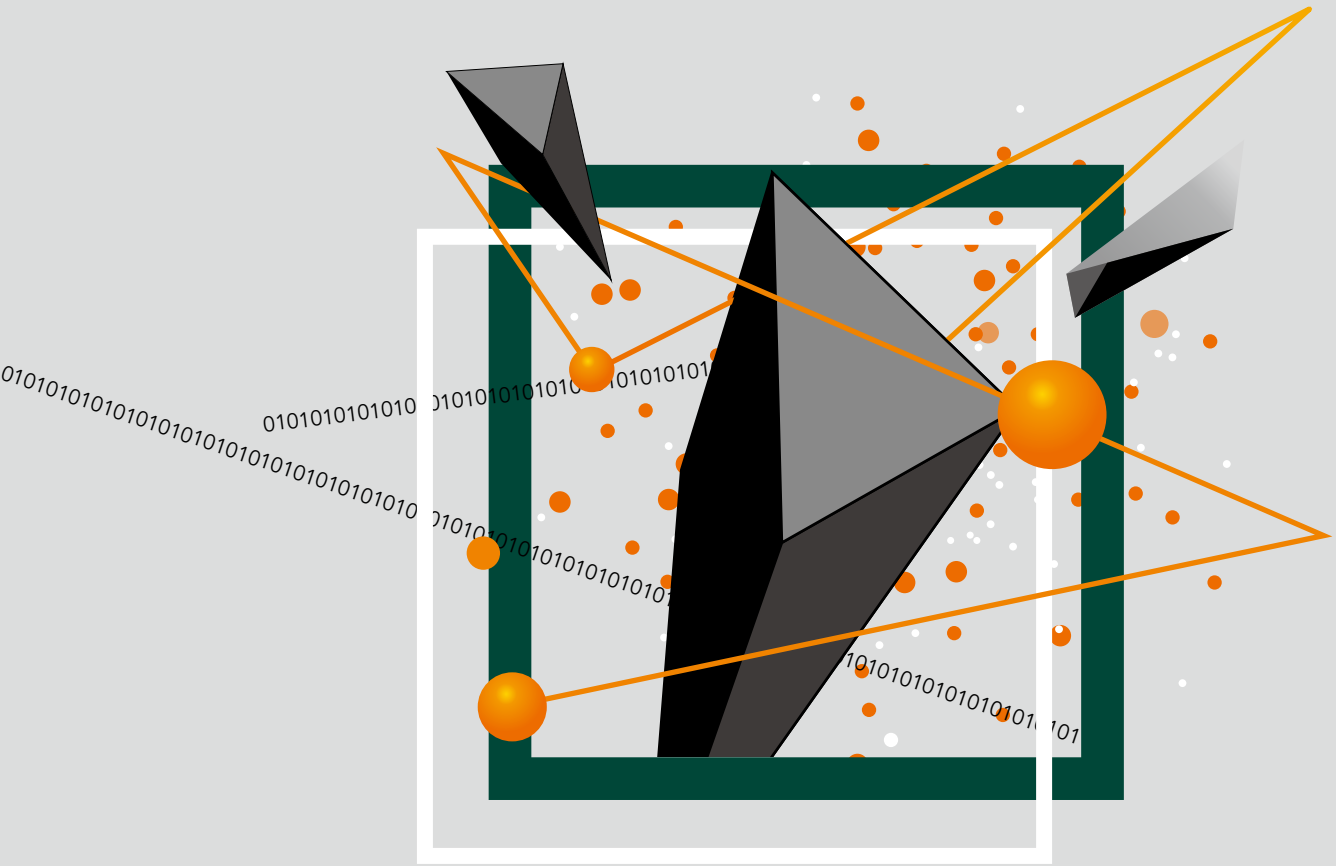


NSFOCUS

2017 Botnet Trend Report

NSFOCUS

About NSFOCUS

NSFOCUS is an iconic internet and application security company with over 18 years of proven industry experience. Today, we are operating globally with 2000+ employees at two headquarters in Beijing, China and 40+ offices worldwide including the IBD HQ in Santa Clara, CA, USA. NSFOCUS protects four of the ten largest global telecommunications companies and four of the five largest global financial institutions.

