PROFESSIONAL, SCIENTIFIC + TECHNICAL SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
14,073	3.4 Gbps	Professional, Scientific, and Technical Services

8



SOFTWARE PUBLISHERS

# OF ATTACKS	MAX ATTACK	CATEGORY
8,030	77.7 Gbps	Information

9



COLLEGE, UNIVERSITIES, PROFESSIONAL SCHOOLS

# OF ATTACKS	MAX ATTACK	CATEGORY
7,595	31.2 Gbps	Educational Services

10



INTERNATIONAL AFFAIRS

# OF ATTACKS	MAX ATTACK	CATEGORY
7,582	20.9 Gbps	Public Administration

2H 2018

1



WIRED TELECOMMUNICATIONS CARRIERS

# OF ATTACKS	MAX ATTACK	CATEGORY
889,860	346.6 Gbps	Information

2



TELECOMMUNICATIONS

# OF ATTACKS	MAX ATTACK	CATEGORY
480,543	202.8 Gbps	Information

3



DATA PROCESSING, HOSTING + RELATED SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
440,133	388.5 Gbps	Information

5



WIRELESS TELECOMMUNICATIONS CARRIERS

# OF ATTACKS	MAX ATTACK	CATEGORY
137,939	371.7 Gbps	Information

6



INTERNATIONAL AFFAIRS

# OF ATTACKS	MAX ATTACK	CATEGORY
21,700	27.8 Gbps	Public Administration

7



PROFESSIONAL, SCIENTIFIC + TECHNICAL SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
20,656	20.1 Gbps	Professional, Scientific, and Technical Services

8



EDUCATIONAL SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
19,076	113.0 Gbps	Educational Services

9



COLLEGE, UNIVERSITIES, PROFESSIONAL SCHOOLS

# OF ATTACKS	MAX ATTACK	CATEGORY
18,388	68.9 Gbps	Educational Services

10



SOFTWARE PUBLISHERS

# OF ATTACKS	MAX ATTACK	CATEGORY
12,266	25.4 Gbps	Educational Services

10



CUSTOM COMPUTER PROGRAMMING SERVICES

# OF ATTACKS	MAX ATTACK	CATEGORY
11,313	186.2 Gbps	Professional, Scientific, and Technical Services

DDoS HIGHLIGHTS

CARPET BOMBING

The majority of DDoS attacks are launched using attack vectors which have been around for a long time. As the majority of enterprises (and even some internet service providers) lack even the most rudimentary DDoS protection, a 15-year-old attack like TCP SYN flood, or a simple NTP reflection flood, is sufficient to take these organizations offline.

However, as attackers often focus on high impact targets that take DDoS defense seriously, they constantly evolve new attack vectors designed to bypass or take advantage of limitations or vulnerabilities in traditional DDoS defense solutions.

One of the attack vectors we've seen used since November 2017 is carpet bombing. This is a new variant of the more common reflection, or flooding, attacks. Instead of focusing the attack on a single destination, the attacker targets every destination within a specific subnet or CIDR block (for example, a /20). Doing so makes it harder to detect and mitigate the attacks, and the flood of attack traffic across network devices and internal links can potentially cause outages. These attacks are often fragmented, resulting in a flood of non-initial IP fragments (Figure 9). This will often happen when the attacker is using UDP reflection attacks. This results in an attack that can be tricky to mitigate as the non-initial fragments don't contain any information from the UDP header, such as the source port used in the attack.



