NETSCOUT THREAT INTELLIGENCE REPORT: POWERED BY ATLAS

Cybercrime's Innovation Machine

Findings from 1H 2019

TABLE OF CONTENTS

EDITOR'S NOTE

HARDIK MODI *Senior Director, Threat Intelligence*

It's hard to express the scale of today's cyber threat landscape, let alone its global impact. We can tell you that there were nearly four million DDoS attacks around the world in the last six months, and that attack frequency grew by 39 percent. Or that the NETSCOUT ASERT team saw 20,000 unique samples per month from just one family of IoT malware. Or even that it can take only five days from the discovery of a new attack vector to the availability of tools for the script-kiddie designed to exploit that vulnerability.

But those numbers, while startling, don't fully convey the impact of that steady drumbeat of new threats. Cybercrime has entered the mainstream of our culture to an unprecedented extent, and it is here to stay. We already saw online gamers hire DDoS botnets to take down opponents; now, college students can easily do the same — to take down their testing platform. Globally, cyber tactics like malware, DDoS attacks, and social engineering are increasingly used by geopolitical adversaries. Ransomware has become common enough to prompt 225 US mayors to sign a resolution vowing not to pay ransoms to hackers.

That increasingly mainstream pervasiveness makes what we do even more relevant. 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. 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. By using ATLAS data 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.

In conjunction with this report, we're also launching an information service designed to represent the threat landscape in real time. NETSCOUT Cyber Threat Horizon (horizon.netscout.com) is powered by ATLAS and represents much of the same underlying data you'll see this in report. Our objective is to enhance situational awareness for key stakeholders — those who care about how attack activity impacts organizations like themselves worldwide. As you read this report and reflect on our observations from the past six months, please turn to Cyber Threat Horizon to see what is happening today.

EXECUTIVE SUMMARY

In the past six months, NETSCOUT Threat Intelligence saw the cybercriminal business model grow into a stunningly efficient operation.

Crimeware has not just gone to B school; it could teach classes at this point. Botmasters are weaponizing everything from smartphones to smart homes to Apple software. It can take as little as five days from new attack vector discovery to weaponization, widening access to fast, efficient tools for anybody with an axe to grind. Internet of Things (IoT) devices are under attack five minutes after they are powered up and are targeted by specific exploits within 24 hours. Indeed, at this point cybercrime is thoroughly embedded in mainstream culture. College students can hire botnets to take down testing platforms, while nation states are increasingly turning to cyber weapons as part of their toolkit in geopolitical skirmishes. Two Florida cities used insurance to pay off ransomware attacks, while device manufacturers such as D-Link face legal consequences for leaving their hardware open to attacks. Advanced persistent threat (APT) groups are combining freely available malware with custom code to target countries — and the victim often modifies and reuses that same malware against the originator.

▲39%

increase in attack frequency compared to 1H 2018.

▲776%

growth in attacks between 100 Gbps and 400 Gbps.

5 DAYS

It can take only five days for a new attack vector to be weaponized.

HERE ARE A FEW HIGHLIGHTS OF THE MAJOR TRENDS WE OBSERVED:

BOTMASTERS GETTING SMART

Rapid weaponization of multiple vulnerable services continues, as attackers take advantage of everything from smart home sensors to smart phones, routers, and even Apple software[1] to discover and weaponize new attack vectors at a breathtaking clip.

FIVE DAYS, THAT'S IT

It can take only five days from new attack vector discovery to weaponization, giving anybody with a grudge fast access to inexpensive — and devastatingly effective — tools for revenge.

BAD ACTORS FEAST ON MID-SIZE DDOS ATTACKS

In the first half of 2019, DDoS attack frequency grew 39 percent compared with 1H 2018. In particular, bad actors feasted on the juicy middle of attack sizes, resulting in staggering growth of 776 percent in attacks between 100 Gbps and 400 Gbps in size.

DON'T WANT TO STUDY FOR FINALS? HIRE A BOTNET

The NETSCOUT security operations center (SOC) worked with one university to shut down targeted local attacks to online test platforms and curriculum. The culprit was likely a student, highlighting just how easy it is for novices to access very sophisticated attack tools. Why study when you can kill the test instead?

GEOPOLITICAL SKIRMISHES GO CYBER

Geopolitical adversaries increasingly target one another using cyber tactics ranging from malware and DDoS attacks to social engineering and misinformation.

FIREWALLS GET HIT

We've seen proof-of-concept malware targeting IoT devices behind firewalls — a rich opportunity, considering that there are 20 times more IoT devices behind firewalls than directly connected to the internet. An average of 7.7 million IoT devices are connected to the internet every day, many of them with little to no security.

POINT-OF-SALE MALWARE: STILL, IT PERSISTS

Despite ongoing efforts to stop such malware, point-of-sale (POS) infections often persist for many years. A single infection on a retail POS terminal can result in thousands of stolen credit cards on a daily basis. Two malware families, Backoff and Alina, continue to report hundreds of infections to our sinkhole.

MIRAI REMAINS THE KING OF IoT MALWARE, WITH NEW VARIANTS TO EXPLOIT DEVICES

Due to the lack of skill needed to take advantage of new exploits, default credentials, and features of the original code, Mirai and its variants will continue to dominate. We saw more than 20,000 unique Mirai samples and variants monthly in the first half of 2019, flattening any competition in the IoT malware space. These malware binaries and variants mimic predecessors by using a mixture of hard-coded administrative credentials and exploits to compromise IoT devices.

MIRAI

continues to dominate the IoT malware scene with a growing number of variants reported in 1H 2019.

20:1

is the estimated ratio of IoT devices behind firewalls vs. directly connected to the internet.

7.7M

IoT devices are connected to the internet every day.

ADVANCED THREAT

APT group activity grew worldwide. ASERT actively tracks about 30 groups while being aware of some 185 globally. The team worked to assign activities to various campaigns before eventually assigning specific campaigns to a variety of named groups—a complicated and fascinating process.

In particular, APT activity seen during 1H 2019 showed that geopolitical adversaries increasingly target one another by using cyber tactics, another finding that points to mainstreaming of the threat landscape.

While APT groups certainly developed new and sophisticated malware, many also used widely available existing tools, along with tactics such as social engineering and deception. Why expend existing resources to create custom tools when what you already have still works? It's a good reminder that most APT groups are defined by being nation-state sponsored rather than by their cutting-edge technique.

KEY FINDINGS

1 GEOPOLITICAL SKIRMISHES RAMP UP

Geopolitical adversaries increasingly target one another using cyber tactics ranging from malware and DDoS attacks to social engineering and misinformation.

2 DECEPTION RULES

While bespoke and sophisticated malware continues to make the rounds, many campaigns had little to no malware at all and relied entirely on deception and social engineering, since email remains the dominant intrusion vector.

3 EXPLOIT AND REPEAT

Continuing a trend that escalated last year, adversaries made use of widely available exploitation tools such as mimikatz, njRAT, and PsExec, even when APT campaigns appear to have substantial resources or expertise available to create custom tools.

4 BROWSER WARNINGS

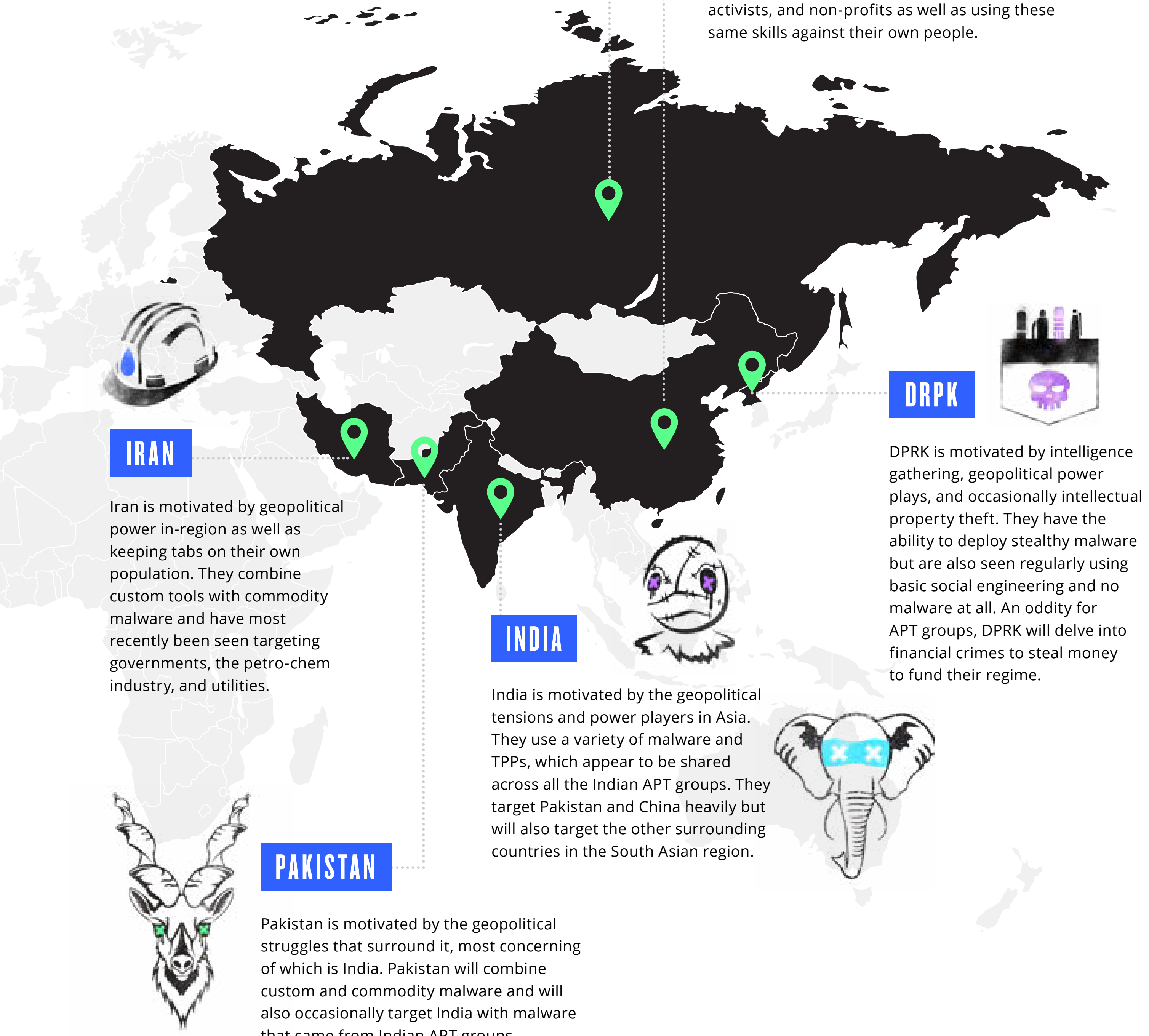
Malicious browser add-ons and extensions appear to be gaining in popularity.

RUSSIA

Russia is motivated by geopolitical tensions in former USSR nations, Central Asia, and the entirety of Western nations. They have the capability and resources to combine tailored cyber campaigns with human espionage or disinformation. Their historical and current targeting of elections and industrial control systems, often with never-before-seen malware, highlight how catastrophic their attacks can be.