With its multi-tenant and distributed cloud security platform, NSFOCUS effectively moves security into the internet backbone by: operating in data centers around the world, enabling organizations to fully leverage the promise of cloud computing, providing unparalleled and uncompromising protection and performance, and empowering our partners to provide better security as a service in a smart and simple way. NSFOCUS delivers holistic, carrier-grade, hybrid DDoS and web security powered by industry leading threat intelligence.

Special Statement

All data for analysis is anonymized and no customer information appears in this report to avoid information disclosure by negligence on our part.

Contents

NSFOCUS Threat Intelligence (NTI)

NSFOCUS Threat Intelligence center (NTI) is a professional security research organization set up by NSFOCUS for implementing the intelligent security 2.0 strategy, promoting sound development of cyberspace security ecology and applications of threat intelligence, and enhancing customers' capabilities of defending against various attacks. Thanks to the company's competent security teams and powerful security research capabilities, NTI is able to continuously observe and analyze the global cybersecurity threats and landscape. With a focus on the capabilities and key techniques for threat intelligence production, operations, and applications, NTI 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.

Botnets are always a hazard that cannot be overlooked in the Internet environment. As a common malicious program, botnets feature high elusiveness and share some common characteristics with worms and trojans. Botnets can take control of the target host by exploiting vulnerabilities, so as to steal information from the host or manipulate the host to launch network attacks. Botnets can be a great menace to the controlled hosts and even the entire network environment.

Generally, when starting an attack, a hacker first breaks into a target host via spoofing or a vulnerability exploit, dropping a simple loader in the host. Then, this loader will download necessary program code from a remote host to install core functions, allowing the hacker to take control of the target host. In this way, the hacker can steal sensitive information and encrypt mission-critical files on the host for a ransom. Turning this host to a bot, the hacker can also use a C&C server to issue commands to instruct this target host to launch attacks such as scanning, spam, and distributed denial of service (DDoS) attacks.

Based on NTI's ongoing botnet monitoring, we gain insights into the botnet situation from such dimensions as activity, scale change, and new technology trend. In addition, we have followed up with samples of the family, the most active botnet found in China recently, and make a detailed analysis of the history and overall situation of this family here. Our findings include the following:

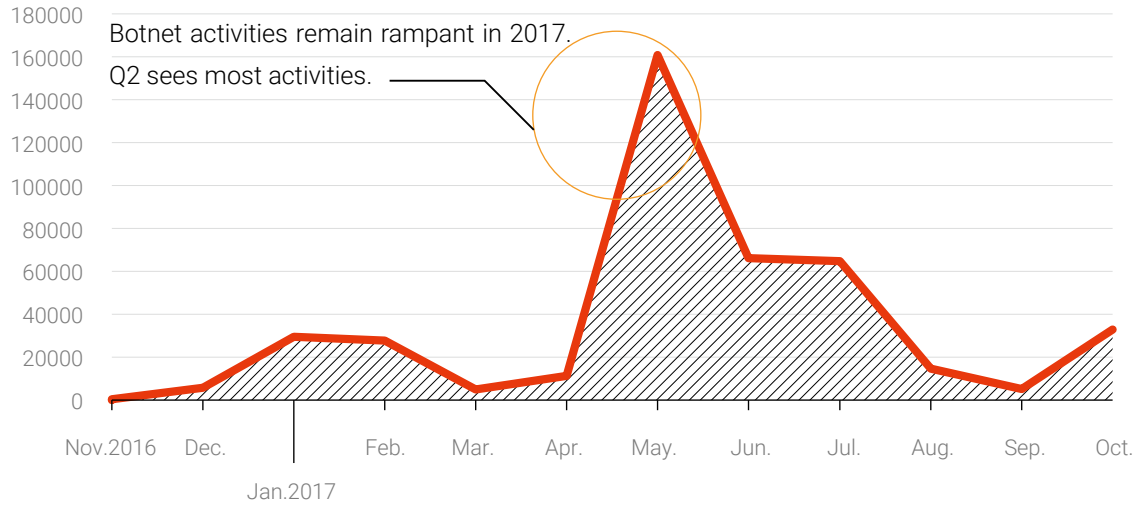
1. Botnet activities are quite rampant.
2. Botnets are expanding in size.
3. With the rapid development of the IoT, the botnet threat landscape is changing drastically.

