SUMMARY REPORT

ADVANCED THREAT AND CRIMEWARE

NETSCOUT THREAT INTELLIGENCE LANDSCAPE REPORT FINDINGS FROM SECOND HALF 2018

NETSCOUT®

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 groups 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 RogueRobin[4]. 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, APT28, or Sednit

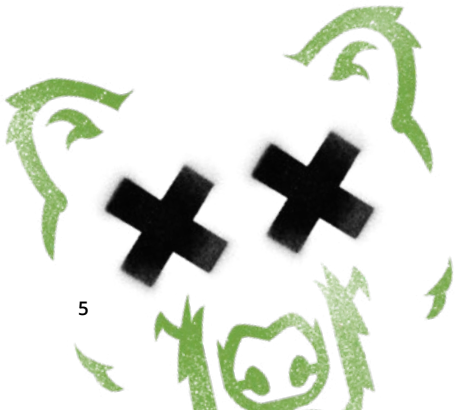
This APT group employed legitimate UEFI rootkit software to establish a backdoor on victim machines. The malicious files, originally classified as "unwanted software" by anti-virus vendors, avoided detection by minimally tweaking the software to phone home to the attacker C2 servers without changing 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."

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]



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.

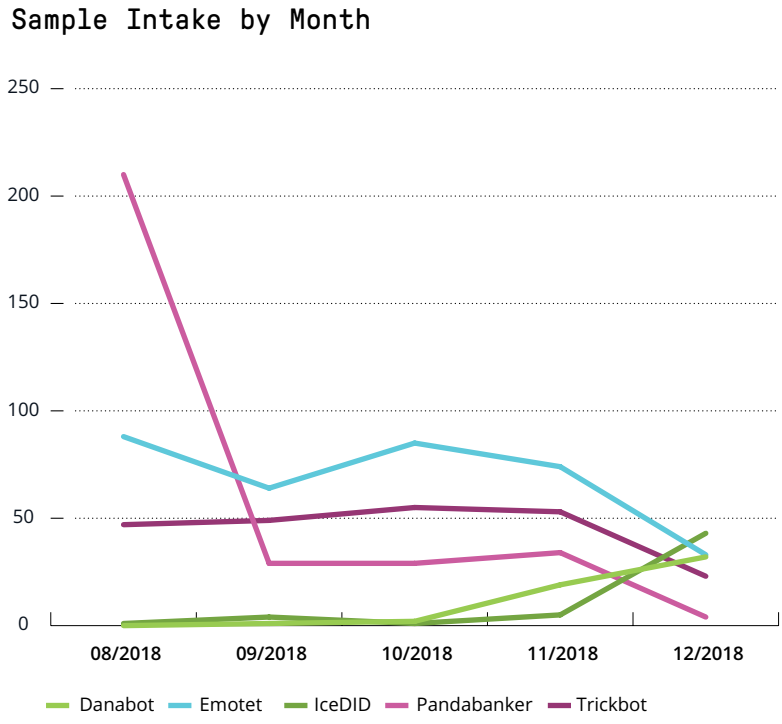
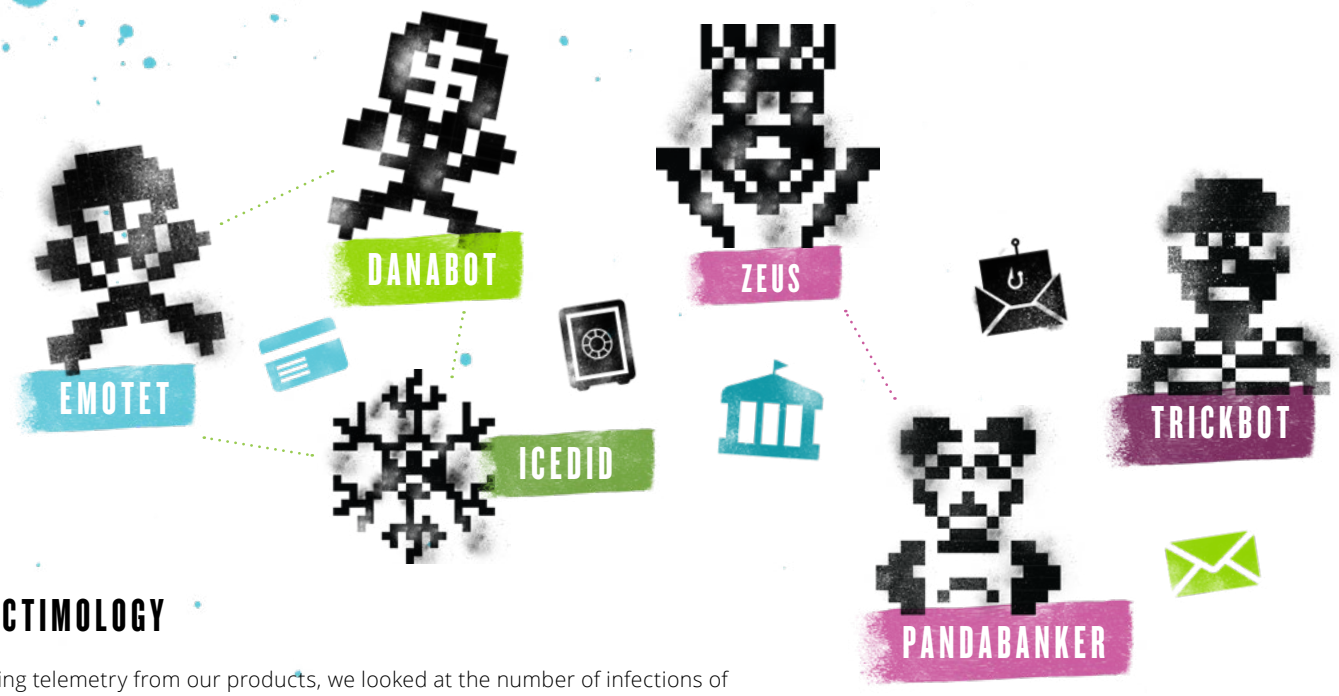