CHINA

China is motivated by intelligence gathering and intellectual property theft, targeting governments and industry alike. They are adept at creating new malware, using commodity malware, and exploiting 0-days. China's APT groups are numerous and well-funded; there's likely not a corporation on earth who hasn't seen one of them. They also target lawyers, journalists, activists, and non-profits as well as using these same skills against their own people.



IRAN

Iran is motivated by geopolitical power in-region as well as keeping tabs on their own population. They combine custom tools with commodity malware and have most recently been seen targeting governments, the petro-chem industry, and utilities.

DRPK

DPRK is motivated by intelligence gathering, geopolitical power plays, and occasionally intellectual property theft. They have the ability to deploy stealthy malware but are also seen regularly using basic social engineering and no malware at all. An oddity for APT groups, DPRK will delve into financial crimes to steal money to fund their regime.

INDIA

India is motivated by the geopolitical tensions and power players in Asia. They use a variety of malware and TPPs, which appear to be shared across all the Indian APT groups. They target Pakistan and China heavily but will also target the other surrounding countries in the South Asian region.

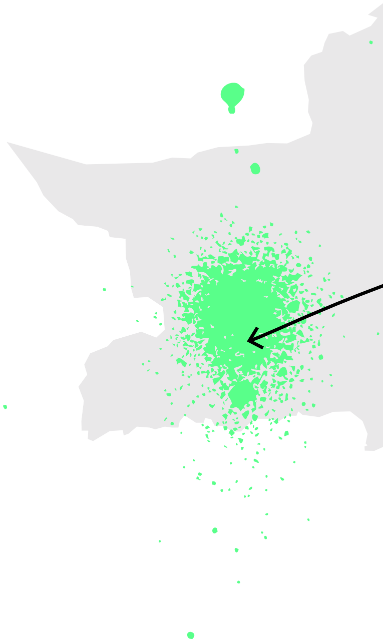
PAKISTAN

Pakistan is motivated by the geopolitical struggles that surround it, most concerning of which is India. Pakistan will combine custom and commodity malware and will also occasionally target India with malware that came from Indian APT groups.

INDIA + PAKISTAN

TENSION IN SOUTH ASIA

APT activity in India and Pakistan, historically quiet, saw a sharp increase over the last six months: the ASERT team discovered almost daily activity. The targets? Almost exclusively each other.*



ASERT currently tracks six distinct Indian APT groups and three Pakistani APT groups, and the sheer number of individual campaigns and associated malware samples spiked dramatically in recent months. ASERT assesses that increasing tensions in South Asia have contributed to both countries prioritizing intelligence-gathering activities against one another. This has had a domino effect, since neighboring countries gather intelligence on both in order to keep tabs on the situation.

India has one of the world's largest militaries, which is used, among other things, to assert the territorial boundaries it shares with six neighboring countries — an ostensible motivation in India's APT targeting. Pakistani APT targeting is heavily focused on India, but also gathers intelligence on other neighbors and keeps tabs on internal dissent.

The cyber component of this hostile relationship dates to the early 1990s. APT motives include traditional intelligence-gathering operations and credential theft for follow-on operations.

The specific campaigns the countries launch against each other are nearly always in service of current events and government priorities.

OTHER POPULAR TARGETS OF BOTH COUNTRIES

Military, Government + Diplomatic

South and Central Asian neighbors for military, government, and diplomatic information.

Financial

Corporations and entities with financial or economic ties that operate regionally.

Government Officials

Each other's government officials, businessmen, and diplomats residing in or visiting other countries. Embassy targeting remains popular and continues to be one of the methods ASERT uses to find their campaigns.

Independent Businesses

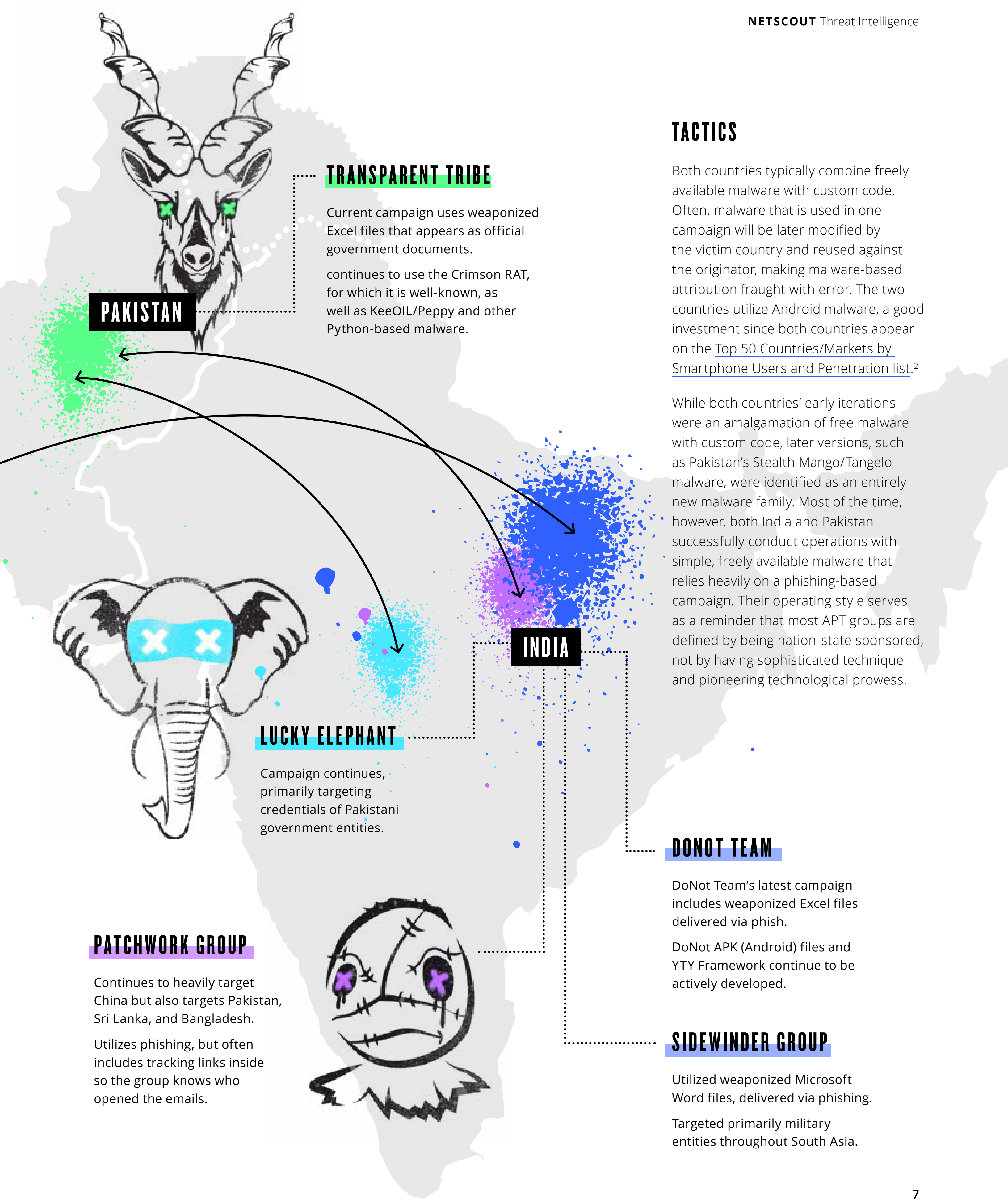
Businesses in Europe and the United States, especially defense contractors, have also seen Indian and Pakistani hackers. In those cases, the attackers are interested in those businesses' operations in South Asia, but theft of missile technology data has happened more than once.

**Both countries do occasionally target European and North American defense contractors involved with missile technology.*

TACTICS

Both countries typically combine freely available malware with custom code. Often, malware that is used in one campaign will be later modified by the victim country and reused against the originator, making malware-based attribution fraught with error. The two countries utilize Android malware, a good investment since both countries appear on the Top 50 Countries/Markets by Smartphone Users and Penetration list.[2]

While both countries' early iterations were an amalgamation of free malware with custom code, later versions, such as Pakistan's Stealth Mango/Tangelo malware, were identified as an entirely new malware family. Most of the time, however, both India and Pakistan successfully conduct operations with simple, freely available malware that relies heavily on a phishing-based campaign. Their operating style serves as a reminder that most APT groups are defined by being nation-state sponsored, not by having sophisticated technique and pioneering technological prowess.



TRANSPARENT TRIBE

Current campaign uses weaponized Excel files that appears as official government documents.

continues to use the Crimson RAT, for which it is well-known, as well as KeeOIL/Peppy and other Python-based malware.

LUCKY ELEPHANT

Campaign continues, primarily targeting credentials of Pakistani government entities.

PATCHWORK GROUP

Continues to heavily target China but also targets Pakistan, Sri Lanka, and Bangladesh.

Utilizes phishing, but often includes tracking links inside so the group knows who opened the emails.

DONOT TEAM

DoNot Team's latest campaign includes weaponized Excel files delivered via phish.

DoNot APK (Android) files and YTY Framework continue to be actively developed.

SIDEWINDER GROUP

Utilized weaponized Microsoft Word files, delivered via phishing.

Targeted primarily military entities throughout South Asia.

RUSSIA

A BEARY FANCY PROBLEM

Fancy Bear (APT28) is the most visible Russian APT group and alone accounts for 12 percent of ASERT's APT observations. The Russian Federation, a "multi-party representative democracy" (at least on paper), is intensely interested in Western/NATO advances on the world stage, particularly where they intersect with Russian interests. This fuels the motivation behind their APT targeting.

Fancy Bear's phishing over the past few years has targeted the United Nations, NATO, and diplomatic organizations such as the U.S. State Department and embassies around the world. Fancy Bear's formulaic phishing usually includes masquerading as a known entity and using malware such as mimikatz, PsExec, or the group's well-known Sofacy.

Amidst the constant Russian APT activity, ASERT continued tracking the ever-stealthy LoJax malware in early 2019, used primarily against geopolitical targets of interest. X-Agent and Sofacy also persist in Fancy Bear's toolkit, a testament to the fact that they still work.

Thus far in 2019, Fancy Bear has been involved in sophisticated LoJax collection as well as its typical phishes. Fancy Bear continues to receive credit for all Sofacy, X-Agent, and Seduploader malware, and the group is also linked to the Zebrocy malware. Fancy Bear was involved in past[6] election tampering and disinformation campaigns and continues these operations into present[7] day. Additionally, sometimes Industrial Control Systems (ICS) targeting gets thrown into the same Fancy Bear umbrella.

THE PROBLEM? WE'RE ALL PUTTING ENTIRELY TOO MUCH INTO THE FANCY BEAR BUCKET.

Fancy Bear has long been attributed to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), which is true,[8] but the entirety of GRU operations does not equal Fancy Bear. One group cannot possibly manage years-long, ridiculously amateurish phishing campaigns, create and deploy something as unprecedented as LoJax, and publish a wicked meme campaign — concurrently.

