

NSFOCUS

2018 Botnet Trend Report



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 Information Technology Co. Ltd., the company has operations in the Americas, Europe, the Middle East and Asia Pacific.

About NTI

NTI is the NSFOCUS Threat Intelligence division of NSFOCUS. With over 90 researchers around the world, NTI's charter is to help customers better defend against current and next-generation cyber threats. NTI provides an array of threat intelligence products and services.

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

1. Executive Summary	2
2. Overview	4
3. Botnet Behavior	6
3.1 Botnet Instructions	7
3.1.1 Behavior Seen	7
3.1.2 Analysis	8
3.2 Family Activity	10
3.2.1 Behavior Seen	10
3.2.2 Analysis	12
3.3 Geographical Distribution	14
3.3.1 Behavior Seen	14
3.3.2 Analysis	20
3.4 DDoS Attacks	21
3.4.1 Behavior Seen	21
3.4.2 Analysis	23
3.5 Delivery and Propagation	25
3.5.1 Behavior Seen	25
3.5.2 Analysis	28
4. Active Botnet Families and Attack Payloads	30
4.1 Gafgyt: The Choice for IoT Botnets	31
4.2 BillGates: Best Cross-Platform Family	34
4.2.1 Evolution of the Family	34
4.2.2 Analysis	37
4.3 XMRig: Cryptomining For Fun and Profit	39
4.4 Satan: Evolving Ransomware	43
5. Conclusion and Recommendations	45

1

Executive Summary

Botnets, one of the oldest threats on the internet, are still the most popular weapon in a hacker's arsenal. They offer ease of use, flexibility, and high availability, traits ideal for launching large-scale lethal cyber-attacks around the world.

Current, accurate and high-value threat intelligence is one of the best defenses against Botnets. Intelligence about global botnet activity allows analysis of attacks to identify and predict botnet behavior based on attack types, attack sizes, targets and other indicators. NSFOCUS has developed profiles on 82 IP Chain-Gangs, groups of bots from multiple botnets acting in concert during specific cyber-attack campaigns. Understanding botnets in general and IP Chain-Gangs in particular helps improve defensive strategies and, thus, better able to mitigate attacks.

Through continuous monitoring and research of botnets, NSFOCUS Security Labs has discovered significant changes taking place in the coding of malware used to create bots, operations & maintenance of botnets and IP Chain-Gangs, as well as the monetization of these attackers in 2018.

Poor security has made IoT platforms the bot of choice over historically Windows based systems. And with billions of IoT devices online and millions more each week, attack capability is ever increasing to massively destructive levels.

Much of the newer malware shows mature coding practices leading to more efficient software that can launch multiple and different types of attacks than just DDoS. Network/system scanning, cryptomining and ransomware are only some of the capabilities of these newer Swiss Army knife bots.

Rising from these more mature malware developers are several malware families that are preferred because they are more stable with access to global Command & Control (C&C) servers hosted on high-bandwidth internet connections. Less C&C servers with access to high-speed internet reduce the complexity and O&M requirements for managing botnet networks.

Controllers of botnets have started to monetize their capabilities both by offering Botnet-as-a-Service (BaaS), DDoS-as-a-Service (DaaS) as well as turning them in to crypto-miners for profit and for hire.

In the future, defeating botnets will require not only local security protection, but also a concerted effort by governance organizations worldwide to enforce security best practices to reduce the proliferation of botnets and their use.

2

Overview

Botnets have evolved since 2017. New active families and platforms have become dominant. Attack types used have also changed.

In 2018, NSFOCUS detected 111,472 attack instructions from botnet families that were received by a total of 451,187 attack targets, an increase of 66.4% from last year. On average, each attack instruction was received by four attack targets. However, the number of active botnet families issuing more than 100 attack instructions decreased from 12 to 9. Evidently, several full-fledged botnets have come to dominate the cyberthreat landscape, demonstrating that the botnet lifecycle includes a maturity phase.

Except for the BillGates family that erupted at the end of 2017, botnet families' mayday, Gafgyt, and Mirai were the most active, contributing 21%, 9.5%, and 7.4% of attack instructions respectively.

IoT platforms, especially those based on Linux, became the platforms of choice for command & control (C&C) servers surging from 4.4% in 2017 to 31% in 2018, indicating that IoT platforms are becoming the frontline of botnet attacks and defense.

Geographically, the USA, having the most C&C servers (30.64%), is also the most targeted victim of botnet attacks (47.2%). China came in second for both number of C&C servers and targeted victims (29.79% of C&C servers and 39.78% of victims of attacks).

The most active botnet family types were related to ransomware, cryptomining, and DDoS. In addition, banking trojans, remote access trojans (RATs), and account hacking trojans are were seen in high profile campaigns.

There was a shift for DDoS botnet families to use multi-vector attacks and the becoming the dominant DDoS attack types. Botnets monitored by NSFOCUS have issued DDoS attack instructions to carry out nearly all kinds of attacks such as TCP flood, SYN flood, ACK flood, UDP flood, DNS flood, HTTP flood, and ICMP flood. Of these attack instructions, 39.8% and 35.5% are respectively issued for UDP and TCP flood attacks, also being the top DDoS attack types seen.

Botnets were not short on propagation and delivery. Among botnet intrusion logs analyzed in 2018, attack using weak password cracking accounted for 55.3%. Botnet families used 54 topical vulnerability exploits, 90.7% of which are against IoT devices.

3

Botnet Behavior



This chapter discusses various aspects of botnet behavior. Behavioral characteristics include activity level of botnets overall and per botnet family, DDoS attack characteristics, C&C server use and distribution, and geographical locations of attack victims. Also discussed are characteristics of the most active botnet families themselves.

3.1 Botnet Instructions

3.1.1 Behavior Seen

Botnets receive instructions from C&C servers. Instructions detected in 2018 can be divided into high-threat instructions and low-threat instructions. The former includes attack, attack stop and self-replication/download instructions. The latter include heartbeat, information collection, and other communication instructions. Figure 1 shows the distribution of instruction types.

Figure 1 Distribution of instruction types

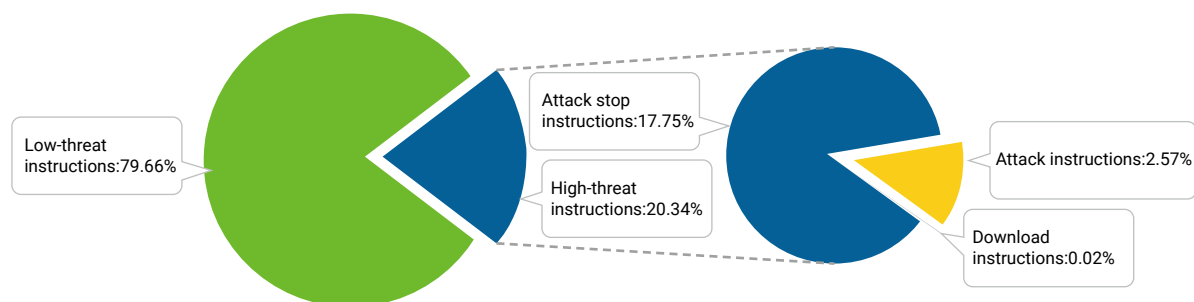
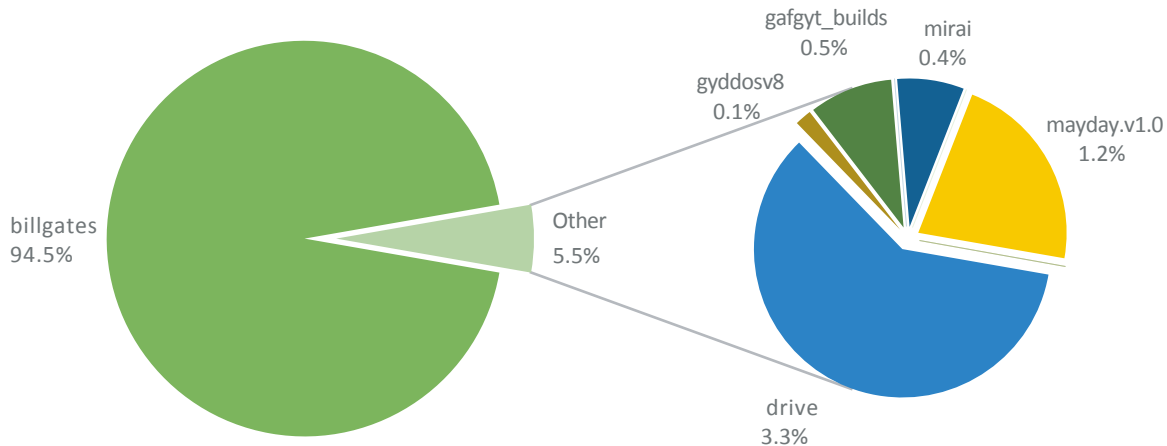


Figure 2 shows the distribution of attack instructions by botnet family. We can see that BillGates generated the most attack instructions.

► Botnet Behavior

Figure 2 Distribution of attack instructions by botnet family



botname

■ billgates	■ drive	■ mayday.v1.0
■ gafgyt_builds	■ mirai	■ gyddosv8
■ microfake_s	■ DDOS.NITOL.S1P0R3.WV	■ artemis
■ DDOS.NITOL.S0P1R1.WU	■ DDOS.NITOL.S0P0R3.WV	■ DDOS.HYBRIDMQ.S0P0R0.IV

3.1.2 Analysis

Botnets Take Low and Slow Approach Through Reconnaissance and Testing

NSFOCUS has observed botnet controllers behaving more cautiously by repeatedly conducting reconnaissance and testing activities before issuing attack instructions.

It is generally accepted that the botnet kill chain consists of two phases: pre-intrusion and post-intrusion. Controllers are very careful about delivering malicious programs prior to intrusion. They often try to reduce the odds of being detected by forging source IPs and domains, using multilingual texts, and adding misleading or meaningless information. In contrast, the delivered malicious programs behave more recklessly; they may use simple communication formats and exposed attack sources. Thus, detection of malicious behavior is traditionally performed at the post-intrusion phase.

Statistics show that many botnet families remain cautious during the "control" and "execution" phases. Botnet controllers often use information collection instructions to detect honeypots and obtain information about the host and running process. Using this information to better detect the running environment adds to the difficulty of spoofing them through sandbox masquerading.

Figure 1 shows the percentage of attack stop instructions and attack instructions among high-threat instructions. We see from this figure that botnet controllers minimize manipulating the infected bot. We suspect that the far larger number of attack stop instructions sent are redundant to guarantee that controlled nodes hosted on poorer performance networks can be made dormant in order not to be easily identified after the attack.

Based on how successful and prolific certain botnet attacks are, the above-mentioned information collection and attack stop instructions greatly raise the probability of survival of individual bots, making these botnet families less likely to be detected and tracked.