NEW ATTACK VECTOR

CARPET BOMBING

NEW VARIANT OF REFLECTION,
OR FLOODING, ATTACKS

Carpet Bombing Overview

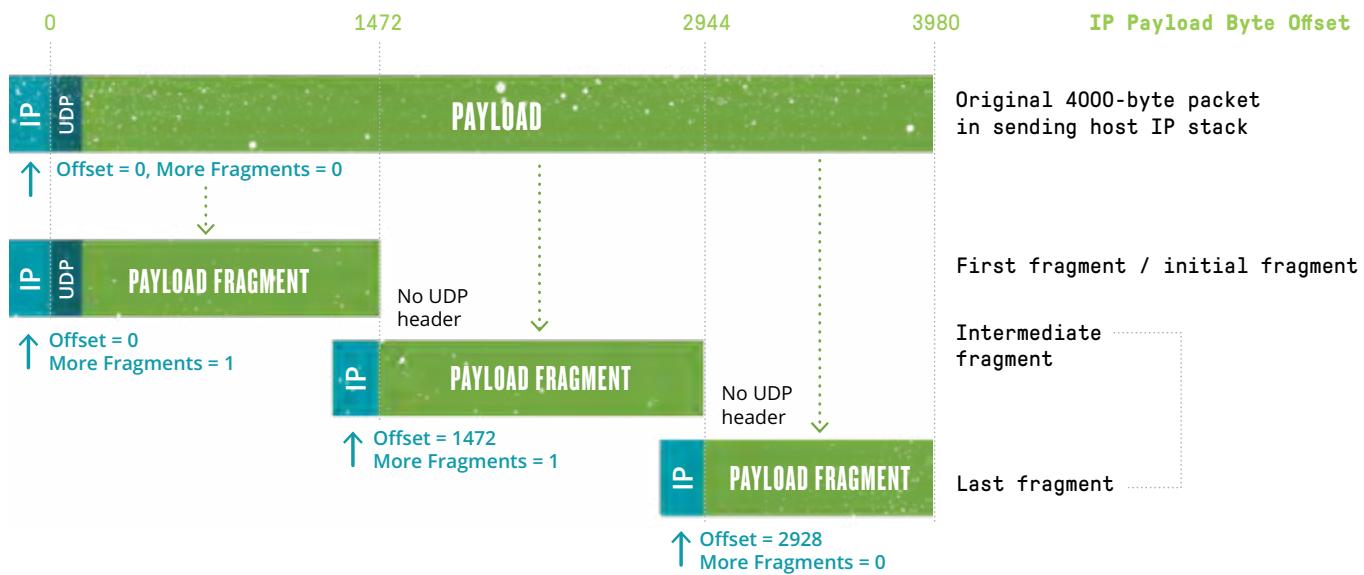


Figure 9: Carpet Bombing overview

9 OUT OF 12

ATTACK TYPES LISTED
SHOW A SIGNIFICANT
INCREASE IN NUMBER
OF ATTACKS

mDNS AMPLIFICATION

ATTACKS INCREASED

▲ 233%

MAX ATTACK SIZE

8.28 ➤ 186
GBPS GBPS

IN 2H 2017

IN 2H 2018

SSDP AMPLIFICATION

NUMBERS INCREASED

▲ 55%

In addition, the attacker will often shift their attacks from one subnet (or CIDR block) to another, complicating the detection and mitigation even further.

Detecting carpet bombing attacks requires a slightly different technique. Traditional flow-based detection that focuses on specific destination IP addresses will usually not work, as the attack traffic will be spread across all IP addresses in the networks under attack. Instead, companies must analyze traffic volumes crossing network boundaries or traversing specific network devices as this will show the broader attack volume. Network traffic should therefore be profiled and average volumes measured on a regular basis to understand what normal traffic volumes look like, including typical spikes within them. These attacks can also be detected by profiling traffic to groups of resources or larger subnets within the network and then detecting anomalies over this traffic.

When it comes to mitigation, carpet bombing attacks use traditional DDoS reflection type attacks or flooding attacks, and can be mitigated using the same approaches:

- Traffic from unwanted source ports can be dropped or rate-limited using infrastructure access lists (iACL) or FlowSpec.
- The source IPs producing the attacks can be blocked using iACLs, FlowSpec or source-based, remote-triggered blackholing (S/RTBH).
- Non-initial fragments can usually be safely rate-limited down to low values (1 percent). For DNS replies, an exemption should be made for each DNS recursive infrastructure to avoid blocking large ENDSO replies. This can in some cases block up to 50 percent of the attack volume when dealing with fragmented attack traffic.
- Attack traffic can be diverted to IDMSs but care must be taken to not divert too large a chunk of the attack traffic. The total traffic (both legitimate and attack traffic) can be quite large when entire network blocks are diverted.