ASERT's theory is that what the community calls Fancy Bear actually encompasses multiple APT groups as well as other intelligence operations. Here's our thinking:

- InfoSec companies often use language that indicates multiple group activity. For example, Kasperky referred to "a subset of Sofacy activity,[9]" while highlighting Zebrocy within the Central Asian/Caucasus region.
- That activity is quite different from the Western/NATO geopolitical targeting.
- Both of those are quite different from the targeting that occurs against VIP targets.
- The disinformation campaigns are barely an InfoSec operation, except that they use the internet.
- The ICS targeting is another Bear entirely.

It's important to remember that although the United States often places cyber operations in its own special category, the rest of the world just calls it spying. It's therefore misguided to assume that the legion of concurrent GRU cyber operations originate from a single area. The GRU is made up of multiple directorates, various front organizations, and a network of loosely affiliated contractors, which gives the GRU flexibility and plausible deniability when warranted. Each of these entities has different responsibilities, although they can overlap. Separate groups operating under one larger organization might share malware, occasional infrastructure, and even personnel. Things that are likely to differ are the targeted entities (often geographically), specific C2 servers (with individualized server configurations and settings), and specific compromise techniques (such as phish fabrication).

These subgroups are also likely to differ on resources and funding, typical with any government-run operation, and will likely be based on national priorities. This means the depth and breadth of campaigns will be different; some will be wide and broad, while others will be limited and surgical. High-value targets and priorities will likely be given to experienced operators, with newer malware and clean infrastructure that is quickly abandoned. Lower-priority targets will see more-obvious malware, reused infrastructure, and imprecise techniques likely from less-experienced operators.

ASERT's theory is that what the community calls Fancy Bear actually encompasses multiple APT groups as well as other intelligence operations.

IRAN

NEIGHBORLY INTEREST

Iran targets government, military, and industry entities as related to its strategic goals and objectives. The country is particularly interested in its neighbors as well as in being able to understand and counter adversaries.

Chafer has continued to target transportation and aviation, while OilRig focuses on Middle Eastern issues. Charming Kitten has a long history of targeting dissidents, expats, and journalists, and activities continue to focus on issues of "Western influence." Contrary to popular belief, a reduction in espionage activities was not a condition of the Joint Comprehensive Plan of Action (JCPOA), an agreement narrowly focused on economic and nuclear proliferation issues. ASERT had not observed a decrease of cyber activity during JCPOA, nor an increase following the United States withdrawal from that agreement.

CHINA

FIVE POISONS ESPIONAGE

China conducts espionage against government, military, and related industries, especially as it relates to Chinese national interests such as the country's economy, foreign relationships, and the South China Sea.

China also appears to have focused more espionage activities against the Five Poisons (Uyghurs, Tibet, Falun Gong, democracy movements, and Taiwan), plus Hong Kong. We've seen an increase in regional targeting related to these specific strategic interests.

BIOMEDICAL RESEARCH TARGETED

The Democratic People's Republic of Korea (DPRK) targets universities and organizations, with a heavy focus on the biomedical engineering industry.

The actors behind the STOLEN PENCIL campaign additionally have targeted a disease-prevention nonprofit operating in Asia, a company involved in gene editing and CRISPR, and general-science departments. DPRK also has continued to target government and diplomatic entities, especially as related to the United States and South Korea, and continues to use malware to generate revenue.

THE ASERT APPROACH TO NAMING APT GROUPS

It may seem as though there are no rules when it comes to naming APT groups, since different organizations come up with differing monikers for various groups and campaigns. Fancy Bear, for example, has at least half a dozen names.[3] But while the process may look chaotic, the information security (InfoSec) community actually takes a very nuanced approach to assigning attribution and compartmentalization of APT groups. In general, as many campaigns become available, often through the participation of the entire InfoSec community, it makes sense to combine those campaigns under the umbrella of a group name.

That's where things get complicated. This isn't always a clean process, and not every organization will do it the same way—or choose to do it at all. Here at ASERT, we combine the Cyber Kill Chain[4] and the Diamond Model[5] to organize tactics, techniques, and procedures (TTPs) into campaigns that we track. Different organizations often have their own names for APT groups, which critics note can be confusing and hard to remember. It may be helpful to dig into the reasons why this happens, however:

1

GROUPS OUTGROW THEIR DEFINITIONS

Due to an organization's internal attribution processes and its visibility into the APT activity, each name essentially represents a different definition of what characterizes that APT group. As time goes on, those definitions might evolve or grow such that the names from different organizations are no longer synonymous.

Several examples of APT groups that evolved over time include Patchwork Group, Fancy Bear, Lazarus Group, and Equation Group. In each of these cases, the InfoSec community often lumped all activity with a nexus from one country into one of these group buckets, when in reality there are many different groups that make up these buckets and have differing agendas.

2

DIFFERENT ORGANIZATIONAL FOCUSES DRIVE DIFFERENT NAMING CONVENTIONS

Governments, for example, often focus the attribution process where their skillset lies, namely in classified intelligence. Governments will often name their APT groups based on groups of people, organizations, and even the ultimate financiers. Grouping based on these aspects complements intelligence analysis, because it aligns with other specialties, such as military, political, or financial analysis.

Private infosec companies, on the other hand, tend to group malicious activity by the TTPs observed throughout the process of the Kill Chain. This creates a guide of sorts, intended for a net defender to discover, predict, and combat the threats on their network. The Diamond Model focuses on the adversary, infrastructure, capability, and victim. This complementary and broadened perspective allows for the additional step of context and intelligence — just the thing needed to prepare for follow-on attacks.

GEOGRAPHIC DISPERSION OF APT ACTIVITY

ASERT actively blocks threats and/or has some level of visibility into APT group activity.

HERE ARE THE COUNTRIES:

1 Brazil

2 Canada

3 China

4 France

5 India

6 Iran

7 Israel

8 Kazakhstan

9 Lebanon

10 Mexico

11 North Korea

12 Pakistan

13 Palestine

14 Russia

15 Singapore

16 South Korea

17 Spain

18 Syria

19 Tunisia

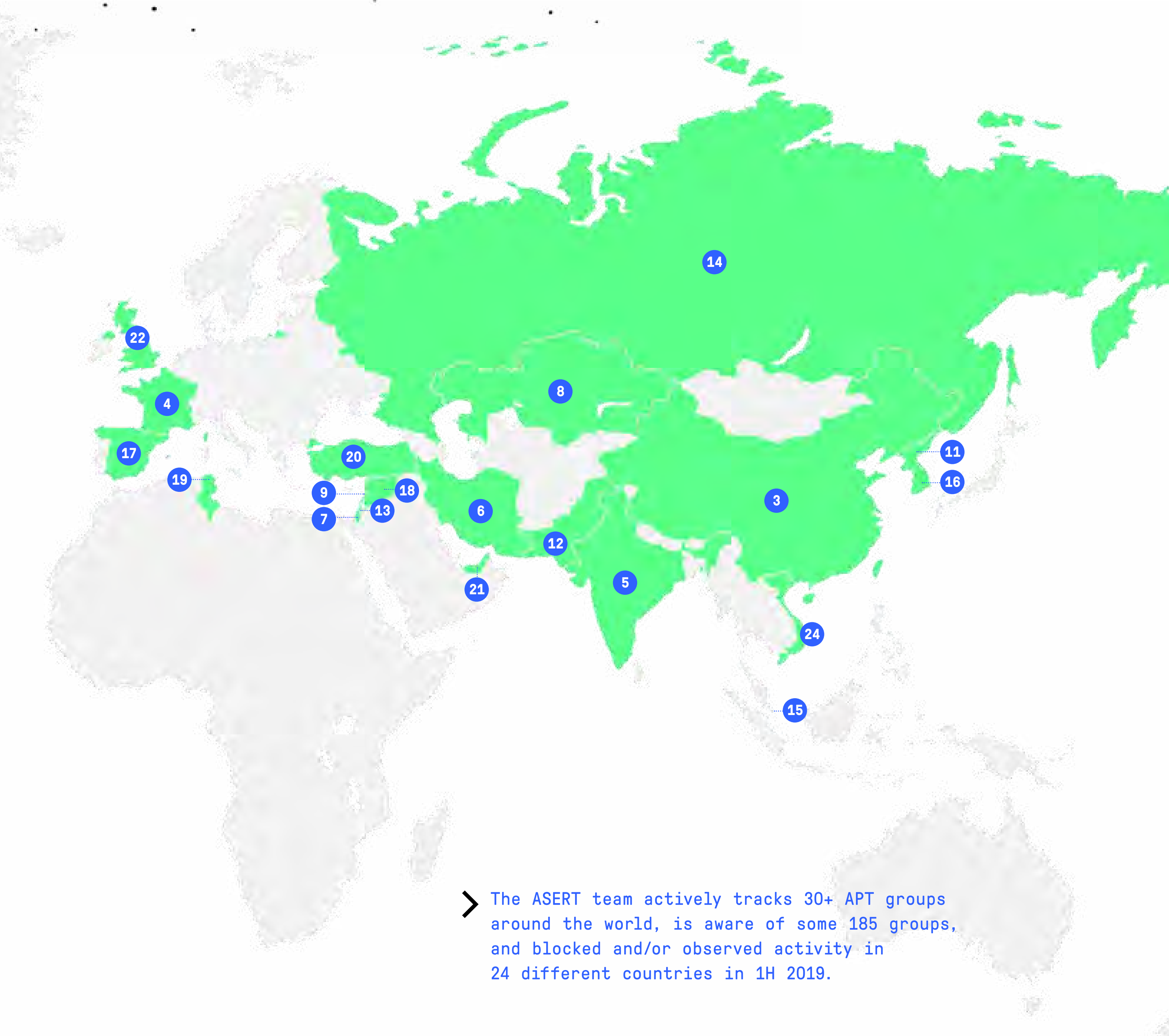
20 Turkey

21 United Arab Emirates

22 United Kingdom

23 United States

24 Vietnam



The ASERT team actively tracks 30+ APT groups around the world, is aware of some 185 groups, and blocked and/or observed activity in 24 different countries in 1H 2019.

CRIMEWARE

What if you had a business model so innovative that it could spot market opportunities within minutes of their inception? And even better, roll out new products for them within five days? Move over, Google — right?

These new digital superstars are underground cybercrime organizations with stunningly efficient business models that create innovative new weapons at a breathtaking pace.

Last year, cybercriminals buckled down and went to B school, creating platforms and services via many of the same methods and practices used by legitimate business around the world. This year, these same criminals focused not just on innovation but also on efficiency, streamlining their operational models into a digital machine that exploits new innovations while continuing to monetize old tactics.

Case in point: Crimeware families such as DanaBot gained a global foothold in the latter half of 2018 by using an affiliate model to outsource installation of the malware.[10] This year, the already-efficient crimeware framework capitalized on ransomware's effectiveness by adding a module that encrypts files to bolster revenue.[11]

With the advent of chip and Europay, Mastercard, and Visa (EMV) technology and the global efforts to squash ransomware, many thought that POS malware and ransomware would become all but extinct. However, examples such as DanaBot's ongoing success and evolution; reports about local governments and insurance companies making ransom payments for file decryption; and the re-emergence of groups such as FIN8, which focus on POS malware to steal credit card data, prove otherwise. And let's not forget the ever-increasing number of IoT threats saturating the globe. The reality is that cybercriminals know how to get the most bang for the buck with operations that run like well-oiled machines.