1. General Trend

Botnet Activities Raging On

According to data from NTI, botnets were still active in 2017, especially the second quarter that saw the most botnet activities. As for attack instructions, C&C servers of botnets, in the most active state, issued 5187 instructions on average each day and a single C&C server even issued 114 instructions in a day.

Figure 1.Trend of quantitative changes of C&C instructions[1] (Unit: Times)



We find that the activity level of botnets is connected with major events. In March and September when national conferences were held, network monitoring was enhanced, significantly restraining botnet activities. Around May, botnets became most active because of the emergence of the WannaCry ransomware that exploits the EternalBlue vulnerability. Motivated by profits, botnet activities have a tendency to rise when networks become apparently vulnerable but decline in the case of strong governance so as not to be noticed.

Our statistics reveal that most of those instructions are about DDoS attacks which are the dominant form of botnet activities. Botnet attacks mainly target the gaming and entertainment sectors, especially emerging business such as porn games, perverted games, room card games, and live streaming. Such business has a big market and generates high profits, thus catching the eye of the black market. Also, cut-throat competition via cyberattacks is commonly seen between competitors, thus opening up profitable opportunities for botnet attacks.

1 Instructions indicate control signals sent from the C&C server to a botnet for the purpose of instructing it to attack a target. The frequency of sending signals reflects how active a botnet is.

Botnet Widening in Size

Host Quantity

In 2017, botnets increased in both number and size. On the one hand, C&C servers continued to grow, registering a remarkable increase since August and an increase of 1.67% in October compared with September. On the other hand, an intermittent increase was observed in controlled hosts all around the world, with a triple (320%) increase in August compared with July.