Several Mature and Full-Featured Botnet Families Starting to Dominate

Organized botnet groups prefer using stable botnet family versions and C&C servers. This reveals that botnet lifecycle includes a maturity phase.

According to statistics, although each botnet family has diverse variants and countless C&C servers distributed throughout the world, most of the effective attack instructions are issued from just a small group of C&C servers.

Let us use the BillGates botnet, the 2018 Q4 quarterly champion for the most active families, as an example. Among all its C&C servers detected in 2018, the two most active IP addresses, 23.*.*.131 and 207.*.*.245, issued more than 90% of all effective attack instructions. Of the family's four variants in the wild, the original version discovered is the most active¹.

Interestingly, different controllers exercise version control and C&C in a remarkably similar way, whether using DDoS families or families delivering other types of payloads, and on both mainstream and IoT

1 For detailed description of the BillGates family, see BillGates: Best Cross-Platform Family.

► Botnet Behavior

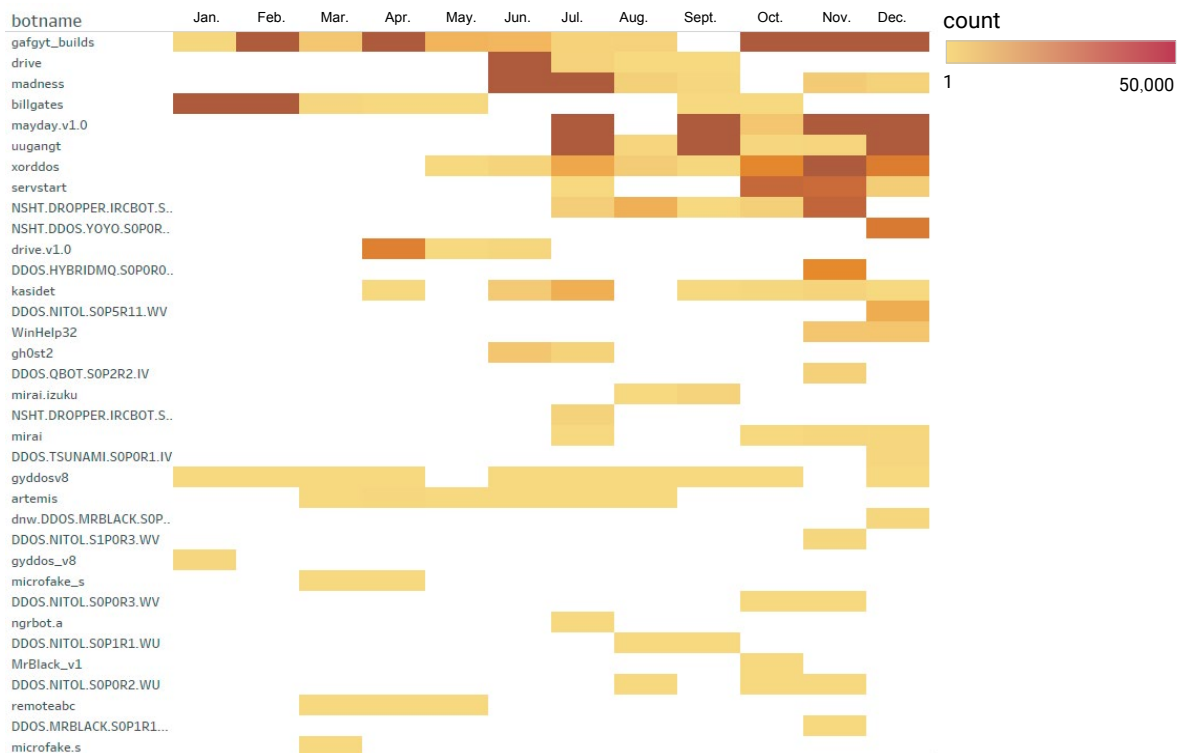
platforms. Controllers using long-established and well-known families launch most attack tasks. While large numbers of attack instructions often lead to massive attack events, a mature full-fledged attack group with several elite bots receiving less attack instructions can impose far more damage than a looser collective of bots that churn out a larger number of attacks. NSFOCUS believes that improving our ability to detect and track different high-threat variants is important.

3.2 Family Activity

3.2.1 Behavior Seen

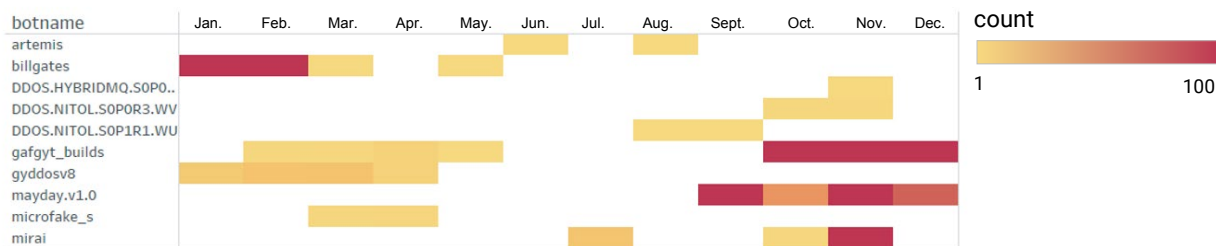
In 2018, a total of 35 active families were found to issue more than 100 botnet instructions, accounting for 24% of all known families. Several families with the highest level of instruction activity accounted for most of the malicious activities throughout 2018.

Figure 3 Monthly distribution of instructions from each family



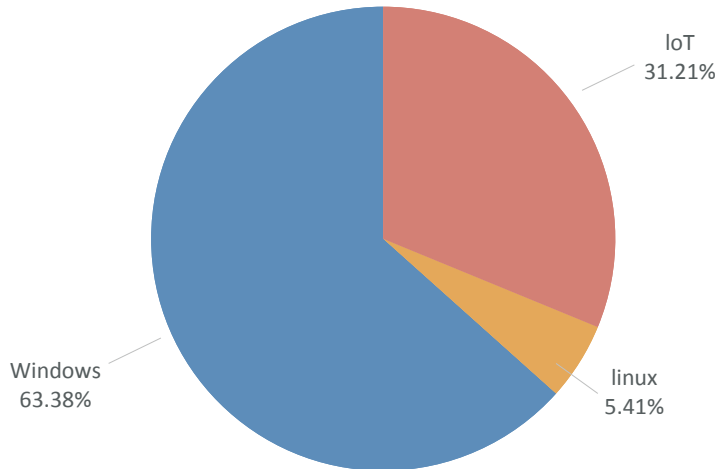
As shown in Figure 4, the most active botnet families issuing instructions were active from January to March and September to December, but became relatively lethargic in June and July, when a smaller number of instructions issued.

Figure 4 Monthly distribution of attack instructions from most active families



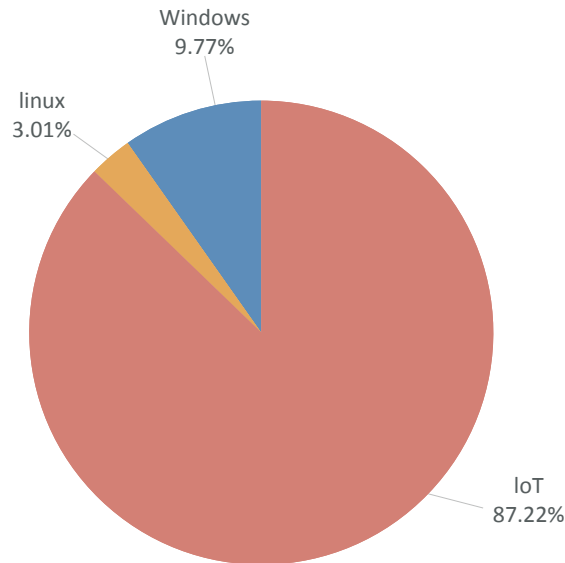
As for platforms hosting C&C servers, families using IoT platforms, though smaller in quantity, were more active, attracting 87% of attackers.

Figure 5 Distribution of C&C server platforms used



► Botnet Behavior

Figure 6 Distribution of C&C server platforms launching attacks



3.2.2 Analysis

IoT Devices with Poor Security Favored by Botnets

In 2018, botnets were shifting from Windows platforms towards Linux and IoT platforms, leading to the fast decline of older Windows-based families and the thriving of new IoT-based ones.

In previous years, Windows platforms were the primary target of all sorts of malware. Research shows that the longest established families, including previous closely monitored families such as Huigezi, gyddos, and Darkshell, mainly run on Windows platforms. Therefore, malicious behavior detection was based around Windows platforms at that time. In 2018, as variants from Gafgyt and Mirai families grew at an explosive rate, we shifted our detection focus to other platforms from Windows.

The shift of attack platforms is due to three factors:

1. Full upgrade of Windows platforms. According to StatCounter² (an analysis website), before

² <http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide>

December 2018, Windows 10 had had a global share of 52.36%, overtaking Windows 7 as the most popular Windows operating system. Thanks to its forced update policy, Windows 10 significantly improves over Windows 7 security such that it can block much more malware prior to intrusion.

2. Out-of-date security of IoT platforms. While the total number of IoT devices globally surges rapidly and IoT product lines are increasingly diversified, IoT devices still have poor security. Insecure firmware and communication protocols lead to numerous vulnerabilities in IoT platforms. Meanwhile, IoT device users' lack of security awareness is a contributing factor to IoT security issues. Currently, a great many IoT devices still use default usernames and passwords, making it possible for hackers to use a wide range of cracking tools to take control of these devices and turn them into new weapons. This is one of the reasons the state of California passed the first of its kind IoT security legislation in the USA, if not the world³.
3. Botnet market segmentation. According to rough statistics on platforms, Windows platforms usually run high-value targets or hold sensitive user information, making them the primary target of information stealing groups. Active families rely on successful banking trojans and ransomware, both of which feature a high degree of covertness. In contrast, Linux platforms run high-performance devices and families usually install multipurpose trojans on these platforms to execute a variety of malicious activity predominately cryptomining. Characterized by their ubiquitous and ease of penetration, IoT devices have also grown to be the new hotbed of DDoS attacks.

While California requires security vendors to improve their security implementations, vendors themselves need to give serious thought about how to respond to changing attack platform segmentation when implementing in-product defenses.

³ Companion bills SB-327 and AB-1906 in the state of California mandate all IoT devices sold in California will implement “reasonable” security features, such as forcing users to change default passwords during installation or provide a unique password on each device at manufacture.