There are some silver linings, however. We are seeing more crackdowns on illicit operations, arrests of botnet operators, and regulations on IoT device security. Even the indictment of foreign adversaries in relation to cyber activities helps shine a spotlight on groups that wreak financial havoc from the shadows. These efforts go a long way toward making a better, more secure internet.

KEY FINDINGS

1 BULLSEYE ON IoT

The presence of IoT devices on the internet continued to grow at a staggering pace, providing an ever-growing target for malware operators leveraging IoT malware. The growth of the IoT space has also seen an alarming increase in the number and variants of Mirai in the wild.

2 MIRAI REMAINS THE KING OF IoT MALWARE

Mirai's dominance also means that telnet brute-forcing still remains the reigning champ for compromising IoT devices. Moreover, exploitation via old, little used, or unknown vulnerabilities is on the rise.

3 RANSOMWARE AND POS MALWARE PERSIST

Just as IoT, brute-forcing, and exploitation are a continued threat, ransomware and POS malware continue to thrive and succeed. Recent events showcase local governments shelling out for ransom payments and the re-emergence of well-known groups such as FIN8, showcasing POS malware's continued relevance as a moneymaker.

THE ERA OF MIRAI

In August 2016, an IoT-based botnet called Mirai was released on the internet, causing massive disruption in multiple high-profile, high-impact DDoS attacks. What made the Mirai botnet so devastating was its support of multiple architectures and DDoS attack vectors.

The author behind Mirai built massive botnets by exploiting hard-coded administrative credentials on IoT devices such as cable/DSL modes, DVR systems, and IP-based cameras. To make matter worse, the author of Mirai released the original code for Mirai several weeks after it originally appeared, including build scripts for different processor architectures. This gave criminal entrepreneurs a sterling opportunity to capitalize on the success of Mirai by cloning the source code, thus letting anybody easily build his or her own IoT botnets. Over the past three years, we have observed an increase of Mirai-based variants in the wild. Working with our partner, **Reversing Labs**, we plotted the number of Mirai samples and its variants over the past three years (see Figure 1).

Timeline of Mirai Sample

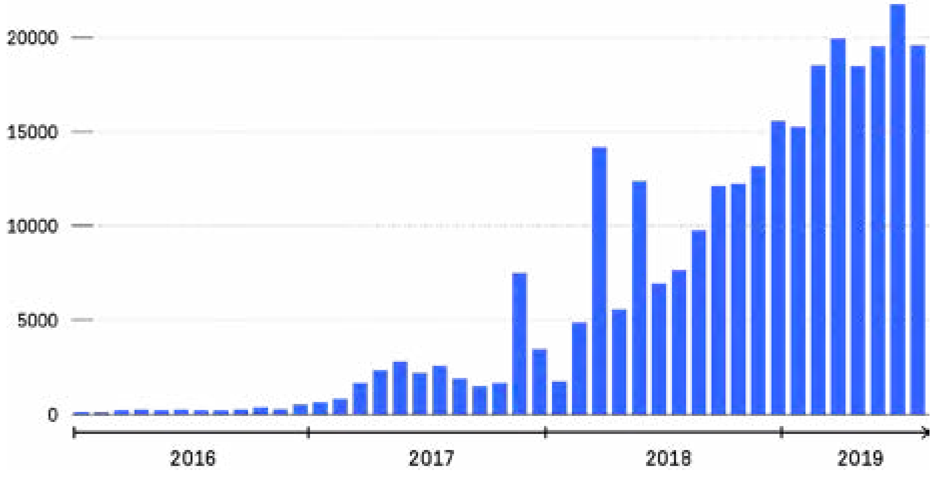


Figure 1: Mirai-based Samples over the Past Three Years (Reversing Labs)

> Several spikes in late 2017 and 2018 indicate Mirai variants evolved to use exploits that targeted vulnerabilities in IoT devices.

WE WITNESSED THE RISE OF SEVERAL BOTNETS THAT USED MIRAI AS A FOUNDATION TO BUILD UPON:

OMG

Variants such as OMG added new features such as incorporating 3proxy, which allowed them to enable a SOCKS and HTTP proxy server on the infected IoT device. With proxy capabilities, a bot author can proxy any traffic of its choosing through the infected IoT device. This includes additional scans for new vulnerabilities, launching additional attacks, and pivoting from the infected IoT device to other networks that are connected to the device.[13]

SATORI BOTNET

One of the first Mirai variants to include IoT-based exploits as an additional means of propagation and added support for ARC architecture.[12]

HADOOP YARN EXPLOIT (EDB-ID 45025)

This was used by threat actors to deliver even more variants of Mirai.[14]

While the trend of 2018 was to include exploits that targeted IoT vulnerabilities, 2019 showed that tried-and-true Mirai tactics such as the use of hard-coded administrative credentials remain incredibly effective. We've also seen an increase in Mirai variants that use a mixture of hard-coded administrative credentials and exploits to compromise IoT devices (see Figure 2).

TOP 5 MIRAI VARIANTS FOR 1H 2019

Top 5 Busybox Markers for 1H 2019

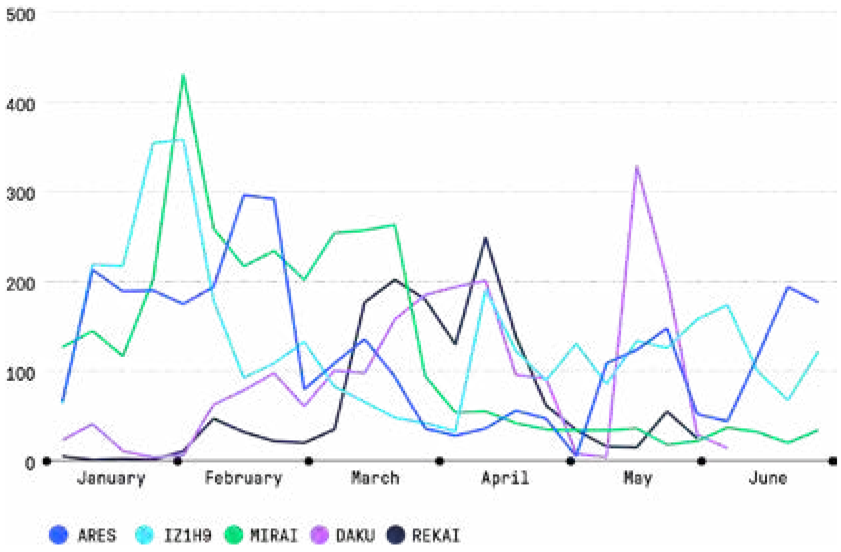


Figure 2: Top 5 Busybox Markers for 1H 2019

Perhaps one of the reasons for the continued popularity of this exploit lies in the fact that user names and passwords are remarkably static, with several of the same passwords still in use year over year. No wonder IoT devices are such hot targets, since they are commonly deployed with default configurations and little to no ingress filtering.

For the first half of 2019, our honeypots logged more than 61,220 unique attempts that used default or hard-coded administrative credentials to deliver a Mirai variant. Of those attempts, the following were the top five Mirai variants being delivered (see Figure 3 and 4).

Top 5 IoT Exploits Based on Unique Source IP

EXPLOIT NAME	EDB-ID	UNIQUE SOURCE IPS
AVTECH IP Camera/VR/DVR Devices *Multiple Vulnerabilities*	45000	322
Hadoop YARN ResourceManager *Command Execution*	45025	5,602
Huawei Router HG532 *Arbitrary Command Execution*	43414	36,334
Linksys E-series *Remote Code Execution*	31683	448
Realtek SDK *Miniigd UPnP SOAP Command Execution*	37169	14,692

Figure 3: Top 5 IoT Exploits Based on Unique Source IP

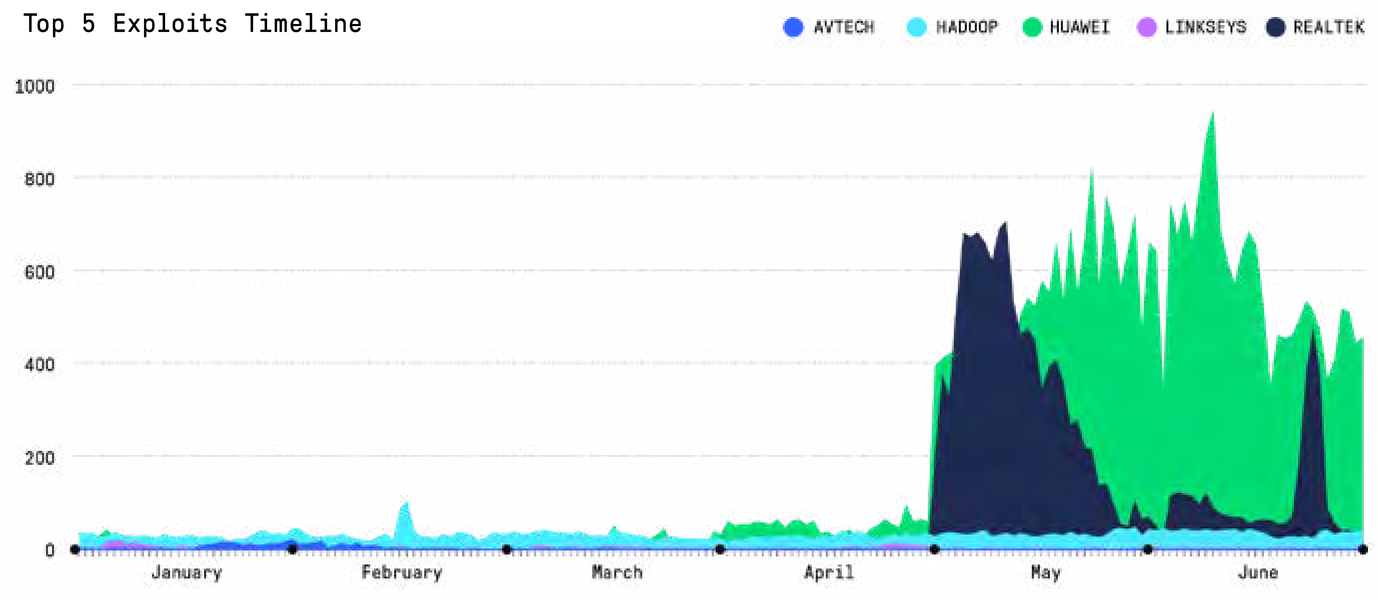


Figure 4: Top 5 Exploits Timeline

In addition to brute-force telnet attempts, our honeypots also track exploits used to deliver IoT-based bots by monitoring connections attempting to exploit known vulnerabilities within IoT devices. We currently track 50-plus IoT-related exploits. Based on our observation of the top five exploits, approximately 75 percent of the exploit attempts delivered variants of Mirai.