Figure 2. Monthly growth rate of C&C hosts

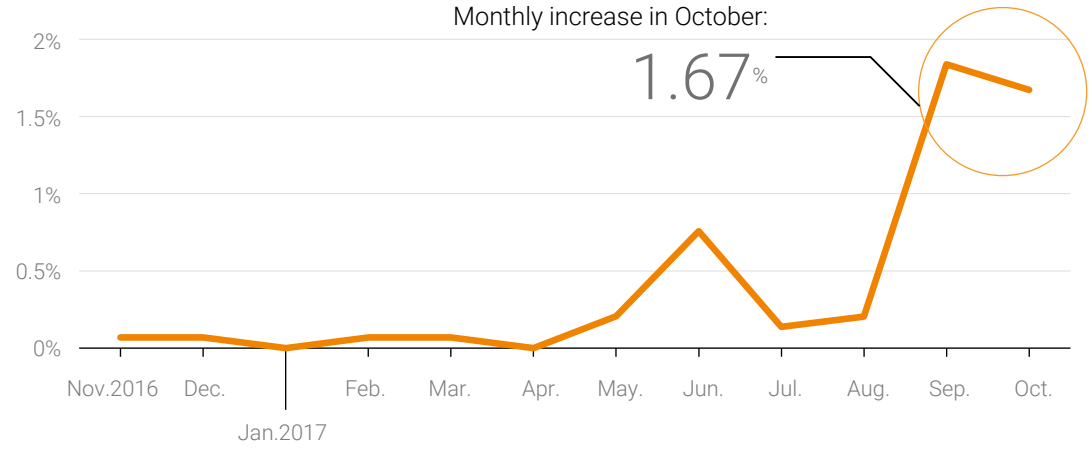
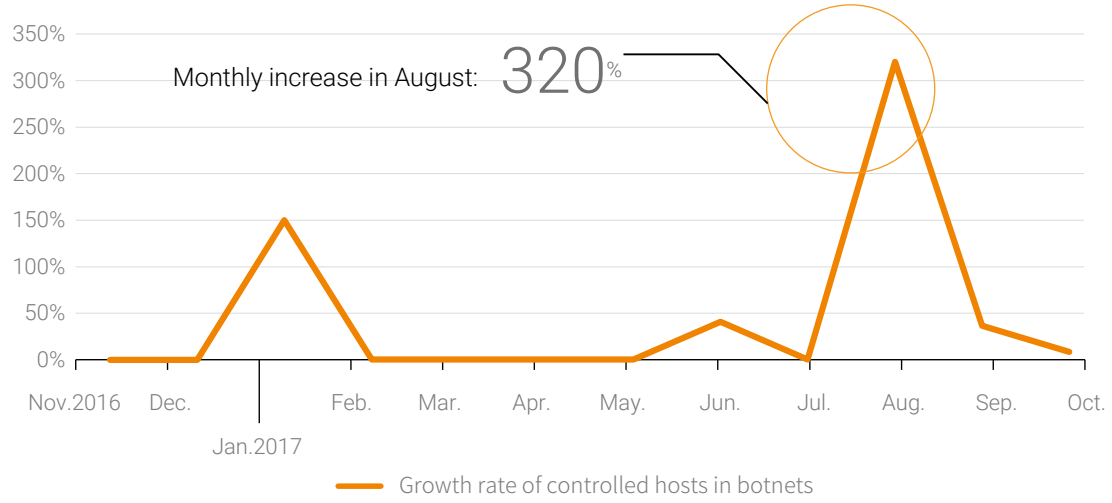


Figure 3. Monthly growth rate of controlled hosts in botnets



Geographic Distribution

According to statistics from NTI, most C&C servers are located in southeast coast areas in China and west coast areas in the USA, while the controlled hosts of botnets are mainly found in China, USA, and Russia.