Figure 1: Sample Intake by Month

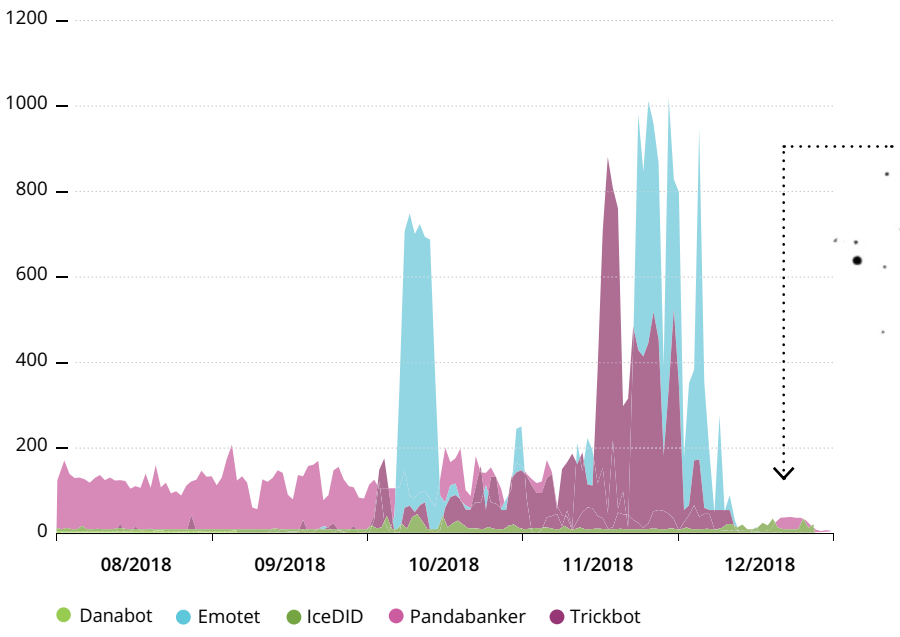


VICTIMOLOGY

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).