We also monitored the continued use and upward trajectory of IoT malware that uses exploitation as a means for initial infection and propagation.[15] Between April 22 and May 10, 2019, our honeypots observed a 5,043 percent increase in exploit attempts targeting Realtek SDK miniigd SOAP vulnerability in consumer-based routers, an older exploit with plenty of juice remaining. The reason? IoT devices are patched at a glacial pace, if at all. In fact, IoT devices such as home routers are often installed and forgotten.

Because adversaries have such success with both brute-forcing and exploiting older vulnerabilities in devices, we anticipate this trend will continue in the foreseeable future. Figure 5 shows a first-half 2019 comparison of brute-force attempts as compared to exploitation attempts against known vulnerabilities.

As we move into the latter half of 2019, we predict a continued rise in the number of Mirai variants. Fueling this growth will be newly discovered exploits, reuse of older exploits, and hard-coded credentials.

Due to the ease with which unskilled operators can take advantage of new exploits, credentials, and features in the original Mirai code, Mirai and its variants will continue to dominate the IoT malware scene.

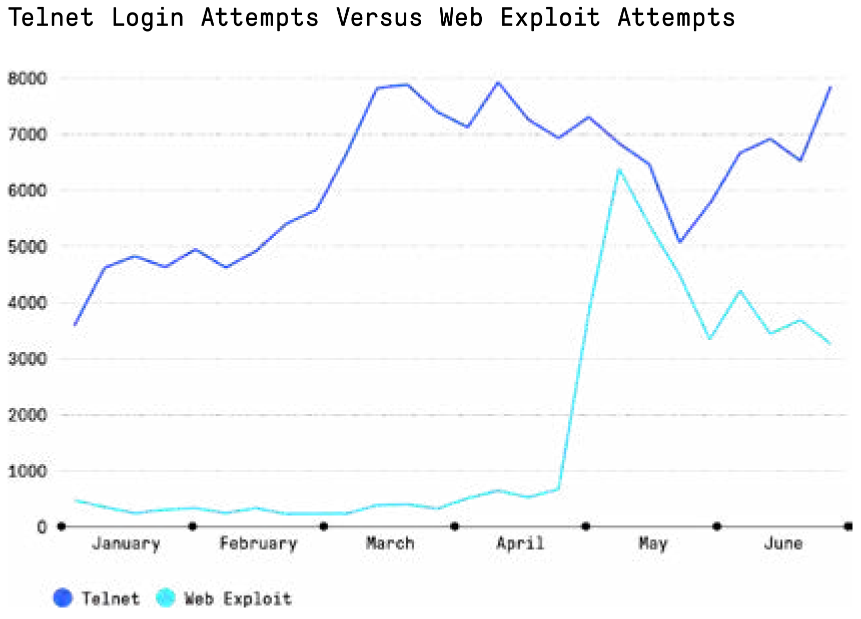


Figure 5: Telnet Login Attempts Versus Web Exploit Attempts

POS MALWARE: STILL, IT PERSISTS

POS malware operations persist despite ongoing attempts to eradicate them, often for many years. Two malware families, Backoff and Alina, continue to report hundreds of infections to our sinkhole. Although the number may not seem overly large, a single infection on a retail POS terminal can result in thousands of stolen credit cards on a daily basis.

The move to chip and pin, or EMV, makes it harder for attackers to deploy POS malware effectively, but there are still many organizations and retailers that use magnetic stripes, which are susceptible to POS malware, for credit-card transactions. Even organizations that use chip technology often default to magnetic-stripe transactions should the chip fail to read properly or the system experience technical problems. It's also possible to override the required use of a chip in many devices after that device fails to read the chip three times. POS malware, although not as common or frequent today, is still a threat that should be taken seriously.

The reality is, POS malware, though not as common or frequent today, is still a threat that should be taken seriously.

Unique IPs by Day by Malware Family

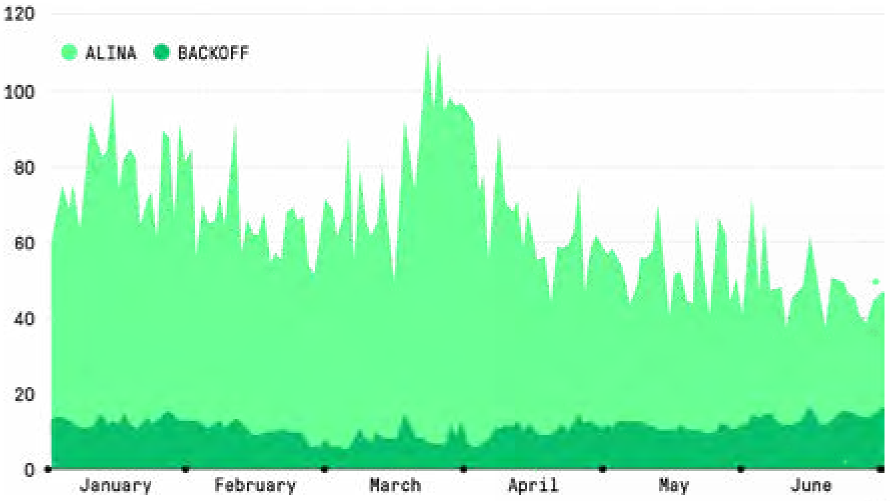


Figure 6: Unique IPs by Day by Malware Family

DDoS

It's safe to say that our DDoS section will never open with "All quiet on the DDoS front." In the first half of 2019, we saw attack frequency grow 39 percent compared with 1H 2018. In particular, bad actors feasted on the juicy middle of attack sizes, resulting in a 776 percent growth in attacks between 100 Gbps and 400 Gbps.

KEY FINDINGS

1 BOTMASTERS GET SMART

Rapid weaponization of vulnerable services has continued as attackers take advantage of everything from smart home sensors to smartphones, routers, and even Apple software. On average, 7.7 million IoT devices are connected to the internet every day, many of them with known security issues or with no security at all. Even worse, proof-of-concept malware has appeared, targeting the untold number of vulnerable devices behind firewalls.

7.7M IoT devices connected to the internet every day

2 FIVE DAYS TO ATTACK

It can take just five days from new attack vector discovery to weaponization, making these powerful attacks available to anyone with a grudge.

3 DON'T WANT TO STUDY FOR FINALS HIRE A BOTNET

The NETSCOUT SOC worked with one university to mitigate very targeted local attacks targeting online test platforms and curriculum. The culprit was likely a student, highlighting just how easy it is for novices to access very sophisticated attack tools. Why study when you can kill the test instead?

4 ATTACK FREQUENCY GROWS. AGAIN.

Overall, global DDoS attack frequency grew by 39 percent between 1H 2018 and 1H 2019. Once again, we saw staggering growth of 776 percent in attacks between 100 Gbps and 400 Gbps in size.

▲ **39%** Global DDoS attack frequency

▲ **776%** Attacks 100–400 Gbps

5 WIRELESS AND SATELLITE UNDER FIRE

Attackers increasingly targeted satellite communications and wireless telecommunications, which experienced a 255 percent and 193 percent increase in attack frequency, respectively.

▲ **255%** Targeting satellite communications

▲ **193%** Targeting wireless communications

GLOBAL DDoS ATTACK FREQUENCY	▲ 39%
Attacks in 1H 2018	2.8M
Attacks in 1H 2019	3.8M

MAX ATTACK SIZE	▼ 63%
Max Attack in 1H 2018	1.7 TBPS
Max Attack in 1H 2019	634 GBPS

ATTACKS 100–400 GBPS	▲ 776%
Attacks in 1H 2018	458
Attacks in 1H 2019	4,014

DECREASE IN ATTACKS GREATER THAN 500 GBPS	▼ 32%
Attacks in 1H 2018	19
Attacks in 1H 2019	13

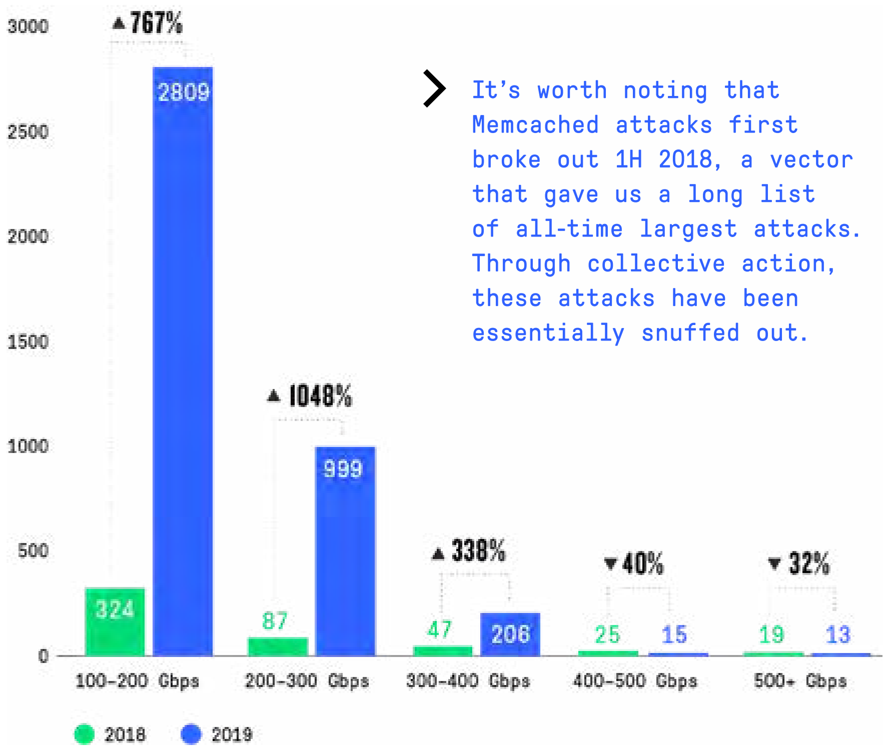
DDoS ATTACK TRENDS

For the first half of 2019, DDoS attack frequency jumped by 39 percent compared with the same time period in 2018. In particular, attacks between 100 Gbps and 400 Gbps in size experienced staggering growth.

Indeed, attacks in this "juicy middle" section grew by 776 percent. In comparison, the frequency of very large attacks dropped significantly: we saw a 40 percent reduction in attacks between 400 and 500 Gbps and a 32 percent decrease in attacks of more than 500 Gbps. This is to be expected, however, because we are comparing data with 1H 2018 — a period that saw the arrival of memcached attacks, a vector that gave us a long list of all-time largest attacks. Thanks to collective action, very large attacks in this vector essentially have been snuffed out.

DDoS-for-hire services continue to thrive and build ever-more operationally efficient business models available to an increasingly mainstream clientele. Students can hire botnets to take down testing platforms, while threat actors are so efficient at monetizing new attacks that it can take only five days from the initial discovery of a new attack vector to weaponization.

Year to Year Attack Size Trends



> It's worth noting that Memcached attacks first broke out 1H 2018, a vector that gave us a long list of all-time largest attacks. Through collective action, these attacks have been essentially snuffed out.