Figure 4. Global distribution of C&C hosts

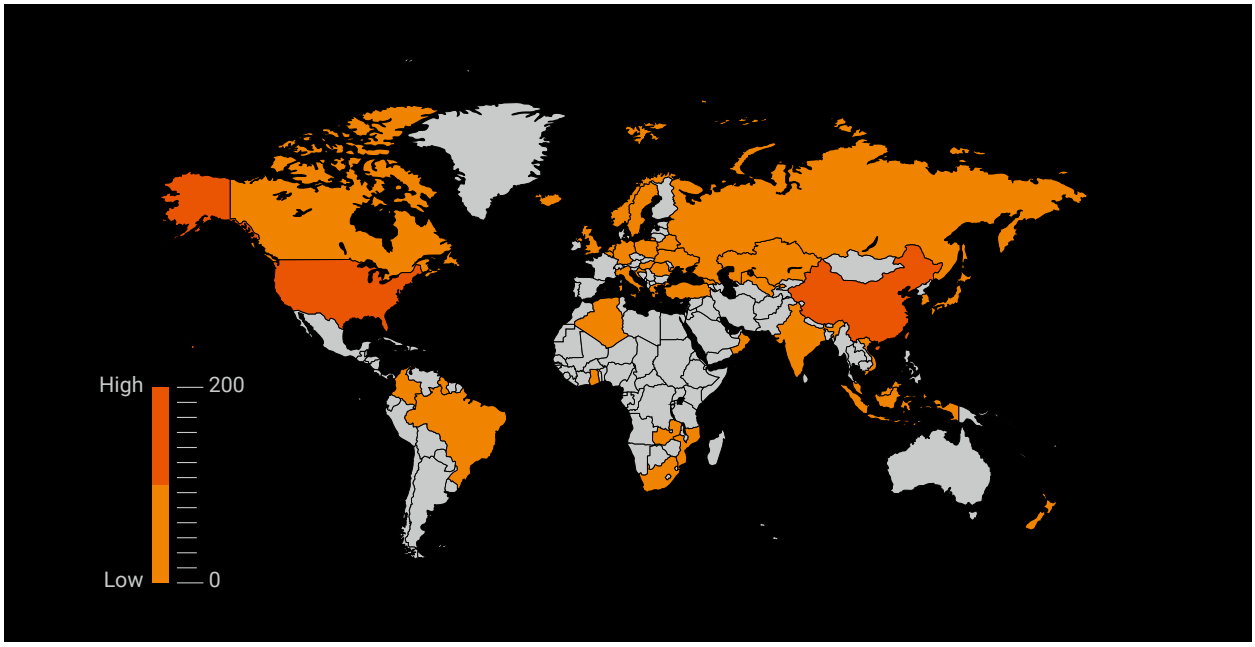