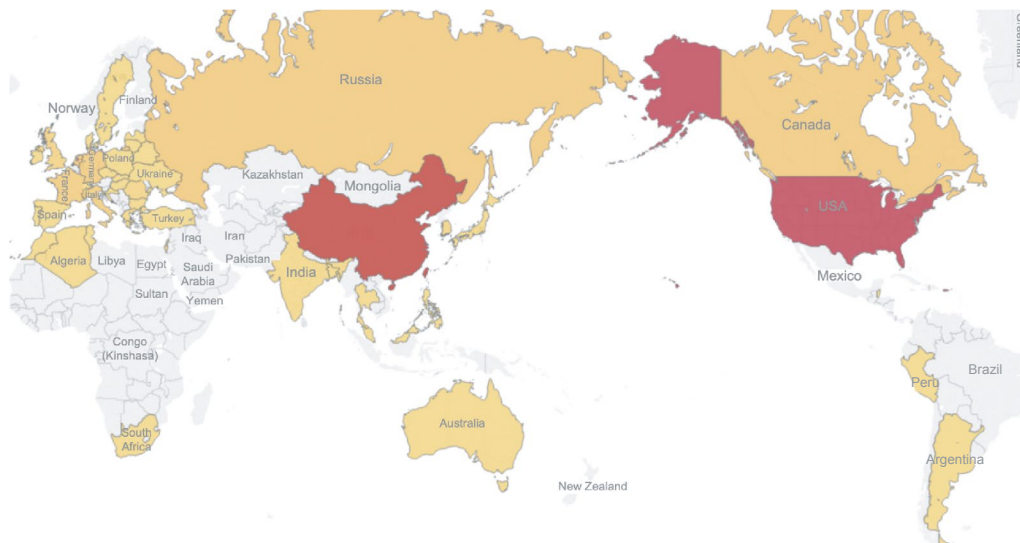
► Botnet Behavior

3.3 Geographical Distribution

3.3.1 Behavior Seen

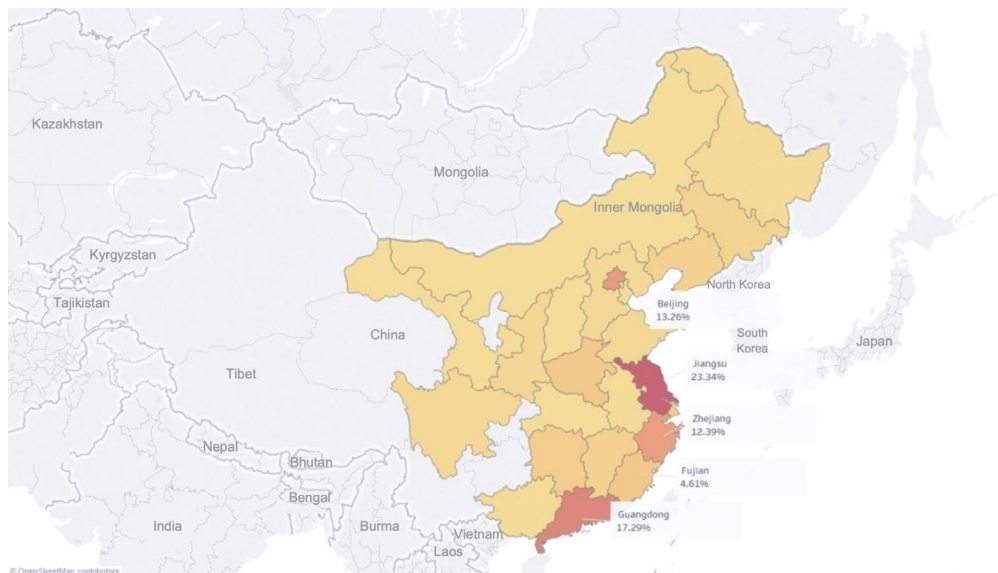
According to geographical analysis of IP addresses, 2018 saw most new C&C servers in the USA (30.64%), closely followed by China (29.79%). Other top C&C hosting countries include Canada, Russia, Germany, France, and Italy.

Figure 7 Global distribution of C&C servers



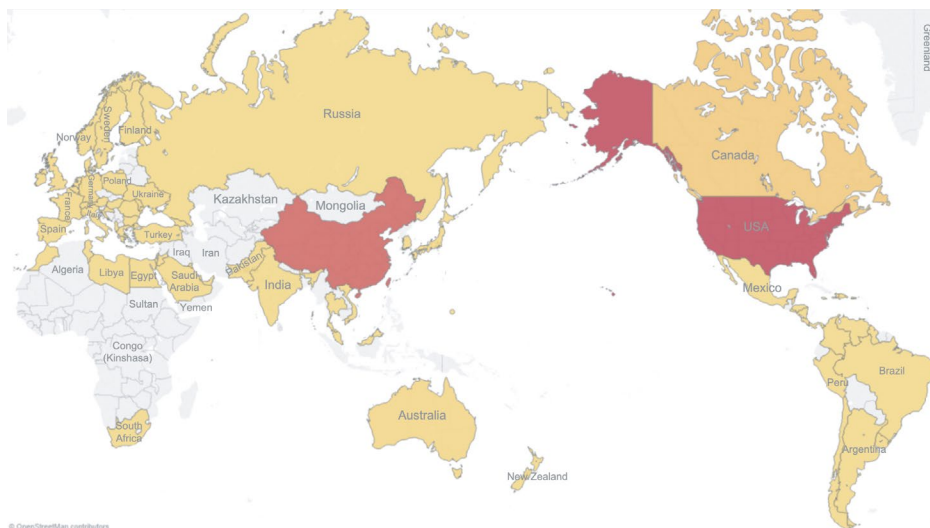
In China, most C&C servers were scattered along the eastern coastal area, with over 60% located in Jiangsu, Guangdong, Beijing, and Zhejiang.

Figure 8 Distribution of C&C servers in China



In terms of the distribution of botnet attack victims, the USA (47.2%) and China (39.78%) were two worst-hit countries. Canada, Japan, and Australia were also affected by botnet attacks.

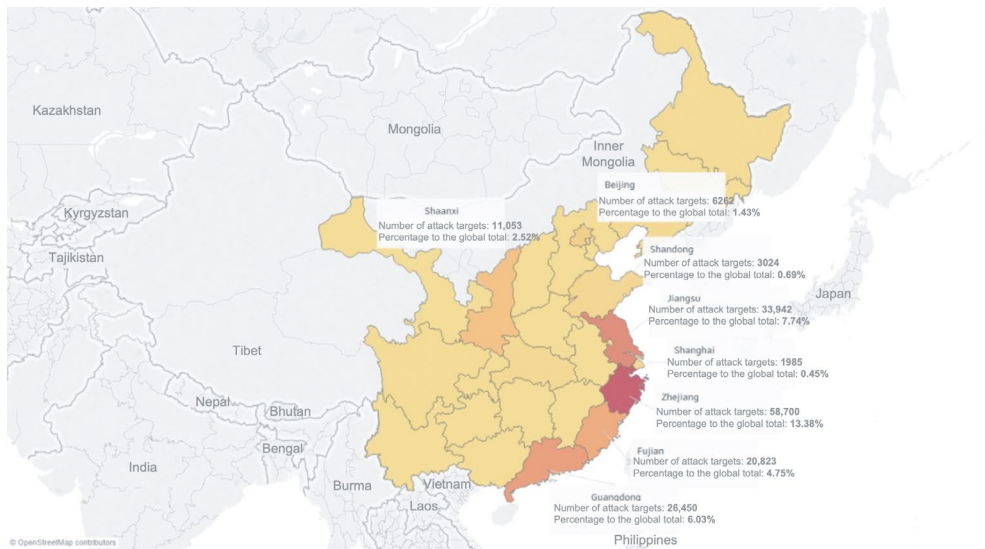
Figure 9 Global distribution of attack targets



► Botnet Behavior

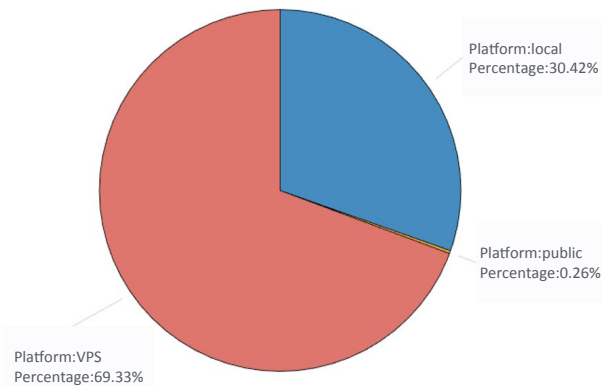
In China, botnet attacks mainly targeted economically developed provinces and municipalities such as Jiangsu, Zhejiang, Guangdong, and Beijing, where C&C servers are densely distributed, and all sorts of attacks are active. It is worth noting that Shaanxi became a new favored attack target in central China.

Figure 10 Distribution of attack targets in China



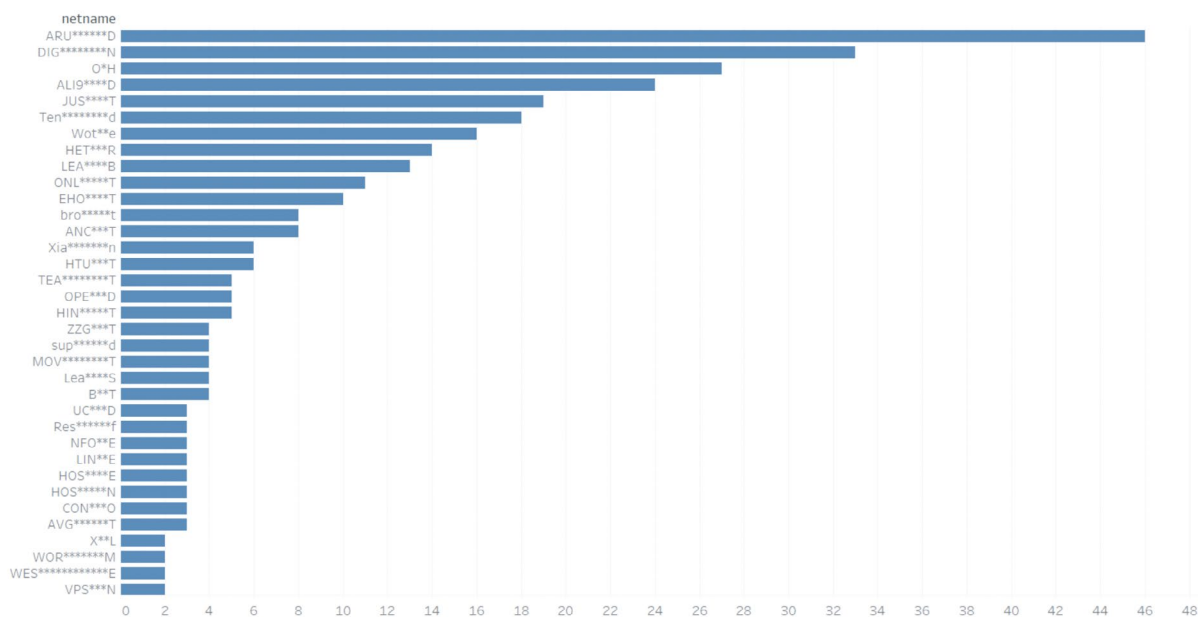
According to analysis of platforms, most C&C servers are deployed on virtual private servers (VPSs) located in private clouds.