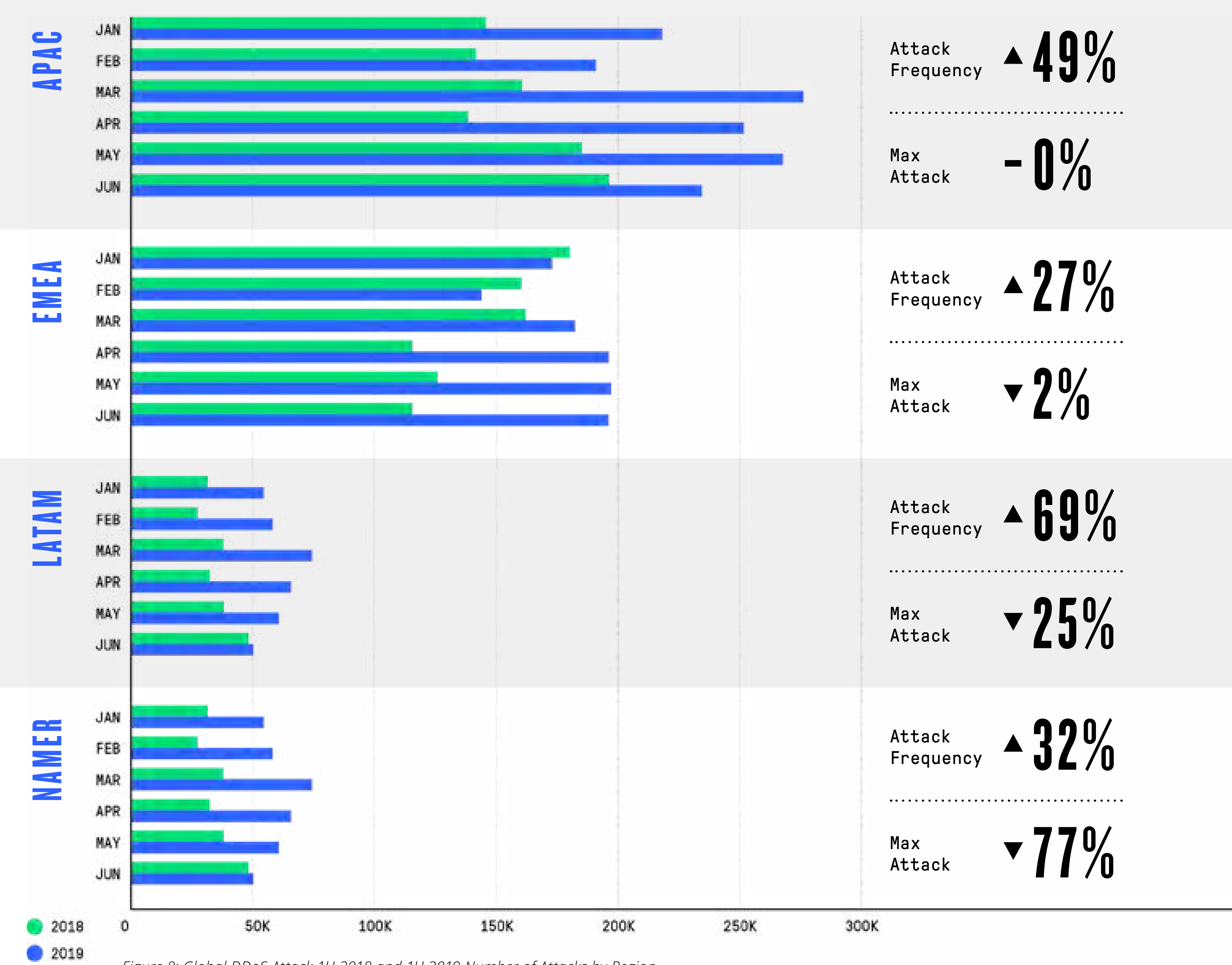
Figure 7: Year to Year Attack Size Trends

REGIONAL ATTACKS

Attack frequency increased across all regions in 1H 2019, with APAC once again receiving a far larger number of attacks compared with other global regions.

For example, while all regions experienced increases in attacks between 100 and 200 Gbps, the disparity in numbers is startling: APAC saw 2,093 attacks in that range — a growth rate of more than 1,900 percent, compared with 716 total attacks across the other three regions combined. This is not meant to dismiss the impact on other regions, however. EMEA, in particular, experienced a significant increase in attacks of more than 100 Gbps, a growth of 431 percent year over year. Similarly, North America's attacks in the same range increased by 99 percent during the same time period. Overall, the max attack sizes shrunk across all regions, as attackers turned their focus away from very large attacks of more than 400 Gbps to concentrate on the "small big" attacks that range between 100 Gbps and 400 Gbps.

Global DDoS Attacks by Region



APAC — Attack Frequency ▲49% — Max Attack -0%

EMEA — Attack Frequency ▲27% — Max Attack ▼2%

LATAM — Attack Frequency ▲69% — Max Attack ▼25%

NAMER — Attack Frequency ▲32% — Max Attack ▼77%

Figure 8: Global DDoS Attack 1H 2018 and 1H 2019 Number of Attacks by Region

VERTICAL INDUSTRY ATTACKS

We analyzed attack data by North American Industry Classification System (NAICS) codes, which group companies into 22 broad categories that contain multiple large subvertical sectors. Comparing first-half data from 2018 to 2019 for the top 10 most-targeted sectors, we found an attack landscape with several emergent target areas.

Attackers have turned their attention to wireless and satellite communications, while attacks on wired telecom are growing at a far more modest rate. Education categories have also come under increased fire in terms of both attack size and frequency.

As has been the case for every threat report thus far, the top four subvertical sectors remained the same, although there was some jostling for position: Wireless Telecommunications Carriers leapfrogged Data Processing, Hosting, and Related Services into third place compared with 1H 2018.

THE TOP FOUR SUB-VERTICAL SECTORS

1. Wired Telecommunications Carriers
2. Telecommunications including Satellite and Cable
3. Data Processing, Hosting + Related Services
4. Wireless Telecommunications Carriers

We expect to see this top four, since such activity is inherent to their role as connectivity providers, with attacks focused on their residential and business subscribers as well as on their operational infrastructures. However, there were some variations year over year that illustrated a continued diversification of attack size, with some significant shifts in targets across several vertical sectors.

▼73%

MAX ATTACK SIZE PLUMMETS FOR WIRED TELECOM

The first half of 2018 saw the Dawn of the Terrorbit[16] attack, including the largest attack yet seen — a 1.7 Tbps memcached attack mitigated by NETSCOUT Arbor solutions.

This year, the max attack size for this category fell by 73 percent, to 473 Gbps.

HOT ATTACK TARGETS

SATELLITE COMMUNICATIONS HIT THE TOP TEN

Companies in this vital support sector for the telecommunications and broadcasting industries saw a significant bump in attacks, as the sector jumped from 17th to 6th place year over year, with a 246 percent increase in attack frequency.

▲ 246% Increase in attack frequency

FULL SPEED AHEAD ON BRAKES

The Motor Vehicle Brake System Manufacturing sector saw a 1,238 percent increase in frequency but a 54 percent drop in size.

▲ 1,238% Increase in attack frequency

BIG BUMP FOR EDUCATION

Colleges, Universities, and Professional Schools moved up three slots into 9th place, while the max attack size increased by nearly a quarter (24 percent). The Educational Services sector moved from 10th to 7th place. Educational Support Services, which includes educational consultants and testing services, moved from the 27th to 11th spot, with a 487 percent jump in attack frequency.

▲ 487% Increase in attack frequency

BIOTECH UNDER ATTACK

The Professional, Scientific, and Technical Services sector jumped from 13th to 8th place, with a 46 percent increase in max attack size. This category includes computer programming and design services, as well as bio and nano technology research.

▲ 6% Increase in attack frequency

ATTACKERS FOCUS ON WIRELESS

The Wireless Telecommunications Carriers sector saw a 150 percent increase in frequency, while wired telecom grew at a far more modest 16 percent.

▲ 150% Increase in attack frequency

INCREASED TUBE STAKES

There was a 35 percent increase in attack frequency in the Radio and Television Broadcasting sector.

▲ 35% Increase in attack frequency

DECREASED INTEREST

DIPLOMATS GET A BREAK

The International Affairs sector, which includes everything from the US State Department to immigration services to the World Bank, saw an 89 percent drop in attack frequency, falling from 6th place to 15th place year over year.

▼ 89% Decrease in attack frequency

ECOMMERCE FALLS FROM THE TOP

The Electronic Shopping and Mail-Order Houses sector fell seven spots to 14th place, with an 82 percent drop in attack frequency.

▼ 82% Decrease in attack frequency

OTHER TELECOMMUNICATIONS DISAPPEAR FROM VIEW

Companies in the Other Telecommunications sector caught a break, falling from 8th place to 39th place year over year with a 99.8 percent drop in frequency and a drop in max attack size from 600 Gbps to 2.6 Gbps, a 99.6 percent decrease.

▼ 99.6% Decrease in attack frequency

Top Verticals Targeted by DDoS Attacks

1H 2018

RANK	VERTICAL	ATTACKS FREQUENCY	MAX ATTACK	CLASSIFICATION
1	Wired Telecommunications Carriers	793,778	1.7 Tbps	Information
2	Telecommunications	491,314	302.0 Gbps	Information
3	Data Processing, Hosting + Related Services	316,395	316.9 Gbps	Information
4	Wireless Telecommunications Carriers	157,388	327.5 Gbps	Information
5	Software Publishers	44,724	170.6 Gbps	Information
6	International Affairs	40,711	34.3 Gbps	Public Administration
7	Electronic Shopping + Mail-Order Houses	39,493	170.6 Gbps	Retail Trade
8	Other Telecommunications	39,004	600.0 Gbps	Information
9	Custom Computer Programming Services	31,837	170.6 Gbps	Professional, Scientific + Technical Services
10	Educational Services	27,164	96.8 Gbps	Educational Services

1H 2019

RANK	VERTICAL	ATTACK FREQUENCY	MAX ATTACK	CLASSIFICATION	
1	Wired Telecommunications Carriers	1,048,579	472.9 Gbps	Information	– 0
2	Telecommunications	591,033	634.3 Gbps	Information	– 0
3	Wireless Telecommunications Carriers	460,682	301.8 Gbps	Information	▲ 1
4	Data Processing, Hosting + Related Services	312,377	330.4 Gbps	Information	▼ 1
5	Custom Computer Programming Services	34,139	146.4 Gbps	Professional, Scientific + Technical Services	▲ 4
6	Satellite Telecommunications	30,563	54.1 Gbps	Professional, Scientific + Technical Services	NEW
7	Educational Services	24,564	68.3 Gbps	Educational Services	▲ 3
8	Professional, Scientific + Technical Services	22,098	71.6 Gbps	Professional, Scientific + Technical Services	NEW
9	Colleges, Universities + Professional Schools	20,188	176.4 Gbps	Educational Services	NEW
10	Software Publishers	13,368	78.8 Gbps	Professional, Scientific + Technical Services	▼ 5

DDoS HIGHLIGHTS

To botnet operators, the 7.7 million new IoT devices connected to the internet each day look like the most enticing all-you-can-eat buffet in the world. After all, many of those devices lack security or have known security issues.