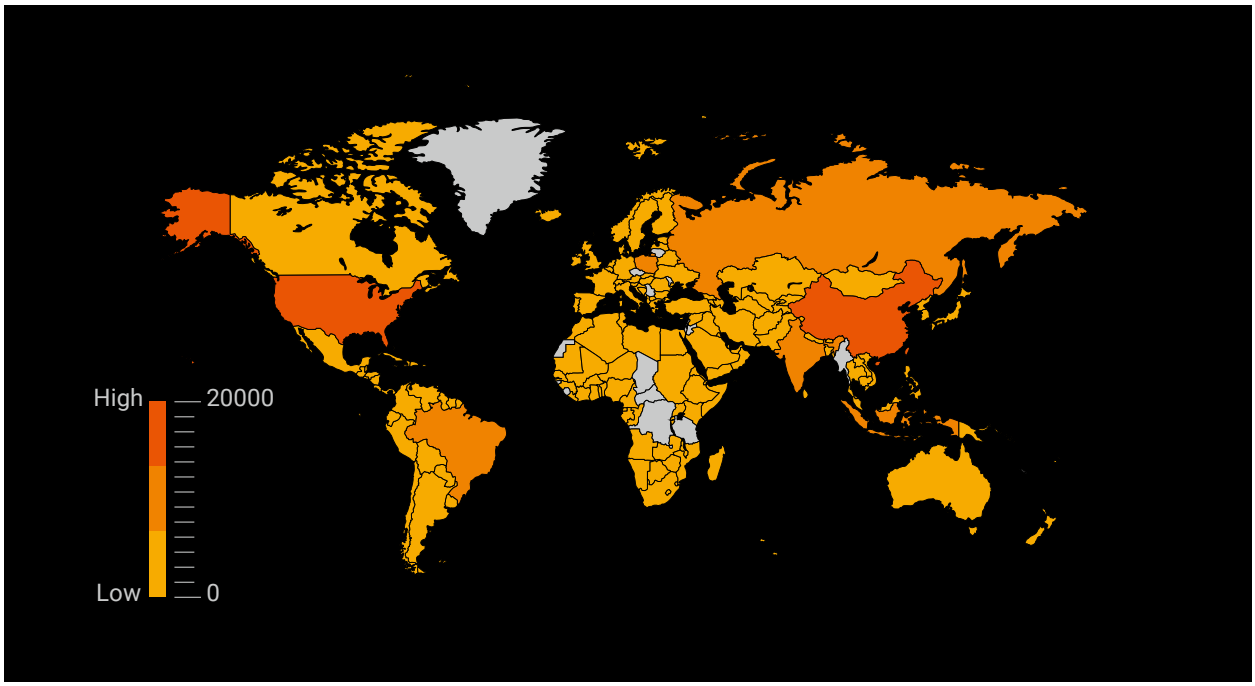
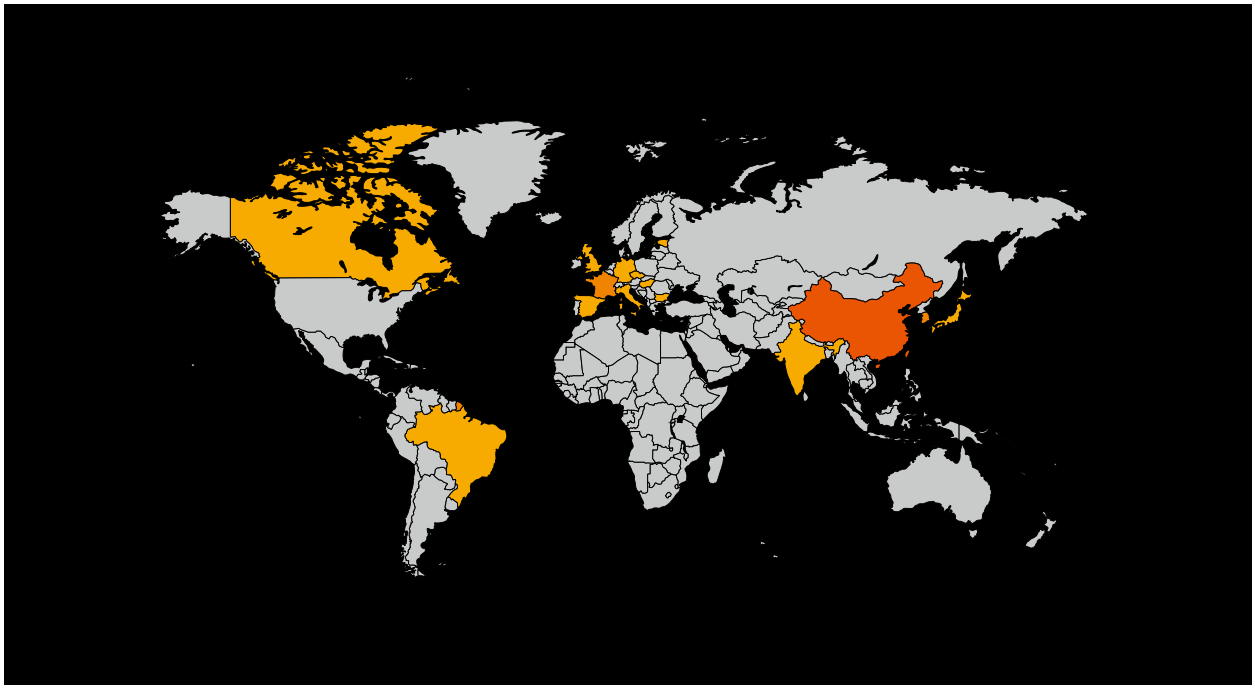