Figure 11 Distribution of C&C server platform deployment



Further analysis of VPS providers suggests that well-known providers in China and globally were especially favored by botnets.

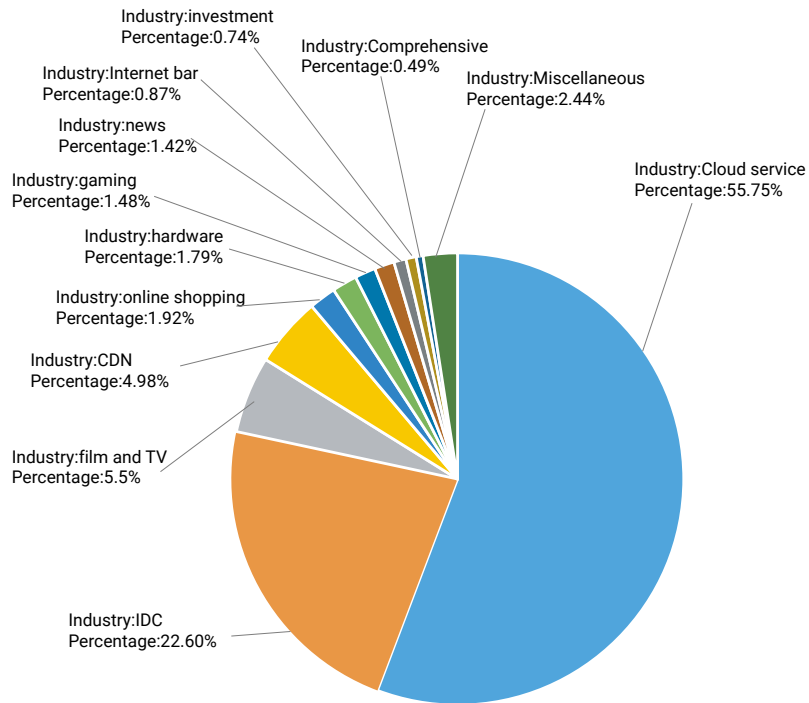
Figure 12 Global distribution of targeted VPS providers



After deduplicating IP addresses, we worked out the distribution of attacked IP addresses by industry. As shown in the following figure, botnets are indiscriminate and attack almost all computer industries. Analysis of IP addresses with a clear attribution show that Internet cloud providers and traditional IDC providers received most attacks.

► Botnet Behavior

Figure 13 Distribution of attacked IP addresses by industry



Studying targeted IPs themselves is informative if not entertaining. Statistical analysis show that gambling and porn websites were the most targeted, with the IP address, 162.218.*.142, suffering 29,161 (an average of 79 per day) DDoS attacks throughout 2018.

3.3.2 Analysis

Most Botnets Deployed on VPSs for Economic Reasons

Low-cost virtual private servers, which have little security oversight, have become the main target for hosting command & control servers.

When setting up C&C servers, botnet groups will attempt to take over any available system. Having evolved past traditional on-premises servers, botnet groups now target platforms such as cloud service providers, compromised smart devices, public platforms where custom contents can be posted, and exploitable chat tools such as Slack and Telegram for C&C server deployment. As popular as those platforms have become, VPSs are the most sought-after platforms, increasing share among C&C deployment platforms in recent years.

Studying geographical locations of C&C servers newly added in 2018, we found that a great number of IP addresses belonged to devices residing in equipment rooms of several renowned VPS vendors. These C&C servers set up on VPSs have a long survival period and a high activity level.

VPSs' following features make them important tools for botnet attacks:

1. **Price.** In recent years, emerging VPS service providers have sprung up all over the world. The price competition in the VPS market is becoming increasingly intense, thus bringing the C&C server deployment cost down. This provides an incentive for mercenary hacking groups to move C&C servers to VPSs.
2. **Covertness.** Currently, many VPS providers exercise marginal review and control over user registration information, thus offering opportunities for hackers to easily hide their real identities.
3. **Flexibility.** VPS hosts are easy to deploy and destroy, allowing botnet groups to develop new ways to evade detection and crackdown by security vendors.

Thus, VPSs provide a new level of flexibility for deploying C&C servers at a much lower cost.

In China, there is a different type of dark web or underground hosting activities considered illegal there. Since there are no protections, the hacking underground controlling botnets has made a huge profit

preying on industries like gambling and porn.

Underground industries represented by gambling and porn, as well as illegal shopping sites, have been using home-grown servers or non-standard managed hosts as main operation platforms. These platforms have little, or poor security protections deployed at best and O&M personnel lack sufficient security awareness. This lack of security makes these platforms popular ransom targets of botnet groups using DDoS attacks to take their operations hostage.

3.4 DDoS Attacks

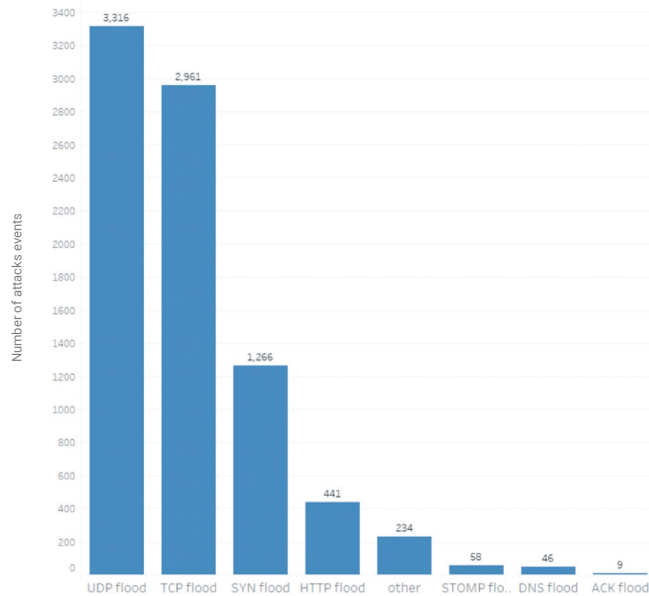
3.4.1 Behavior Seen

Effective attack instructions are botnet attack instructions that control a task other than starting and stopping. Effective attack instructions captured in 2018 included DDoS, Local Area Network (LAN) scanning, and vulnerability exploits among other types of attacks. There were 440,000 DDoS attack instructions issued from botnet families, constituting most effective attack instructions. Categorizing attack instructions by source IP address, target IP address, attack type, and attack initiation time, we found that the DDoS attack instructions were responsible for 8,332 attack events. From key indicators of these attack events, we discovered that UDP and TCP flood attacks, with a total percentage of 75.34%, formed the biggest part of attacks. Figure 16 shows the numbers of various DDoS attacks.

In addition, we captured numerous attack instructions directly against anti-DDoS service providers. These instructions, whether for directly attacking providers, testing anti-DDoS capabilities, or just showing off their botnet attack capabilities, reveal that botnets and their attack controllers still hold the initiative on the DDoS battlefield and need to be taken seriously. Many anti-DDoS providers can mitigate massive attacks by distributing the attack traffic across DDoS scrubbing centers. But a massive attack directed at one or few scrubbing centers could cause great impact to the provider.

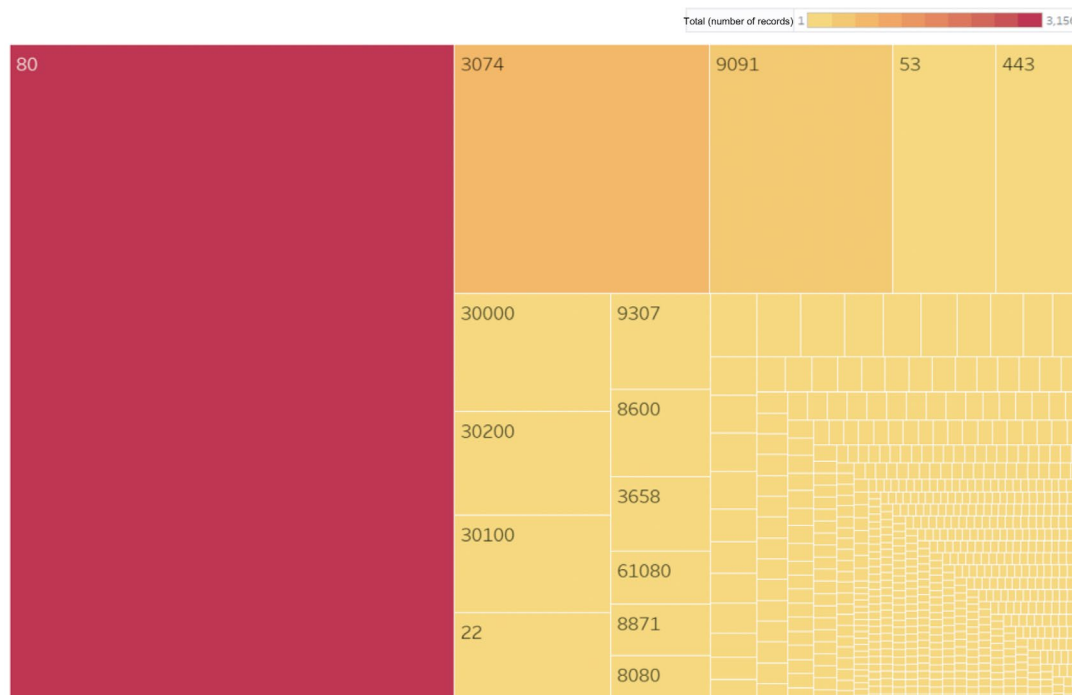
▶ Botnet Behavior

Figure 16 DDoS attack type distribution by count



In terms of ports, port 80 was still most frequently targeted and ports 22, 25, 53, and 443 were also favored by DDoS attacks. It should be noted that two attack events, respectively led by the Gafgyt family and the BillGates family, were against ports 3074 (Xbox Live, both TCP and UDP) and 9091 (TCP: CiscoSecure and Transmission web UI, UDP: xmltec-xmlmail and QuickTime server) which were found to be easy targets. The two attack events are discussed in the Analysis section.

Figure 17 Distribution of target ports



3.4.2 Analysis

Reflection Attacks Making a Resurgence

At the end of 2018, the number of UDP flood attacks rose unexpectedly, surpassing TCP and SYN flood attacks to become the dominant DDoS attack type based on attack DDoS instructions. This may be related to the popularity of some UDP based reflection attacks.