These attackers constantly scan the internet for new vulnerable services, taking advantage of unsecured deployments and services. And they do so with amazing efficiency:

- It can take only five days for new attack vectors to be weaponized, making these powerful attacks available to anyone with a grudge.
- Even worse, attackers' indefatigable research turns up a constant stream of new ways to access that alluring smorgasbord of devices. In the last six months, four new DDoS reflection-type attacks and one new web attack have been seen on the internet, showing that the DDoS weaponization of vulnerable services is rapidly increasing.
- The 1.7 Tbps memcached attack in 2018 demonstrated that researching and launching new attack types can give the attackers powerful weapons that can cause havoc for unprepared defenders.

AND WHILE THAT'S BAD, IT'S JUST THE BEGINNING. CONSIDER THE FOLLOWING:

Secure Assumptions

Usually, IoT devices are deployed behind internet gateways and firewalls and are therefore assumed to be secure. Indeed, the ratio of IoT devices behind the firewalls versus those directly connected to the internet is estimated to be around 20:1.

Proof-of-Concept Malware

We have seen proof-of-concept malware specially designed to infect vulnerable devices behind firewalls. Several businesses have had serious system outages not because they were under attack, but because their systems were busy launching outbound DDoS attacks.

Internal Devices

This means that the IoT botnets and resulting DDoS attacks seen in recent years represent the tip of the iceberg compared to what might be possible when internal devices get compromised.

HERE'S A RUNDOWN OF THE LATEST ATTACK VECTORS:

Apple Remote Management Services (ARMS)[17]

In late June 2019, a new DDoS reflection attack vector using UDP port 3283 was used to attack service providers in Eastern Europe. NETSCOUT ASERT research investigated the issue and discovered that attackers were taking advantage of a vulnerability in the Apple Remote Desktop (ARD) protocol, in this case the operational management of the protocol running on UDP port 3283. ARD is disabled by default on Apple computers, but when remote sharing is enabled, anyone can send a small UDP packet to the computer and receive a large reply. By spoofing the source IP address, the attacker can generate a DDoS reflection attack with a respectable 35:1 amplification factor.

Ubiquity Discovery Protocol

Ubiquiti Networks manufactures a variety of networking devices, including wireless access points, routers, switches, and firewalls. In February 2019, researchers reported new DDoS reflection-type attacks taking advantage of a vulnerability in the discovery protocol used by Ubiquiti devices (UDP port 10001) after seeing these new attacks used on the internet. This vulnerability allowed anyone to send a small 56-byte UDP query to the device and receive a large reply, containing a list of all devices discovered. Using a spoofed source IP, this allowed the attacker to launch a DDoS reflection-type attack with an amplification factor of up to 35:1.

At that time, there were around 485,000 vulnerable Ubiquiti devices on the internet, but because the manufacturers quickly released a patch fixing this issue, the number of vulnerable devices had declined to around 190,000 by April 2019.

.

CoAP[18]

The Constrained Application Protocol (CoAP) is a specialized protocol for constrained devices that enables them to communicate with the wider internet.

This protocol is primarily used for IoT devices (sensors, controllers, and the like) but is also included in smartphones for use in home automation. The protocol is in many ways similar to the memcached protocol, offering memory caching to reduce communication and processing overhead.

The CoAP protocol is designed without any security features, assuming that encryption and authentication will be handled by higher layers in the communication stack. However, when using CoAP on devices with very little processing capability—and in some cases, devices running on batteries — solution developers skip these additional layers.

Unfortunately, this has led to the wide deployment of devices on the internet with unsecured CoAP deployments, allowing attackers to use these devices for launching DDoS reflection-type attacks in similar fashion as memcached reflection-type attacks. A typical CoAP device will allow for a reflection factor of 34:1, meaning that the reply packet is up to 34 times larger than the packet used to trigger the reply.

Attackers started launching DDoS attacks using vulnerable CoAP devices in January 2019. At that time, there were about 388,000 vulnerable devices connected to the internet; this number has been increasing steadily, reaching around 600,000 devices in late May 2019.

Web Services Dynamic Discovery (WS-DD)

The Web Services Dynamic Discovery protocol (WS-DD) is designed to locate services on a local network. Unfortunately, when devices implementing this protocol are connected directly to the internet, they can be used as DDoS reflectors with a reflection ratio of up to 300:1.

Small-scale attacks using this attack vector were seen on the internet in May 2019. At that time there were about 65,000 vulnerable devices connected to the internet, offering the attackers the opportunity to launch very powerful reflection-type attacks.

HTML5 hyperlink auditing ping redirection

In April 2019, several web sites in Asia were compromised such that when they were visited by legitimate users, the user browsers and computers automatically started launching application-layer DDoS attacks against targets around the world. This attack uses a common HTML5 attribute in web sites — the <a> tag ping — tricking any visitor to the web site to send HTML ping packets to the target as long as that user is connected to the site.

The attacks seen in April 2019 were of moderate size, with up to 4,000 users contributing to the attacks, resulting in around 7,500 malicious requests per second in one case.

WHAT CAN BE DONE

Attackers are constantly searching for new DDoS attack vectors and have focused on identifying vulnerabilities in modern solution architectures (memcached) and unsecure IoT deployments (CoAP, WS-DD), and taking advantage of bugs in Common Platform Enumeration (CPE) devices (Ubiquiti). The only way to deal with these and upcoming issues and vulnerabilities is to:

1

DEPLOY WITH SECURE PERIMETERS

Deploy all devices and services within secure perimeters (secure VLANs with firewalls controlling access).

2

BLOCK ACCESS

Block access to all services except where absolutely required.

3

REQUIRE BEST SECURITY PRACTICES

Require that IoT and CPE vendors follow best security practices but also treat those devices as potential infection vectors.

4

SCAN FOR VULNERABILITIES

Scan for and isolate vulnerable devices in your own network on a regular basis.

> Unless we take action soon, we risk having our own infrastructure and services used as DDoS attack vectors, also against ourselves.

NETSCOUT SOC: TALES FROM THE TRENCHES

If you think about it, SOC experts rely on an interesting mix of skills: half Eagle Scout and half secret agent.

After all, the Scouts use "Be Prepared" as a motto, and it takes meticulous preparation to automatically mitigate 79 percent of the 4,255 attacks the NETSCOUT SOC saw in the first six months of 2019.

How does NETSCOUT's Arbor Cloud SOC team scale to deal with this level of threat? Deep preparation, which means thoroughly understanding specific network environments and customizing defenses to automatically defend against such a huge number of opportunistic attackers. By building client-specific templates and measures for each client and using the enormous bandwidth available in Arbor Cloud, our SOC aims to make automatic mitigation par for the course. That's the value of having the most focused DDoS expertise in the market — in both technology and personnel.

But the reality is, no amount of preparation will create a system capable of automatically mitigating every attack. And that's when you need to tap into your inner James Bond, fighting motivated attackers wielding a dizzying array of vectors. These are the situations the SOC lives for. The team's collective experience and skills come together to quickly analyze and adapt defenses to match attackers tit for tat. Each confrontation brings the satisfaction of a well-fought fight as well as more material for that Boy Scout side — new tidbits about how attackers work, and how we can shut them down.

SOME HATS ARE WHITER THAN OTHERS.

The Arbor Cloud SOC team received an emergency call from a regional North American telephony provider under siege from a determined attacker that was effectively using carpet bombing techniques to cause disruption. The attacker had warned the company that its current DDoS vendor was not going to be effective and threatened continued attacks until a bitcoin ransom was paid. The telephony provider brushed off the threats, and the attackers proceeded to take the company off-line for three days running. This is a huge deal for a provider that largely services small to midsize businesses, because one outage could result in massive customer churn. The provider was able to discover that the attacker had breached its network as well; the company was actively monitoring the attacker's actions but was still not able to stop the DDoS attacks.

That's when we rode into town. The SOC team conducted an emergency overnight provisioning, and by morning were ready to mitigate. The moment that the Arbor Cloud autonomous system number (ASN) was announced to the internet, the attacker stopped all activities and withdrew from the network completely. Just the indication that Arbor Cloud was taking over protection was enough to drive the attacker away. This town had a new sheriff, and the bad guys had no appetite for a showdown.

SOC BY THE NUMBERS

Arbor Cloud is the largest purpose-built DDoS mitigation network on planet handing over 11 Terabits per second.

THE FIRST FIVE MONTHS OF 2019

Total number of attacks	4,255
Attacks over 50 Gbps	162
Attacks over 100 Gbps	47
Attacks automatically mitigated	3,374

DON'T WANT TO STUDY FOR FINALS? HIRE A BOTNET.

Higher education, like everyone else, has embraced the digital world, adding online classes and moving tests from paper and pencil to keyboard and screen. So it's not surprising to find this has made schools more susceptible to attacks on curriculum and testing — from the student body, that is. Out late last night? Didn't get a chance to study? No problem. Just hire a botnet and take down the test server. No test today!

We worked with a major university in the Northeast United States that was experiencing very targeted attacks on its online test platforms during semester beginnings and endings. School officials were convinced that the attacks came from within the student body, highlighting just how easy it is for novices to access very sophisticated attack tools. The attack vectors used were not particularly innovative, but the traffic was localized to sources geographically close to the university, and the timing of the attacks coincided with typical student cyber activities. The attackers were able to exert fine control on a botnet to closely simulate student traffic demographics and patterns. This typically would make the attacks more challenging to discern, but that wasn't the case for the Arbor Cloud SOC team. They were able to use the wealth of tools and techniques at their disposal to make sure the university's testing continued operating on schedule. Had the attacks succeeded, the school's ability to conduct classes and do online testing would have been nullified.