Figure 5. Global distribution of controlled hosts

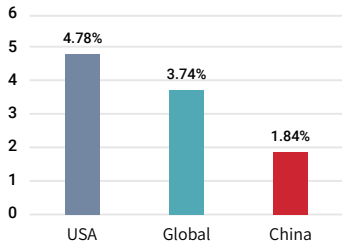


After the hacker gains access to the target host, the victim host, via a loader, downloads malicious code from a remote server to install function modules of the botnet. This remote server, as part of the critical infrastructure of a botnet, stores various functional modules required by the botnet. According to statistics collected by NTI, those servers are mainly located in China, France, South Korea, Germany, and Canada.



From the geographic perspective, China still houses the most botnets across the globe. Statistics released by IDC in November 2017 suggest that the proportion of IT security spending in China is still lower than the global average level, which is the main factor contributing to widespread botnet attacks in China[2].

China Should Increase the Overall Input to IT Security



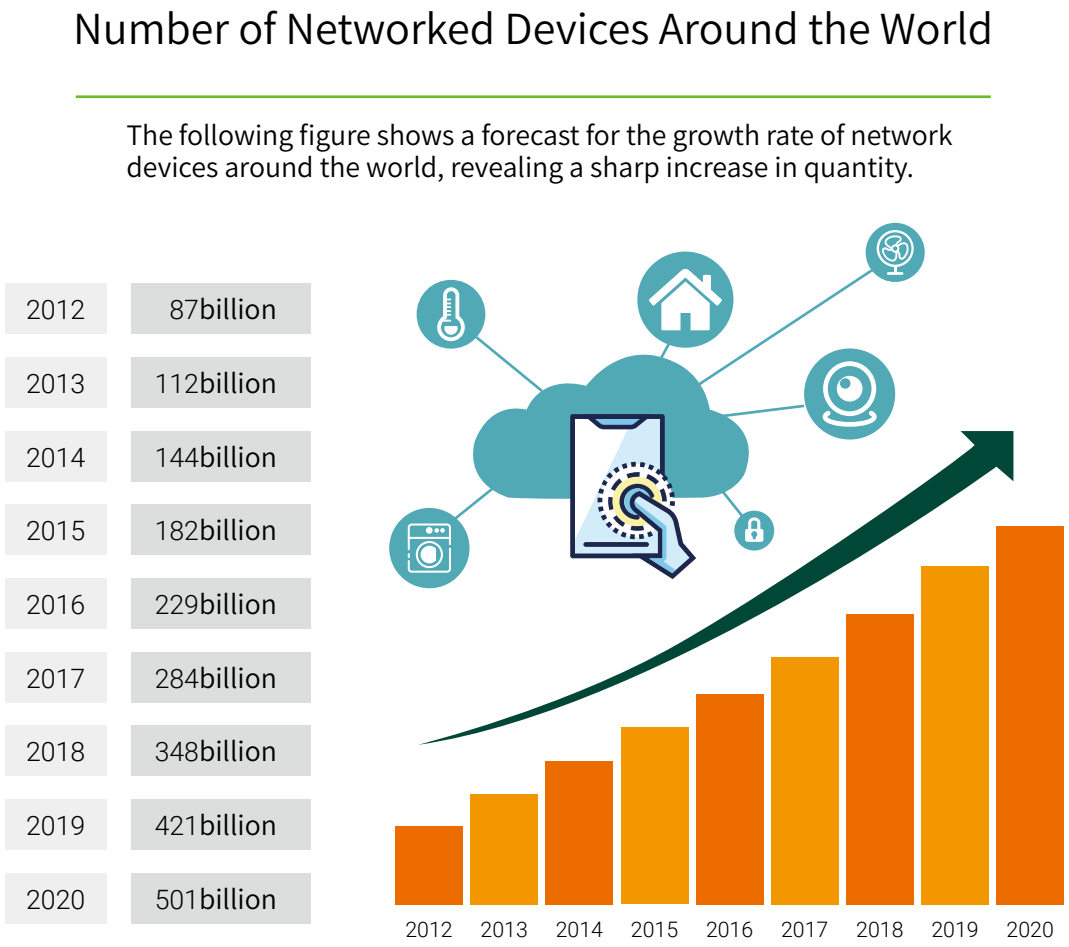
Proportion of USA's IT security spending on its market:	4.78%
Proportion of global IT security spending on its market:	3.74%
Proportion of China's IT security spending on its market:	1.84%

2 http://blog.nsfocus.net/idc-2017-james-wang-ppt/

Changing Battle Situation

For botnet attacks, the defensive side lags obviously behind the offensive side in this competition. In other words, the latter only needs to compromise a single target host to penetrate into the entire network, while the former has to deploy a comprehensive protection solution to block attackers. You can see that the defensive side has a higher cost during the battle. This situation will only go more intense as the network environment becomes further complicated with the connections of mobile devices, smart devices, and IoT devices into the Internet increasing.