Reflection DDoS attacks amplify the amount of UDP response traffic compared to the amount of request traffic initiating the attack such as a small DNS query returning a response with a lot of DNS data. Reflection attacks provide attackers with a lot of flexibility because they can utilize a number of different UDP services for attacks, yet are difficult to detect, trace and prevent. Because of these characteristics, such attacks have long been popular with hackers in conjunction with various botnet families. In 2018 H1, NSFOCUS and several other security vendors detected Memcached-

► Botnet Behavior

based reflection DDoS attacks which generated several massive DDoS attacks, the size of which were previously unseen. NTP reflection and SSDP reflection attacks have also been popular in 2018. What is concerning is the multi-protocol capabilities being deployed in newer malware which allows customization of UDP flood instructions, giving botnet controllers the ability to launch multiple DDoS reflection attacks using different protocols simultaneously or in series.

Figure 18 shows a typical reflection attack instruction sequence. During this sequence, the C&C server dispatches download instructions to direct the controlled end to download the reflector list. The controller then issues customized UDP flood instructions directing the bot to launch NTP reflection attacks against specific target IP addresses.

Figure 18 NTP reflection attack instruction sequence

```

...Linux4.10.0-28-generic.....
1*4294MHZ.....1998MB.....
(null).....wget http://216.176.179.106:9090/
ntpamp.txt.....
2.0.....d`.>.>.....d`.>..q.....q.....>.....e.q
..q.....qp..q..q.....|..q......x.....:K..|.....@.
@. @. @.....|.....@.....@.....h.....@.....
192.133.....155.....
P.....F.....
.....d`.>.>.....d`.>..q.....q.....>.....
..e.q.....qp..q..q.....|..q.....x.....:K..|.....
.....$......p.....1.....|.....x.....(..q.....|4.....:0.....|.....

```

Considering the number of UDP flood attack instructions seen being issued in the wild, we believe governance crackdown on poorly secured reflection sources (as was recently done in China and other countries for DNS servers) is the most effective and economical defense against reflection attacks. After that, organizations still need to implement defensive capabilities to defend against other common UDP flood and reflection attacks.

Internet Gaming Users Fall Victim to Botnet DDoS Attacks

Port 9091 is used by a variety of services including email protection software GFI MailEssentials, BitTorrent client Transmission, and Openfire chat & messaging server. In the first half of 2018, we observed an attack event where BillGates carried out DDoS attacks against port 9091 on certain IP addresses in South China. Although we could not verify if these targets had port 9091 open, if so, the

DDoS attacks would have devastated them.

Port 3074 is used by Microsoft's Xbox home gaming systems to participate in the Xbox Live service. The Gafgyt family launched numerous attacks against this port in Q4 2018. During those attack events, the attacker mounted hybrid DDoS attacks against port 3074 on each IP address monitored. As personal devices are less capable of resisting DDoS attacks than enterprise devices, these attacks could block network communications of host devices immediately, leading to players going offline. These kinds of attack behavior have been seen used against many online multiplayer and esports services, allowing attackers to manipulate matches by increasing the latency of other players or completely knocking them offline.

From the above, we find that targeted DDoS attacks are easy to launch and capable of doing specific, yet extensive damage. If these kinds of attacks become more prevalent, online service providers should consider including basic DDoS protection for users. This could, however, greatly increase the operating costs of online gaming services and may actually be cost prohibitive in which case, revenues could decline as users become frustrated from these tactics.

3.5 Delivery and Propagation

3.5.1 Behavior Seen

Studying 25 million intrusion logs extracted from NSFOCUS managed services customers in 2018, we found that approximately 14 million logs recorded intrusions using weak password cracking mainly against Telnet, RDP, and SSH services. From other logs, a large portion of intrusions seen were vulnerability-based intrusions, with 54 vulnerabilities frequently exploited (Shown in the table) mostly against routers and IoT cameras.

Table 1 Frequently Exploited Vulnerabilities

VULNERABILITY	AFFECTED DEVICES
CVE-2018-10561 & CVE-2018-105620	GPON Routers - Authentication Bypass / Command Injection
CVE-2008-0149 & CVE-2008-0148	Tutos
CVE-2018-14417	SoftNas
CVE-2014-9094	Wordpress PHP

 Botnet Behavior

VULNERABILITY	AFFECTED DEVICES
Dlink CNVD-2014-01260	D-Link DIR-815
CVE-2014-8361	Linksys
Netgear setup.cgi unauthenticated RCE CVE-2017-17215	Different devices using the Realtek SDK with the miniigd daemon
Eir WAN Side Remote Command Injection	DGN1000 Netgear routers
HNAP SoapAction-Header Command Execution	Huawei HG532
CCTV/DVR Remote Code Execution	Eir D1000 routers
JAWS Webserver unauthenticated shell command execution	D-Link devices
UPnP SOAP TelnetD Command Execution	CCTVs, DVRs from over 70 vendors
Netgear cgi-bin Command Injection	MVPower DVRs, among others
Vacron NVR RCE	D-Link devices
CVE-2015-2280	Netgear R7000/R6400 devices
CVE-2014-6271	Vacron NVR devices
CVE-2014- 8361	AirLink101
AVTECH Unauthenticated Command Injection	multi-platform
Google Android ADB Debug Server - Remote Payload Execution	Realtek SDK based devices
CVE-2018-11336	AVTECH IP Camera/NVR/DVR Devices
AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities	Android
Billion / TrueOnline / ZyxEL Routers - Multiple Vulnerabilities	FASTGate
CCTV-DVR Over 70 Vendors RCE	AVTECH devices
CVE-2012-3001	Hardware
CVE-2015-7254	DVR
CVE-2016-1555	Linux
CVE-2016-6277	Huawei Router HG532e
CVE-2017-6334	Netgear Devices
CVE-2017-8221	NETGEAR R7000 / R6400
CVE-2017-8224	NETGEAR DGN2200
CVE-2018-17173	Wireless IP Camera (P2P) WIFICAM
D-Link - OS-Command Injection via UPnP Interface	Wireless IP Camera (P2P) WIFICAM
D-Link DCS-930L - (Authenticated) Remote Command Execution	LG SuperSign EZ CMS 2.5
D-Link DIR-600 / DIR-300 (Rev B) - Multiple Vulnerabilities	D-Link router
D-Link DIR-645 / DIR-815 - 'diagnostic.php' Command Execution	D-Link DCS-930L
D-Link DIR-825 (vC) - Multiple Vulnerabilities	D-Link DIR-600
D-Link DIR-8xx Routers - Root Remote Code Execution	D-Link DIR-645
D-Link DSL-2750B RCE	D-Link DIR-825
Eir D1000 Wireless Router - WAN Side Remote Command Injection	D-Link DIR-8xx Routers
EnGenius EnShare IoT Gigabit Cloud Service 1.4.11 - Remote Code Execution	D-Link DSL-2750B
Hadoop YARN ResourceManager - Command Execution	Eir D1000 Wireless Router
Linksys WAG200G - Multiple Vulnerabilities	Linux
MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution	Hadoop YARN ResourceManager
NetGain Enterprise Manager 7.2.562 - 'Ping' Command Injection	Linksys WAG200G
NETGEAR Voice Gateway 2.3.0.23_2.3.23 - Multiple Vulnerabilities	MVPower DVR
	NetGain Enterprise Manager
	NETGEAR Voice Gateway

VULNERABILITY	AFFECTED DEVICES
NETGEAR Wireless Management System 2.1.4.15 (Build 1236) - Privilege Escalation	NETGEAR Wireless Management System
NUUO NVRmini - 'upgrade_handle.php' Remote Command Execution	NUUO NVRmini
NUUO NVRmini 2 3.0.8 - Remote Code Execution	NUUO NVRmini
NUUO NVRMini2 3.8 - 'cgi_system' Buffer Overflow (Enable Telnet)	NUUO NVRmini
ThinkPHP 5.0.23/5.1.31 - Remote Code Execution	ThinkPHP based devices
WePresent WiPG-1000 - Command Injection	WePresent WiPG-1000
WRT120N 1.0.0.7 - Remote Stack Overflow	Linksys WRT120N

All vulnerabilities listed in the previous table were exploited by botnet families that have been seen across different platforms. Variants from the very active Gafgyt family carried out a total of 43 vulnerability exploits⁴. One strain of OrkSec, a Mirai variant botnet discovered in H2 2018, exploited 22 vulnerabilities.

Table 2 Vulnerabilities Exploited by OrkSec

VULNERABILITY
CVE-2018-10561, CVE-2018-10562
CVE-2015-2280
CCTV/DVR Remote Code Execution
CVE-2014-6271
CVE-2014-9094
Dlink
CVE-2017-17215
JAWS Webserver unauthenticated shell command execution
CNVD-2014-01260
Netgear setup.cgi unauthenticated RCE
Vacron NVR RCE
CVE-2014-8361
CVE-2018-14417
Eir WAN Side Remote Command Injection
CVE-2008-0149 CVE-2008-0148
Vacron NVR RCE
EnGenius RCE
AVTECH Unauthenticated Command Injection
adb-exploit
CVE-2018-11336
NUUO OS Command Injection

(Some vulnerabilities were not numbered but named by Vendor Name + Vulnerability Exploited.)

⁴ For detailed description of the IoT Botnet Gafgyt family, see Gafgyt: The choice for IoT Botnets.

3.5.2 Analysis

New Platforms with Poor Security Fueling Botnet Spreading

Traditional attacks using weak password scanning and social engineering are unable to meet the demand requiring the rapid growth of botnets. Instead, more and more malicious programs are using modules that can exploit dozens of vulnerabilities to first gain a foothold into an environment and then quickly spread to nearby platforms that have not been properly patched or maintained.

Malicious programs usually spread through the following techniques:

- Using spam to trick users into clicking an eye-catching malicious link
- Deploying malware on user's computers by browsing or being redirected to a malicious webpage
- Masquerading as a normal software patch update
- Exploiting poor passwords
- Exploiting vulnerabilities in systems or platforms to gain privileges

The first three usually required some type of manual intervention affected by social engineering to turn a host into a zombie bot. However, as users become more security conscious those methods become less effective.

Today, attackers exploit default passwords and vulnerabilities as a more effective way to propagate bots. This makes IoT platforms with multiple security vulnerabilities the primary victims. Common IoT devices such as routers and cameras, once configured, stay permanently online and often lack timely updates. Since IoT devices may not be updated for months, even years, they have a high probability of being exploited. The incredibly fast spread of the Mirai virus is a testament to that. Hundreds of thousands of IoT devices have been compromised to date and are becoming a dire threat to public networks.