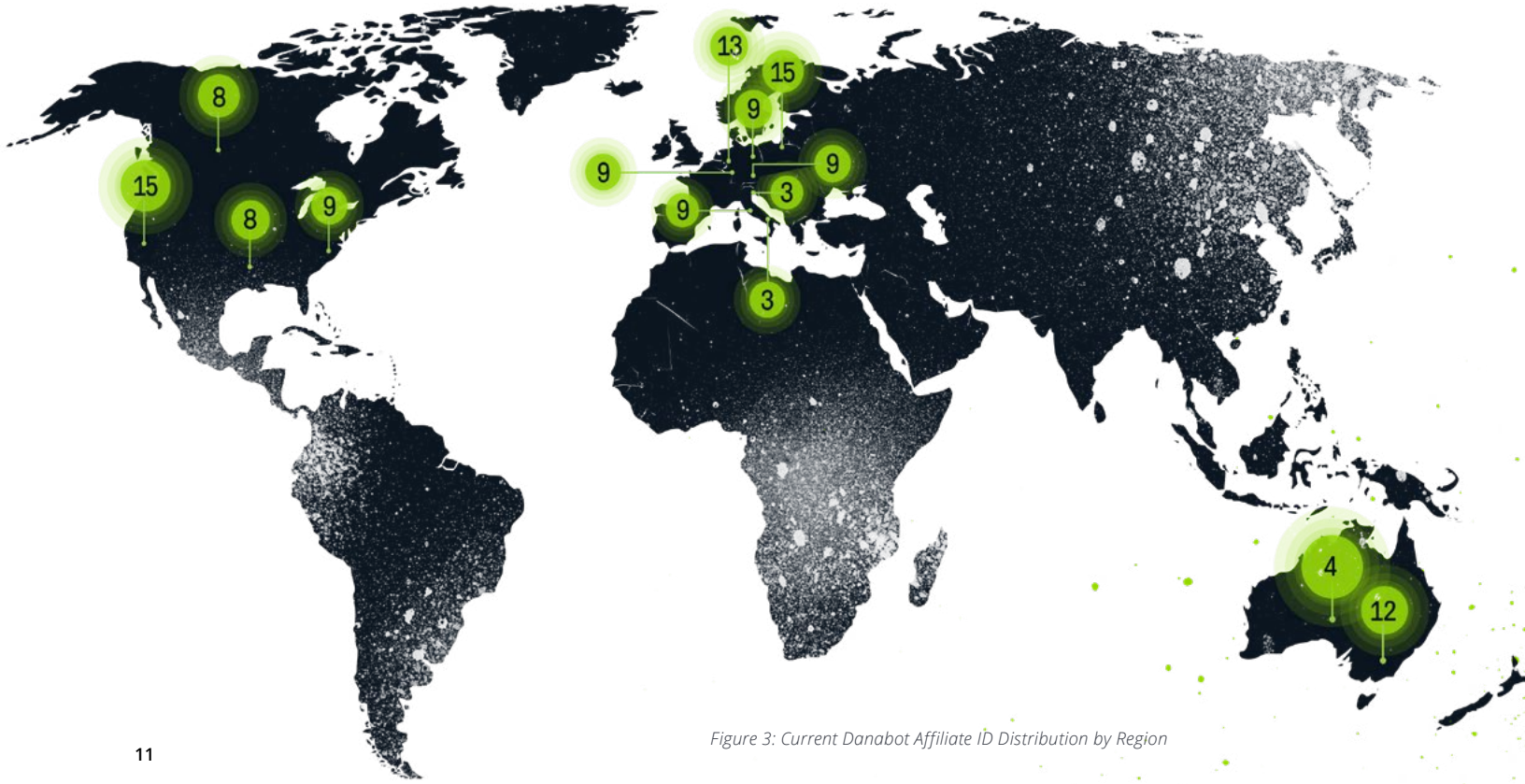


Figure 3: Current Danabot Affiliate ID Distribution by Region

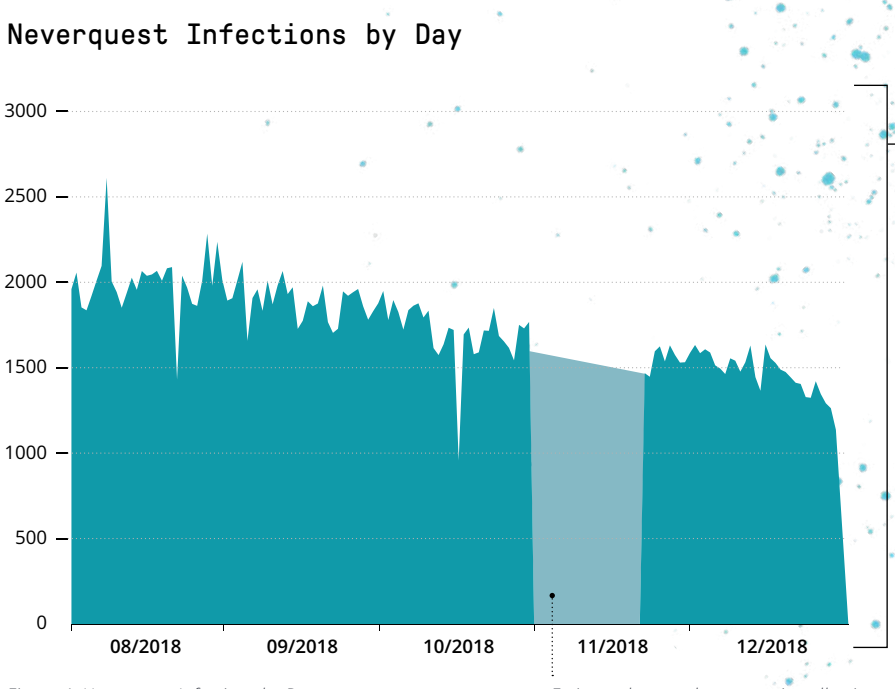


Figure 4: Neverquest Infections by Day

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

THE TOP SOURCE COUNTRIES OF BRUTE-FORCE IoT ACTIVITY

RUSSIA

CHINA

BRAZIL

UNITED STATES

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.