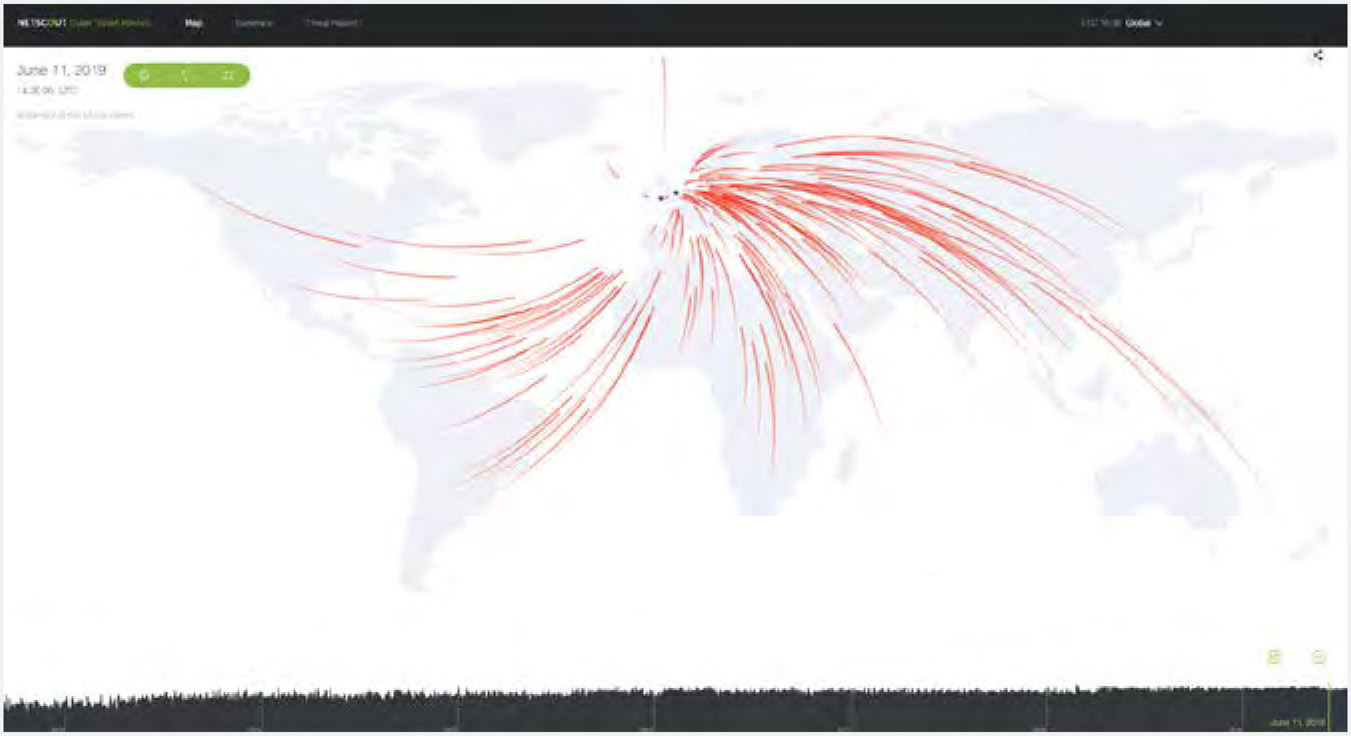
WE CAN PLAY CHESS FOREVER.

One customer, a major Asian gaming platform provider supporting tens of thousands of customers, was hit by a sophisticated attacker using a very large botnet. The pressure was on to find a solution quickly, because gamers can be very fickle and will quickly switch to other games or platforms if performance is not good. A thriving online gaming business could find itself in serious trouble if its service is deemed unreliable by the gamer community.

The botnet used in the attack was very large and quite sophisticated, so it allowed the attackers to vary attack vectors at will. Moreover, a high percentage of legitimate traffic sources originated behind proxy servers, so defenders had to be careful not to block these IP addresses inadvertently.

Commence the chess game. The Arbor Cloud SOC responded to the opening salvo with a typical mix of countermeasures tuned to the gaming environment. As soon as the attackers detected that their attack was not being effective, they switched vectors, forcing the SOC to switch defenses. Some of the attacks became so complex that they required real-time analysis and innovative filtering to thwart. The back-and-forth went on for a long time, but ultimately, the SOC team had the advantage thanks to the combination of know-how and tools that allowed them to adapt to every situation.

The lesson here? Most attackers are all about the opportunity cost — make that cost too high, and they'll depart for easier prey. Checkmate.



CYBER THREAT HORIZON

A global cybersecurity situational awareness platform, NETSCOUT Cyber Threat Horizon provides highly contextualized visibility into global threat landscape activity.

Our team focuses on the capabilities and potential and actual observations of DDoS and intrusion attacks to extract multiple indicators of an attack campaign, displayed graphically in the form of a map as well as summarized in reports. These reports can then be tailored to an organization's specific vertical and geographic profile. The result is a stronger understanding of what is happening "over the horizon" on the threat landscape — that is, to entities that might resemble yours in terms of geography or industry sector or simply those in which you are interested. For example, a North American technology firm with a significant supply chain in Southeast Asia might choose to maintain a view into activity in all sectors in North America, technology worldwide, and manufacturing in Asia. These views can be monitored in real time by analysts, on an operation-center screen, or via summary reports that can be assessed periodically.

Horizon is powered by NETSCOUT's Advanced Threat Level Analysis System (ATLAS), which uses a variety of tools and processes to collect and analyze threat data from a diverse array of sources — from enterprises and service providers to dark web and botnet traffic — and integrate it all into a complete picture.

How specific can we get? Take a look at the image here showing the June 6, 2019, attack on the Telegram messaging app, the objective behind which was alleged to be disrupting communications across Hong Kong activists conducting large-scale protests. We were able to pull out a very specific and granular slice of DDoS activity from global traffic and demonstrate the breadth of devices and reflection/amplification attack types used, as well as the countries where these devices were located. This is another instance where one might surmise the motivation behind an attack, but the nature of DDoS activity doesn't lend itself to clear attribution by observing the sources of traffic. There is a clear lesson here: Such attacks occur with some frequency, and if you're a messaging platform, such denial-of-availability attacks can be expected during high-profile events.

Learn More

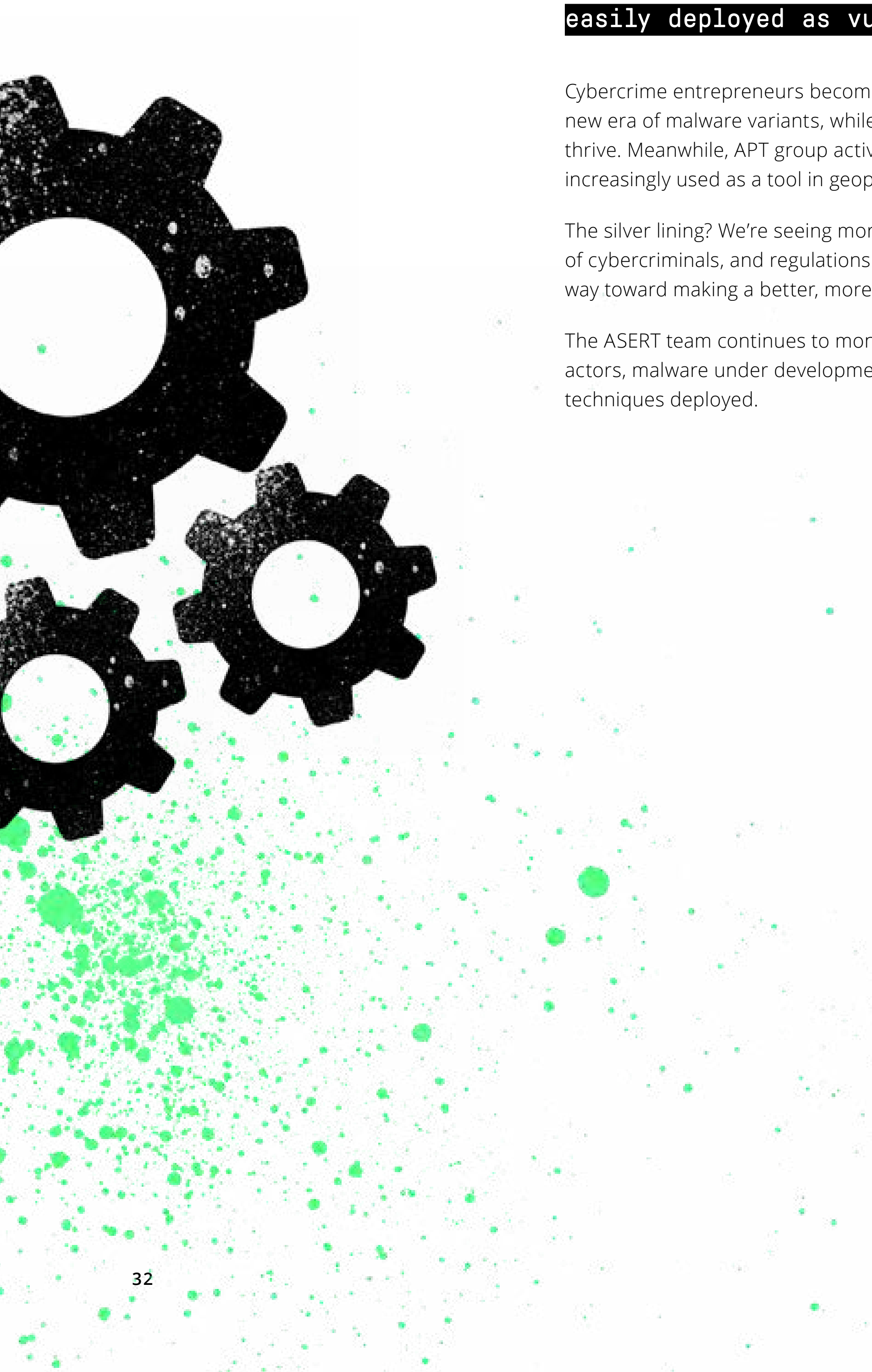
CONCLUSION

2019 has ushered in market-ready crimeware and freely accessible tools that can be quickly and easily deployed as vulnerabilities are discovered.

Cybercrime entrepreneurs become increasingly innovative, shepherding in a new era of malware variants, while older, tried-and-true methods continue to thrive. Meanwhile, APT group activity continues to proliferate, with cyber tactics increasingly used as a tool in geopolitical skirmishes.

The silver lining? We're seeing more crackdowns on illicit operations, indictments of cybercriminals, and regulations on IoT device security. These efforts go a long way toward making a better, more secure internet.

The ASERT team continues to monitor the threat landscape and report on new actors, malware under development, and increasingly sophisticated tools and techniques deployed.



APPENDIX

[1] netscout.com/blog/asert/call-arms-apple-remote-management-service-udp

[2] newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/

[3] attack.mitre.org/groups/

[4] lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[5] activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

[6] zdnet.com/article/microsoft-reveals-new-apt28-cyber-attacks-against-european-political-entities/

[7] zdnet.com/article/microsoft-reveals-new-apt28-cyber-attacks-against-european-political-entities/

[8] justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

[9] securelist.com/a-zebrocy-go-downloader/89419/

[10] netscout.com/blog/asert/danabots-travels-global-perspective

[11] bleepingcomputer.com/news/security/danabot-banking-trojan-upgraded-with-non-ransomware-module/

[12] netscout.com/blog/asert/arc-satori

[13] netscout.com/blog/asert/omg-mirai-minions-are-wicked

[14] netscout.com/blog/asert/mirai-not-just-iot-anymore

[15] netscout.com/blog/asert/realtek-sdk-exploits-rise-egypt

[16] netscout.com/threatreport/

[17] netscout.com/blog/asert/call-arms-apple-remote-management-service-udp

[18] netscout.com/blog/asert/coap-attacks-wild

REPORT PARTNERS

REVERSING
LABS

ReversingLabs

ReversingLabs provides advanced malware analysis and insights into destructive objects. Through its Titanium Platform, ReversingLabs delivers automated static analysis and file reputation services that represent the fastest and most accurate insights in the industry, finding the hidden objects that are armed to destroy enterprise business value. We maintain the largest repository of malware and goodware in the industry including more than 9 billion files and objects, and are the only vendor to speed analysis of files in milliseconds. ReversingLabs seamlessly integrates at scale across the enterprise with connectors that work with existing security investments, reducing incident response time for SOC analysts, while providing high priority and detailed threat information for hunters to take quick action.

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.