Much more attention is needed from not only IoT developers, but security researchers and end users as well. Users should ensure their devices are better secured by updating drivers, applying patches to fix vulnerabilities where possible, and changing default passwords immediately. Developers should be

more responsible for fixing issues with their products and setting good default security controls. The state of California has recently passed new laws to ensure IoT vendors be more responsible. Security researchers should identify how to enhance security protections for IoT platforms to better defend against invasion and exploitation, especially with the historically poor security practices of both users and developers.

4

Active Botnet Families and Attack Payloads

A network diagram background consisting of various sized circles (nodes) connected by thin lines (edges), representing a complex network structure. The nodes are in shades of teal and grey, and the lines are thin and light grey.

▶▶ Active Botnet Families and Attack Payloads

This chapter explores further into active botnet families detected in 2018. We concentrate on four distinct families and tools focusing our analysis on their behavior changes, sample version changes, sample variants, and average age of C&C servers, to better understand the dynamic lifecycle of botnet families throughout 2018.

4.1 Gafgyt: The Choice for IoT Botnets

In August 2014, Sony PlayStation Network (PSN) suffered a massive outage caused by a DDoS attack launched from a legion of IoT devices. The hacker organization, Lizard Squad, claimed responsibility for the attack.

In December 2014, Lizard Squad again used a large number of IoT devices to launch a DDoS attack against Microsoft's Xbox Live, disconnecting millions of game players from game servers.

In January 2015, the source code of the botnet Gafgyt used by Lizard Squad, was leaked. Analysis showed that the source code was written in C and with 1600 lines of code (including a telnet scanning module and a weak password dictionary).

Once in the wild, other hacking groups and threat actors around the world began to develop a myriad of variants based on this family, including Bashlite and Qbot, thus masking the originally unique traces of Lizard Squad attacks.

Despite being older than Mirai, Gafgyt is a latecomer to the cybersecurity battlefield. The first Gafgyt sample we captured exploited weak passwords in Telnet for propagation and had an additional module for exploiting a backdoor in Netis routers. Using the NSFOCUS Network Intrusion Prevention System (NIPS) massive alert log database, we began to track this family in 2017.

Since the time the source code was leaked, the Gafgyt family, like Mirai, has a lot of variants. The code of several major IoT botnet families overlaps, making it extremely difficult to separate these families from one another. Based on the method of communication a botnet family uses, we group several malicious programs with the same network behavior or patterns into the Gafgyt family. The following table lists active variants of the Gafgyt family.

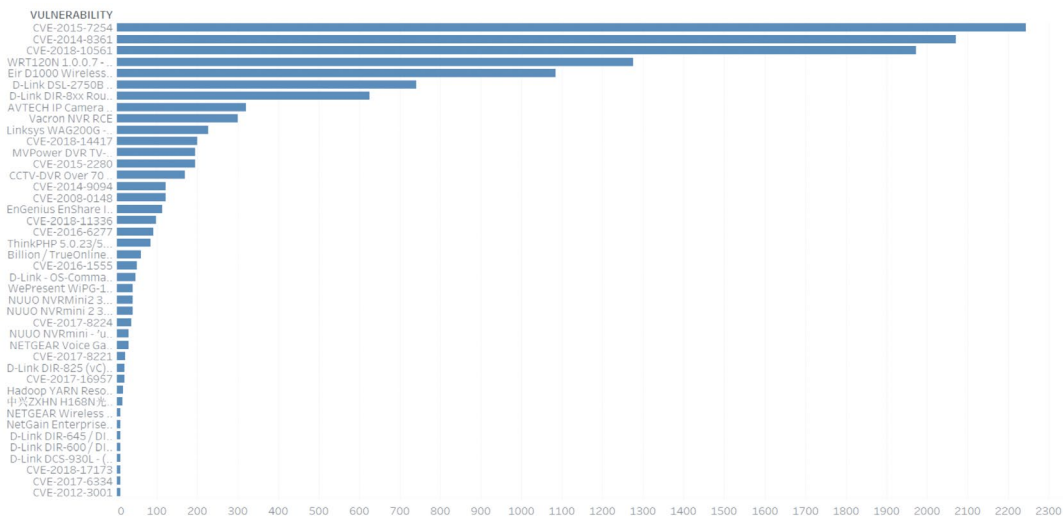
► Active Botnet Families and Attack Payloads

Table 3 Active Gafgyt Family Variants

Variant	Description
BUILD	Based on the original Gafgyt source code, sends the architecture of the infected device to the C&C server.
Shelling	Connecting to port 666 of the C&C server by default, provides the C&C server the operating system version and installed applications on the current IoT device.
Demon	Recompiled from Shelling and named based on port 666 being used with most C&C servers in North America and Europe.
Arch	A popular variant of BUILD, with minor changes made to the source code to fight against specific network protection rules.
Boatnet	Named after a keyword often used by Russia-based C&C servers to notify bots that they get online.
Hakai	Just as its name implies, Hakai (meaning "destruction" in Japanese) is very destructive because of its ability to launch more DDoS attack methods than other variants. For example, its use of external modules to support SSDP reflective amplification attacks.
Katura	Katura (meaning "katsura tree" in Japanese) is focused on scanning payloads. So far 22 different types of vulnerability scanning payloads have been observed.

The Gafgyt family has set a record for the number of vulnerabilities it can exploit on various platforms. A total of 43 vulnerabilities can be exploited by all versions of Gafgyt, as shown in the following figure.

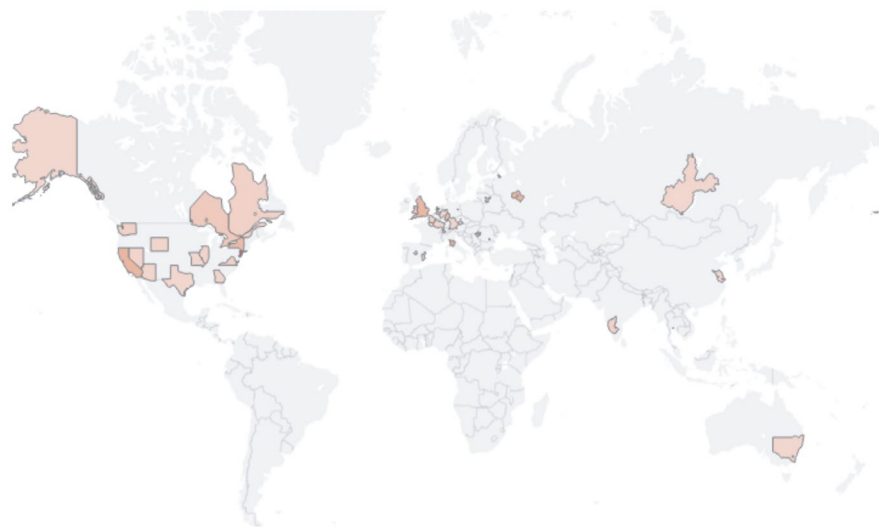
Figure 19 Vulnerabilities exploited by the Gafgyt family



Because of their infection success rate and that their C&C servers are easy to deploy, Gafgyt botnets have propagated rapidly across the globe. The following map shows the global distribution of C&C servers belonging to the Gafgyt family and its variants that had been detected by NSFOCUS as of December 31, 2018.

▶▶ Active Botnet Families and Attack Payloads

Figure 20 Global distribution of C&C servers of the Gafgyt family



Gafgyt is the first IoT botnet successfully offered as a botnet-as-a-service, and originally offered by Lizard Squad. While tracking this family, NSFOCUS researchers found this family so successful that within Gafgyt C&C chatrooms there were people dedicated to answering questions about the use of this botnet.

Figure 21 Part of the Gafgyt chat log

```
: lol  
: lol  
: hahaha  
: pyschocoding is here  
: i have hoho  
: haaaaaaa  
: lol  
: is this strong  
: im so confused  
: help  
: hahaha  
: lmao he bag  
: ha  
: right  
: lol  
: ik tf  
: anyone  
: ayo  
: im doing something  
: i see  
: omfg  
: look on skype  
: have fun
```

► Active Botnet Families and Attack Payloads

For the uninitiated, it will be difficult to interpret, but what can be inferred from the above conversation is that the Gafgyt botnet has switched its business model from traditional sales of attack traffic capability to becoming a bot rental service via cloud platform. This business model further lowers the level of skills required to use the botnets and promises new avenues of attack against a broader range of targets. If this business model becomes popular, botnets will definitely become a greater threat based on upgraded capabilities while becoming ubiquitous.

4.2 BillGates: Best Cross-Platform Family

In February 2014, a new botnet family was reported by the Russian website, [habr](https://habr.com/post/213973/)⁵ and named BillGates because of its bill and gates modules. Subsequently the research group, MalwareMustDie reported that botnet family was operated by a Chinese hacker group, closely related with other known families such as ChinaZ and Elknot. This has helped BillGates attract wide attention.

BillGates is a cross-platform bot family mainly running on *nix platforms. Within four years after its appearance, the BillGates family has grown to include a series of variants such as Webtoos for Windows and BillGates.lite for infecting embedded devices like ARM.

NSFOCUS research shows that BillGates provides UIs making it easier to use and, thus gaining popularity among hacking organizations.

Since the first attack found related with BillGates, Fuying Laboratory has been tracking this family. In the first quarter of 2018, BillGates was extremely active and conducted multiple campaigns in a short period of time and then suddenly stopped. However, the series of attack campaigns lasted long enough against a wide variety of targets that it makes this botnet family worth analyzing and tracking.

4.2.1 Evolution of the Family

BillGates has two widespread variants: V1 and V2. V1 uses RSA encryption to encrypt configuration files, while V2 uses custom algorithms. These two early variants were the major perpetrators of BillGates attacks during the first quarter of 2018. Samples seen based on other variants, such as the

⁵ <https://habr.com/post/213973/>

► Active Botnet Families and Attack Payloads

webtools strain, were also captured, but the quantity of their samples were small and their instructions seen were limited in number, indicating that these other variants were incapable of launching really damaging attacks. We believe that this is due to low compatibility between variants. During the active period of attacks, the number of BillGates samples seen reached a record high in Q1 2018 and then rapidly dwindled to nearly 0 after May.