DIVERSIFIED ATTACK PORTFOLIOS

Everybody knows the benefits of a diversified stock portfolio — it minimizes risk while providing more than one revenue-generating avenue. The same principle can apply to DDoS attacks, and it seems that many in the Booter/Stresser community are doing just that. We saw a significant increase in both attack volume and size across a slew of less widely used attack types, as it appears that attackers branched out from the usual culprits like DNS, NTP, and Chargen (Figure 10). Nine out of 14 attack types showed a significant increase in number of attacks. The number of mDNS amplification attacks, for example, rose 233 percent, while the maximum size attack increased from 8.28 Gbps to 186 Gbps. At the same time the aforementioned attacks all declined in both attack numbers and max size. However, SSDP, another perennial favorite, bucked the decline tide with a 55 percent growth in numbers. That could well be due to the arrival of a new class of SSDP attack discovered by ASERT in 2018.¹ All told, this looks to us like a case of a growing community of professional DDoS-for-hire services finding ways to minimize risk and optimize ROI.

Reflection Amplification Stats

ATTACK TYPE	2017 2H	2018 2H	2017 2H Attack Size	2018 2H Attack Size
DNS Amplification	307,810	251,355	529 Gbps	388 Gbps
NTP Amplification	235,550	206,586	529 Gbps	260 Gbps
SSDP Amplification	51,501	79,960	528 Gbps	287 Gbps
Chargen Amplification	47,223	22,150	157 Gbps	128 Gbps
TCP SYN/ACK Amplification	1,546	21,628	77.9 Gbps	156 Gbps
SNMP Amplification	13,293	18,523	158 Gbps	210 Gbps
rpcbind Amplification	640	9,011	53.3 Gbps	121 Gbps
memcached Amplification	3,700	5,125	43.9 Gbps	245 Gbps
mDNS Amplification	485	1,616	8.28 Gbps	186 Gbps
MS SQL RS Amplification	437	1,593	105 Gbps	75.8 Gbps
NetBIOS Amplification	51	856	24.4 Gbps	121 Gbps
RIPv1 Amplification	68	293	21.2 Gbps	64.7 Gbps
TOTALS	658,651	716,437		

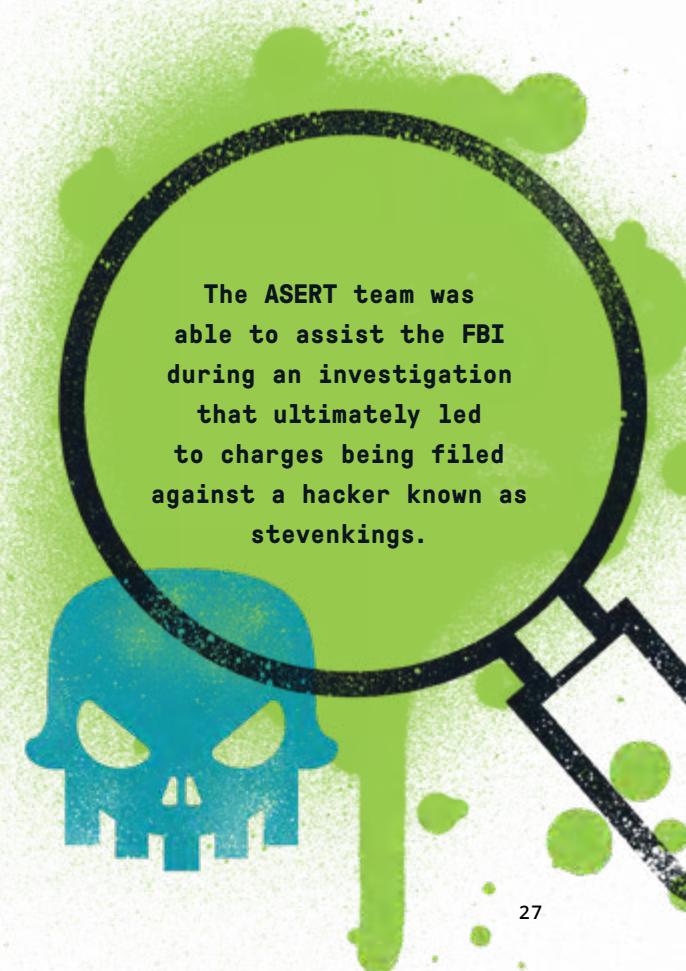
Figure 10: Reflection Amplification Stats