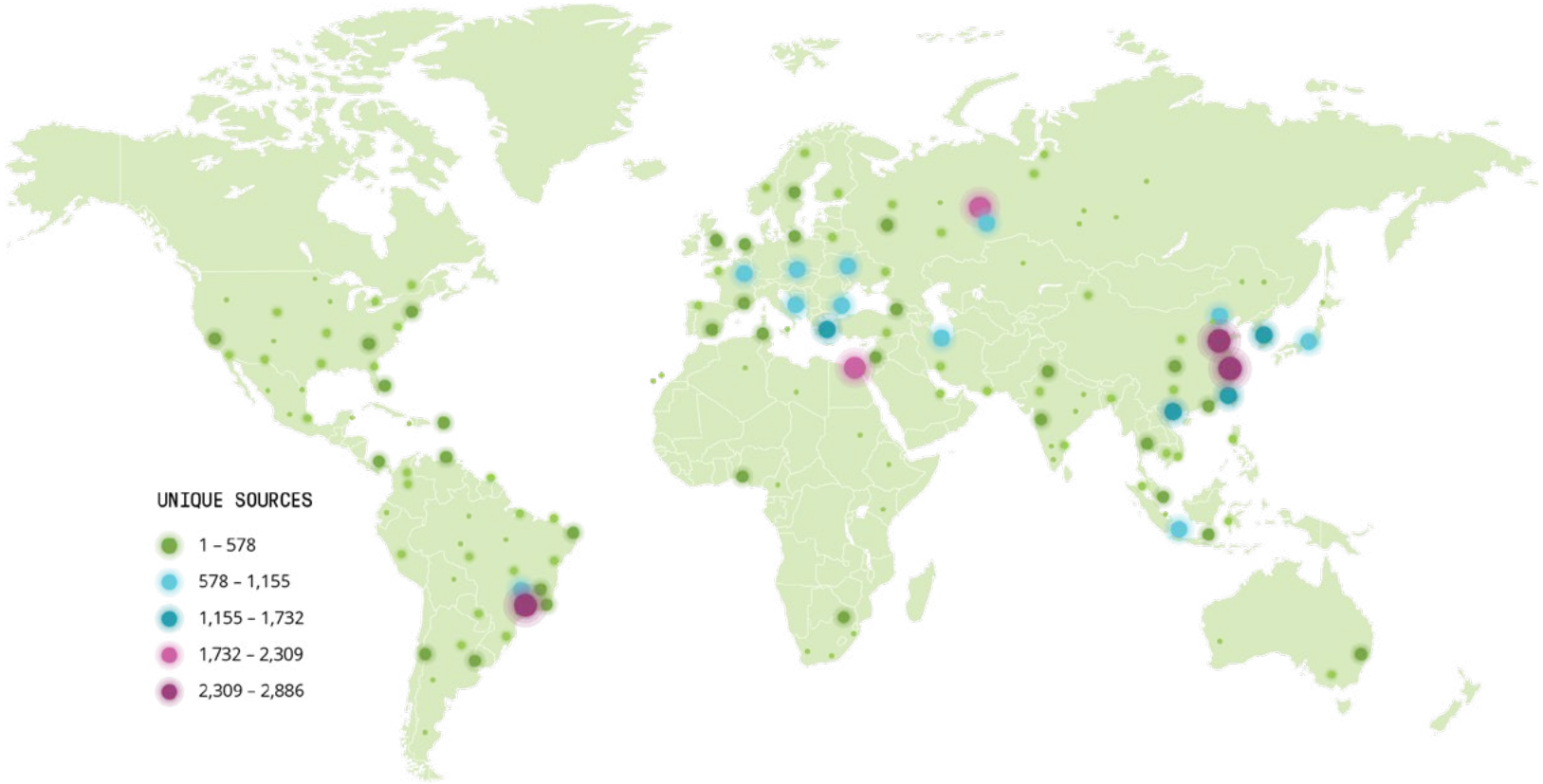


Figure 5: Brute-Force IoT Activity by Country

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

MIRAI

REMAINS THE KING
OF IoT MALWARE

TORii
+
VPNFILTER

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.

THE TAKEAWAY

In the second half of 2018, we saw threat actors building crimeware that's cheaper and easier to deploy—and more persistent once installed.

At the same time, many groups applied business best practices that further extend the reach of attacks, while making it even easier for customers to access and leverage malicious software and DDoS attack tools.

The ASERT team continues to monitor the threat landscape and report on new actors, malware under develoment, and increasingly sophisticated techniques deployed. For a detailed summary of the latest trends, download the updated NETSCOUT Threat Intelligence Report for the second half of 2018.

READ THE FULL REPORT

APPENDIX

[1] www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

[2] www.recordedfuture.com/chinese-threat-actor-tempperiscope/

[3] securelist.com/luckymouse-ndisproxy-driver/87914/

[4] unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

[5] netscout.com/blog/asert/tunneling-under-sands

[6] unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/

[7] unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/

[8] www.eset.com/us/about/newsroom/corporate-blog/what-you-need-to-know-about-lojax-the-new-stealthy-malware-from-fancy-bear/

[9] blogs.360.cn/post/APT_C_01_en.html

[10] netscout.com/blog/asert/stolen-pencil-campaign-targets-academia

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

[12] netscout.com/blog/asert/fast-furious-iot-botnets-regifting-exploits

[13] netscout.com/blog/asert/dipping-honeypot

NETSCOUT®

© 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.

SECR_APTCRIMEWARE2H2018_EN-1901