Figure 22 RSA decryption function of BillGates_V1

```
std::string::string((std::string *)&v29);
CUtility::EString((CUtility *)&v28, (const char *)this);
CUtility::EString((CUtility *)&v27, a2);
CUtility::EString((CUtility *)&v26, a3);
if ( (unsigned __int8)std::string::empty((std::string *)&v28) ^ 1 )
{
    CRSA::Decrypt((CRSA *)&v29, (std::string *)&v28, (std::string *)&v27, (std::string *)&v26, v24);
    std::allocator<std::string>::allocator(&v30);
    std::vector<std::string, std::allocator<std::string>>::vector(&v25, &v30);
    std::allocator<std::string>::~allocator(&v30);
    v3 = std::string::c_str((std::string *)&v29);
    CUtility::Split(v3, 58, &v25);
}
```

Figure 23 Custom decryption function of BillGates_V2

```
v8 = std::string::length(a2);
CIHNSr::Udjf34(this, 0LL);
for ( i = 0; ; ++i )
{
    result = i;
    if ( i >= v8 )
        break;
    CIHNSr::Udjf31((CIHNSr *)&v6, (unsigned int)this);
    CIHNSr::Udjf34(this, &v6);
    CIHNSr::~CIHNSr((CIHNSr *)&v6);
    v3 = *(_BYTE *)std::string::operator[](a2, i) > 47 && *(_BYTE *)std::string::operator[](a2, i) <= 57;
    if ( v3 )
    {
        v9 = *(char *)std::string::operator[](a2, i) - 48;
    }
    else
    {
        v4 = *(_BYTE *)std::string::operator[](a2, i) > 64 && *(_BYTE *)std::string::operator[](a2, i) <= 70;
        if ( v4 )
        {
            v9 = *(char *)std::string::operator[](a2, i) - 55;
        }
        else
        {
            v5 = *(_BYTE *)std::string::operator[](a2, i) > 96 && *(_BYTE *)std::string::operator[](a2, i) <= 102;
            if ( v5 )
                v9 = *(char *)std::string::operator[](a2, i) - 87;
            else
                v9 = 0;
        }
    }
}
CIHNSr::Udjf32((CIHNSr *)&v7, (unsigned int)this);
CIHNSr::Udjf34(this, &v7);
CIHNSr::~CIHNSr((CIHNSr *)&v7);
}
return result;
```

► Active Botnet Families and Attack Payloads

The code structure of BillGates samples is relatively stable. A vast majority of variants use the same attack code, with few additions. According to the samples that NSFOCUS has on hand, BillGates still uses DDoS attack code written in 2016 and before. V2, other than the code for attacking TCP-based DNS servers, has nothing new compared with V1.

Figure 24 Attack function of BillGates_V1

```

        break;
    case 0x40u:
        v8 = (CTcpAttack *)operator new(0x80u);
        CTcpAttack::CTcpAttack(v8, (CThreadNormalAtkExcutor *)((char *)this + 136));
        *((_DWORD *)this + 67) = v8;
        break;
    case 0x41u:
        v9 = (CAttackCc *)operator new(0x94u);
        CAttackCc::CAttackCc(v9, (CThreadNormalAtkExcutor *)((char *)this + 136));
        *((_DWORD *)this + 67) = v9;
        break;
    case 0x42u:
        v10 = (CAttackIe *)operator new(0x88u);
        CAttackIe::CAttackIe(v10, (CThreadNormalAtkExcutor *)((char *)this + 136));
        *((_DWORD *)this + 67) = v10;
        break;
    default:
        break;

```

Figure 25 Attack function of BillGates_V2

```

        break;
    case 0x41u:
        v9 = (CAttackCc *)operator new(0x94u);
        CAttackCc::CAttackCc(v9, (CThreadNormalAtkExcutor *)((char *)this + 148));
        *((_DWORD *)this + 70) = v9;
        break;
    case 0x42u:
        v10 = (CAttackIe *)operator new(0x88u);
        CAttackIe::CAttackIe(v10, (CThreadNormalAtkExcutor *)((char *)this + 148));
        *((_DWORD *)this + 70) = v10;
        break;
    case 0x43u:
        v11 = (CAttackTns *)operator new(0x94u);
        CAttackTns::CAttackTns(v11, (CThreadNormalAtkExcutor *)((char *)this + 148));
        *((_DWORD *)this + 70) = v11;
        break;
    default:
        break;
}

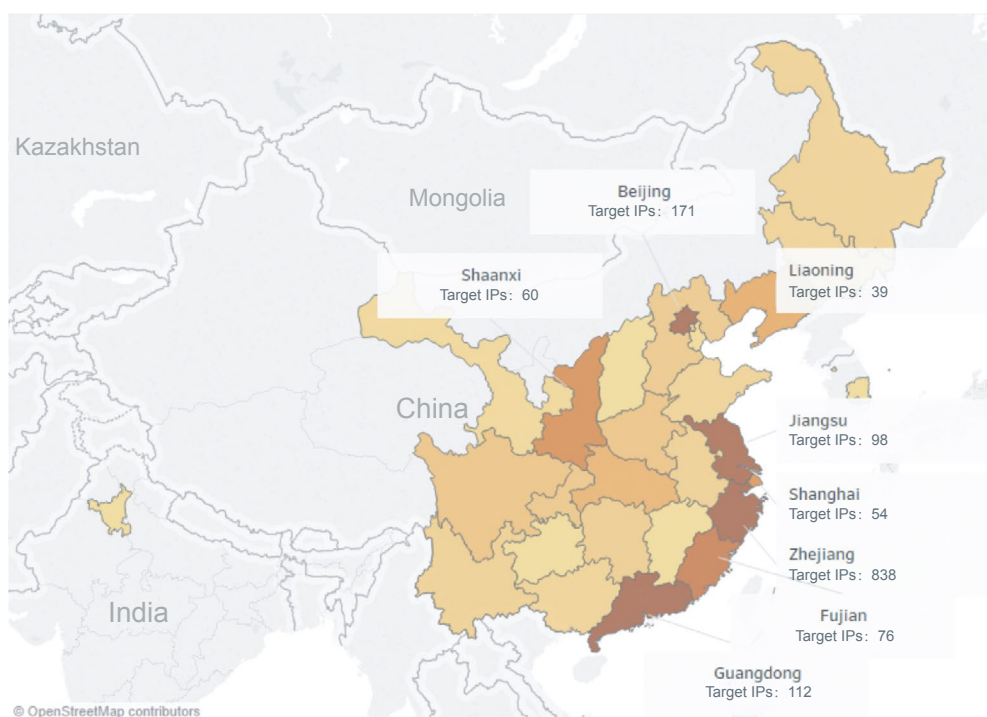
```

► Active Botnet Families and Attack Payloads

4.2.2 Analysis

During the first quarter of 2018 when BillGates was extremely active, the family was found to attack 3962 targets, most of which were in two Central American countries. The following map shows the distribution of BillGates targets in China that NSFOCUS was able to directly monitor.

Figure 26 Distribution of BillGates targets in China

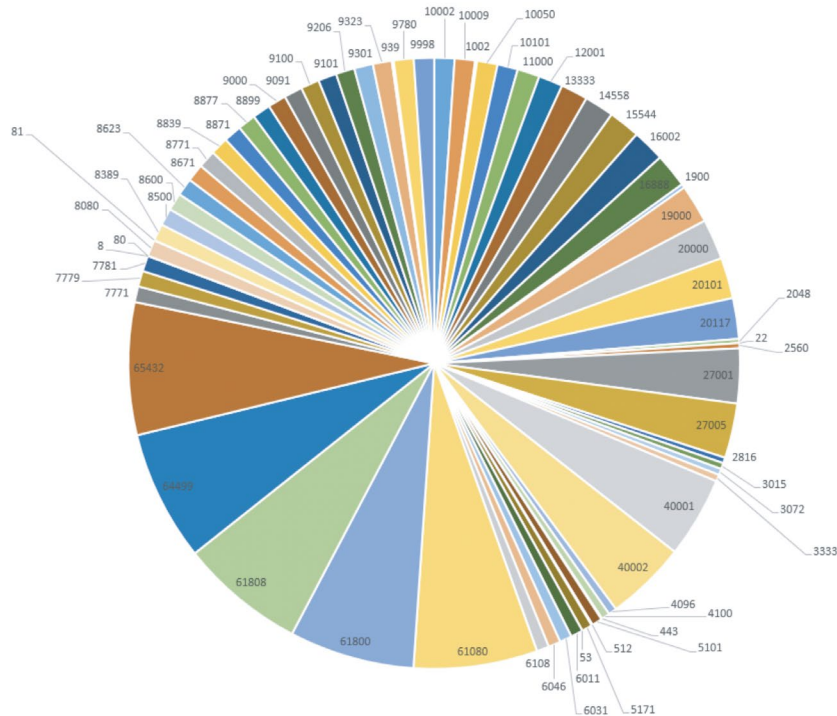


BillGates ignored common ports, such as 22, 23, 80, 8080, and 443, and instead attacked uncommon ports as its targets. These uncommon ports are not usually bound to known protocols but are used to provide agent and gaming services. This leads us to believe that BillGates is focused on agent tools, online gaming servers, and proprietary gaming servers.

The following figure shows ports attacked by the family.

► Active Botnet Families and Attack Payloads

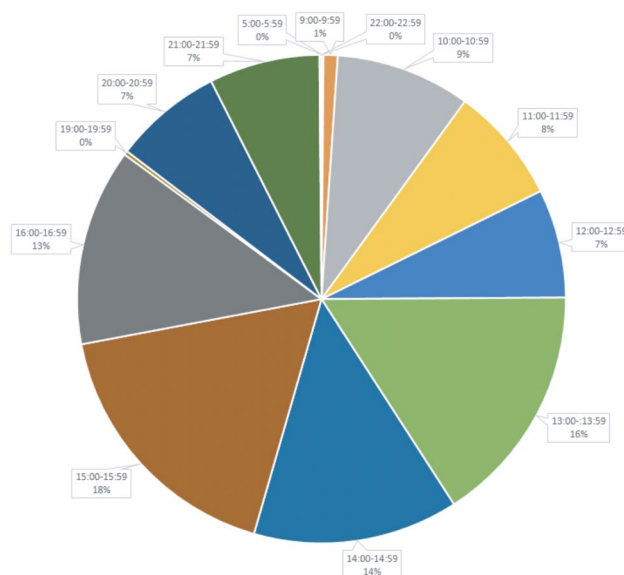
Figure 27 Ports attacked by the BillGates family



The following figure shows that BillGates received attack instructions almost around the clock. In our opinion, the even time distribution suggests that this botnet family is highly automated and likely being used as some form of botnet-as-a-service. Thus, the BillGates family may be deployed in a very efficient environment operated by a well-organized group.

Interestingly, BillGates became inert after members of another active hacking group, Shadow (Anying in Mandarin) DDoS group, were arrested. It is not known whether the two groups were directly linked or BillGates' controllers decided to shut down operations after the high-profile arrest. However, the rise and fall of BillGates is a good view into the lifecycle of botnet development and provides good examples of attack event traceback and behavior analysis.