CRACKDOWN ON CYBERCRIME

After posting research on MedusaHTTP DDoS, a botnet from a hacker known as stevenkings,¹³ the ASERT team was able to assist the Federal Bureau of Investigation (FBI) during an investigation that ultimately led to charges being filed.¹⁴ Such collaborative cybercrime-fighting efforts are on the rise. For example, in December 2018, international crime-fighting agencies joined forces with the FBI to take down 15 DDoS-for-hire services, charging three men with criminal hacking in the process.² In April, a group of agencies worked with the Dutch police to take down webstresser, the world's largest DDoS-for-hire service. The effect was immediate, as researchers attributed an immediate decrease in DNS amplification attacks to the demise of this organization.¹⁰

These are just the latest in a series of operations from western governments and authorities designed to clamp down on cybercriminals and nation-state actors. Moreover, courts are increasingly responding with jail time for cybercriminals like Daniel Kaye, a hacker who launched a Mirai-based botnet attack that ultimately crashed large sections of the internet in Liberia in 2016.¹²

We expect that such actions against malicious actors will increase in 2019 as Western nations build on this collaborative effort to fight cybercrime. This will also rely on collaboration with private sector information security professionals such as the ASERT team.



The ASERT team was able to assist the FBI during an investigation that ultimately led to charges being filed against a hacker known as stevenkings.

CONCLUSION

The overall threat landscape is simultaneously lawless and frighteningly efficient. In the second half of 2018, we saw threat actors building crimeware that was cheaper and easier to deploy — and more persistent once installed. At the same time, many groups applied business best practices that further extended the reach of attacks, while making it even easier for their customers to access and leverage malicious software and DDoS attack tools.

Meanwhile, nation-state APT groups continued to proliferate across the globe, attacking financial institutions, governments, academia, and telecommunications companies, just for starters. Capable of affecting national elections and crippling online access, the threat posed by these groups increased daily.

Moreover, these groups attacked across the entire threat spectrum, as attackers took advantage of increasingly effective tools and techniques and an ever-lower barrier to entry. Attack vectors that were once confined to sophisticated actors are now available from attackers for hire, widening their reach and ability to damage private and public sector organizations. Actors that once relied on closely guarded custom tools became just as efficient "living off the land." And these attacks generally increased in size, as bad actors of all types unleashed attacks that often involved hundreds of thousands — or even millions — of victims who largely served to amplify the attack or ended up as collateral damage. And in the strategic sphere, those large-scale campaigns were often aimed at highly selected targets.

Further, the internet-scale paradigm changed the frontiers for where attacks can be launched, observed, and interdicted. Global threats will require global interventions, involving enterprises, service providers, and governments.

This is an enormously complex scenario and solving it will involve coordinated efforts across the public and private sector on a global scale. Organizations must also regularly evaluate and update security technologies and techniques. 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

- ¹www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html
- ²www.recordedfuture.com/chinese-threat-actor-tempperiscope/
- ³securelist.com/luckymouse-ndisproxy-driver/87914/
- ⁴unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
- ⁵asert.arbornetworks.com/tunneling-under-the-sands/
- ⁶unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/
- ⁷unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/
- ⁸www.eset.com/us/about/newsroom/corporate-blog/what-you-need-to-know-about-lojax-the-new-stealthy-malware-from-fancy-bear/
- ⁹blogs.360.cn/post/APT_C_01_en.html
- ¹⁰asert.arbornetworks.com/stolen-pencil-campaign-targets-academia
- ¹¹asert.arbornetworks.com/danabots-travels-a-global-perspective/
- ¹²asert.arbornetworks.com/fast-furious-iot-botnets-regifting-exploits/
- ¹³asert.arbornetworks.com/dipping-into-the-honeypot/
- ¹⁴blog.apnic.net/2018/12/04/ddos-defences-in-the-terabit-era-attack-trends-carpet-bombing/

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.

© 2019 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.