Figure 28 Time distribution of attack instructions issued to BillGates



4.3 XMRig: Cryptomining For Fun and Profit

Cryptomining by botnets has gained popularity in the past two years. Unlike other common malicious activities like DDoS, ransomware attacks, and confidential information theft, cryptomining has some unique characteristics:

1. Predictable earnings. Cryptominers are good at hiding their presence by controlling their CPU usage within 30%–40%. Based on the reference computing power obtained from open-source information⁶, we calculate expected daily earnings of a bot as follows:

Table 4 Monero Daily Earnings Based on CPU

CPU	DescriptionEarning/day
CPU Intel i7-7700	0.00183438 XMR
AMD Ryzen 7 1700X	0.00334609 XMR

In the first quarter of 2018 the price of Monero was at a lifetime high of over USD \$400/XMR. Thus,

⁶ <https://github.com/xmrig/xmrig>

► Active Botnet Families and Attack Payloads

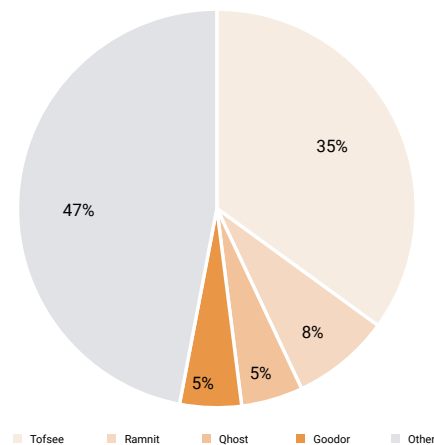
each controlled host could bring in at its peak USD 73 cents/day to an attacker.

2. Concealed attacker information. A cryptominer when running, interacts only with a mining pool (a collection of cryptominers being operated as a group). An attacker can conceal his or her network information by using only public mining pools. In addition, owing to the anonymity of Monero, little information about the attacker can be obtained from wallets or transaction records. Therefore, in a cryptomining event, the defender typically knows only which hosts are mining cryptocurrency and the wallet addresses to which they are bound. This makes it extremely difficult to track cryptomining activities.

For reference, we list the following cryptographic mechanisms that Monero uses to ensure full privacy and obscurity:

- a. Ring signature: a digital signature in which a group of possible signers are merged together to produce a unique signature for authorizing transactions. This makes the sender untraceable.
- b. Obfuscated receiving address: transactions can use stealth or one-time addresses to make the receiver untraceable.
- c. Ring confidential transactions: the transaction amounts are obfuscated to hide the amount of transactions.

Figure 29 Botnet families using XMRig

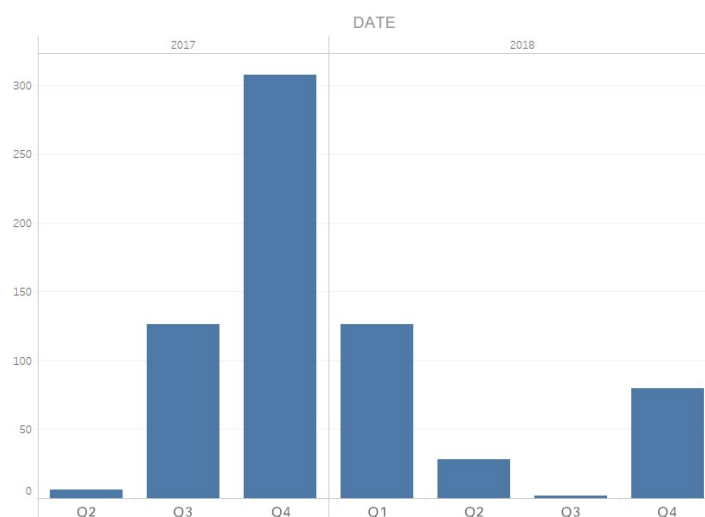


▶▶ Active Botnet Families and Attack Payloads

Although there are a number of botnet families conducting cryptomining attacks, XMRig has its own communication mechanism separate from the botnet control mechanisms. By identifying and capturing these communications, defenders can detect cryptomining events and further determine their scale.

Our analysis of cryptomining events in the past two years show that botnet families are, at first glance, irregular in the use of cryptominers.

Figure 30 Quarterly statistics of cryptomining events in 2017–2018



Deeper analysis shows that the trend of cryptomining events is directly related to the price of Monero. In the fourth quarter of 2017, the price of Monero reached a record high making cryptomining an extremely lucrative business. This led to a sudden influx of botnet groups switching to cryptomining. However, as the cryptocurrency price fell in the second half of 2018, a sharp drop of cryptomining events was also seen. In the fourth quarter of 2018, the number of cryptomining events rose a bit, which may be related with the explosive growth of Monero transactions in this quarter.

For the prices and transaction volumes of Monero in the past two years, see the following figure from WorldCoinIndex⁷.

⁷ <https://www.worldcoinindex.com/coin/monero>

► Active Botnet Families and Attack Payloads

Figure 31 Monero price and transaction volume trends in 2017–2018



While there is a significant increase in interest in blockchain technology, the cryptocurrency market has suffered a serious decline in the last year. Even if geopolitical events in the coming months may again contribute to a rise in the price of cryptocurrency, we think that the possibility of new cryptominer families emerging are very small. Despite that, considering the number of cryptomining events rising in the fourth quarter, we should still be on the lookout for such behavior. It would be prudent to add identifying cryptominer traffic to security monitoring and threat hunting processes. Once seen, analyses of their communications would help identify botnet families and the development of a mitigation strategy for blocking the attacks at the payload delivery and attack execution stages.

4.4 Satan: Evolving Ransomware

In late April 2018, MalwareHunterTeam reported seeing new ransomware that leveraged EternalBlue to propagate. Through analysis, we found that the ransomware was based on a new version (dubbed V2) of Satan, a ransomware family launched in 2017. The ransom demanded in this version increased from 0.1 to 0.3 Bitcoin. At the same time, a certain variant of IRCBOT also captured download instructions related to this malware. From the instruction set, Satan was confirmed to be the ransomware payload. An analysis of the ransomware payload reveals that it RC4 is used for its encryption algorithm and stores keys locally. NSFOCUS Fuying Laboratory has developed and released a decryption tool to counter Satan.

At the end of May 2018, version 3 of Satan was released which exploited multiple web-related vulnerabilities, included weak password dictionaries, and added mimikatz as a payload to better exploit compromised devices. Mimikatz is a tool used gather credentials and then exploit vulnerabilities in authentication systems. This version of Satan is the same as V2 during the encryption and ransom stage. Therefore, no update was required to the NSFOCUS Satan decryption tool.

At the end of July 2018, a vendor reported a series of Satan infection events in China. Through analysis, we found that the ransomware had been upgraded to V3.1, with minor changes to its key storage policy. The new version generates random keys and then uploads them to the C&C server. If no network connection is available to the bot, V3.1 uses defaults to the original mechanism of directly writing keys to the end of encrypted files. Fuying Laboratory updated the decryption tool and provided a sample analysis report and remediation recommendations.

In mid-December 2018, NSFOCUS captured Satan V4, which runs on both Windows and Linux. V4 switches from the relatively weak R4 algorithm to the stronger AES-ECB algorithm. The encryption key is then written to the end of files only after being RSA-encrypted. As a result, to recover from this version, the victim must first decrypt the key, which can be found in running memory, and then decrypt the files. This process similar to that used by WanaKiwi developed by Adrien Guinet and Benjamin Delpy.

► Active Botnet Families and Attack Payloads

The following table shows the evolution of Satan.

Table 5 Evolution of Satan Versions

Version	V2	V3	V3.1	V4
Detection	April 2018	May 2018	July 2018	December 2018
Platform	Windows	Windows	Windows	Windows/Linux
Encryption Algorithm	RC4	RC4	RC4	AES-ECB
Exploit	EternalBlue Tomcat weak password scanning	EternalBlue CVE-2010-0738 CVE-2017-12149 CVE-2017-10271 Tomcat weak password scanning	EternalBlue CVE-2010-0738 CVE-2017-12149 CVE-2017-10271 Tomcat weak password scanning Mimikatz component	EternalBlue CVE-2010-0738 CVE-2017-12149 CVE-2017-10271 Tomcat weak password scanning Mimikatz component

Extortion remains one of the most lucrative ways of generating profit for hackers. Based on the evolution of the Satan family in 2018, we learned a great deal about the lifecycle of ransom botnets. These ransomware families are very sophisticated in early versions but then evolve quickly amid the fierce battles between the offensive and defensive sides. This evolution into a more mature product is characterized by modularization and precise engineering, becoming a greater threat to users' data security.

5

Conclusion and Recommendations

► Conclusion and Recommendations


In 2018, botnets continued using DDoS as their primary weapon to attack regions with ubiquitous high-speed networking for direct economic gains. However, they underwent significant changes in behavioral patterns, host platforms, C&C server deployment, infection methods, attack methods, and payload types. Security service providers need to adapt their strategies to better mitigate the increasing threats posed by the new generation of botnets.

The evolution of botnets taking advantage of more platforms and more attack methods make them more dangerous. IoT environments rife with vulnerabilities have given rise to many huge cross-platform botnet families that are capable of fast propagation. The frequent use of reflection attacks has led to upgrading traditional families with more devastating DDoS capabilities. At the same time, the development of blockchain techniques as well as the price of cryptocurrency has accelerated the outbreak and evolution of cryptominer families.

An emerging trend of botnet development in 2018 was attackers adopting a new economic model that evolved into botnet-as-a-service (BaaS). We have seen changes in the operations of botnets as traditional botnet families are packaging themselves as commercial services giving attack control to their "clients". This model lowers the level of skills required for using botnets to conduct DDoS attacks and expands their attack surface, making the innately flexible botnets more difficult to cope with.

Such a change in botnet lifecycle calls for changes in our defensive and research strategies:

- As defenders, we not only need to enhance our capabilities of countering ransomware and cryptominers but also need to improve the protections for IoT devices, make greater efforts in eliminating reflectors, and better ready ourselves to defend against reflection attacks. Only by doing so can we hope to withstand the coming tsunami waves of reflection attacks.
- As researchers, we must focus research on the evolution of the botnet lifecycle to better defend against the next generation of botnets. We must closely monitor the development and behavior of known botnet families to see how they take advantage of their new modular architectures. How will bots further develop and exploit this new capability? What new malicious activity can be utilized through modularization? Will the ability to launch multiple blended attacks increase their exploitation success and destructive capability?

 Conclusion and Recommendations

The botnet battlefield is by far the fastest growing cyberthreat today. The evolutionary lifecycles in botnet development enable rapid deployment of new attack methods and strategies, moving momentum in favor of the attackers. Inertia is the biggest weakness defenders must overcome just to stay at status quo. Both IoT vendors and end-users must be more proactive in implementing better security of connected devices. If that doesn't happen, cyberattacks could devastate the internet and networks to an extent not even imagined yet. Remember, only you can prevent cyberattack damage.

NSFOCUS

SECURITY MADE SMART & SIMPLE

www.nsfocus.com