Figure 6. McKinsey's forecast of the global growth trend of networking devices [3]



3 http://www.freebuf.com/articles/terminal/128148.html

New networking devices (including IoT devices and smart mobile devices) have unique characteristics, for example, IoT devices are numerous (many are low-cost) and diverse, constantly upgraded, but mostly take weak security measures. The particularity of the IoT presents new challenges to traditional high-cost production solutions. McKinsey expects that the number of global IoT devices will exceed 50 billion [4] by 2020, a challenge to attack protection.

Characteristics of IoT Devices	Offensive Strength	Defensive Challenge
Large scale	high profits, effectiveness	Costly, difficult to measure the effect
Weak security	Easy to attack, even for low-skill attackers	Too many vulnerabilities difficult to detect and fix all
Great diversity	Chances for different attackers	Comprehensive skill set required
Low cost	Cost-efficient	Cost-inefficient

In the new Internet environment, many emerging vendors are involved in the long-lasting botnet battle because they just care about new product functions, but lack necessary security awareness and protection capabilities. To actively cope with such a change in the battle, security vendors should do IoT-related security research and help customers develop security awareness; on the other hand, regulatory agencies should play an active role in the battle by formulating cybersecurity standards for products and establishing an effective mechanism for discovering and fixing vulnerabilities.

4 http://www.freebuf.com/articles/terminal/128148.html

2. Working Mechanism and Technology Trends of Botnets

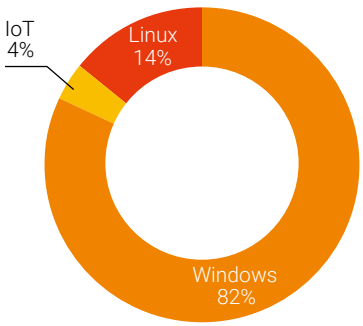
The mechanism and technology trends of botnets:

- **Larger scale.** Larger botnets have stronger attack capabilities, such as volumetric DDoS attacks. Numerous highly vulnerable IoT devices have become their ideal attack targets.
- **High elusiveness.** Botnets have always been pursuing the elusiveness. High elusiveness is essential to successful intrusions and the extension of the survival time. On one hand, botnet programs need to avoid security defenses deployed on bots themselves, as well as detection mechanisms provided by security devices. On the other hand, attackers need to hide their real identities.
- **Rapid propagation.** Just like all other attack protection scenarios, botnet protection is a race of speed between the attackers and the defenders. For attackers, in order to expand the botnet size, it is critical to infect as many devices as possible before attack targets gain protection capabilities. Characterized by self-replication, many botnets can expand their own size as quickly as possible.
- **Easy to control.** A large botnet requires a good network topology to ensure its effective organization. Botnets, under the control of hierarchical central C&C servers, are a relatively reliable mature model. Currently, new models such as P2P-based decentralized botnets are still at the exploratory stage. Such models, though with a great potential of elusiveness and network robustness, are seldom employed because they rely on complicated techniques and are difficult to control.

Cross-Platform Propagation Capability

As indicated in the General Trend section, the power of IoT, smart, and mobile devices can now be in protection against botnet attacks. Among all botnets under our constant monitoring, at least 4% targeted IoT devices. It is true that most botnets are still based on the Windows platform. But in recent years, with more and more IoT, smart, and mobile devices connected to the network, we expect to see an increasing number of malicious samples targeting these devices.

Figure 7 Distribution of botnet operating platforms



PCs can be compromised via emails, watering hole websites, or malicious code injected in software installation packages. For IoT devices that are large in quantity and need to always stay online but lacking timely

configuration and sufficient protection, a simple scan is enough for hackers to capture a great number of vulnerable devices. The set-top box (STB) worm detected by NTI in October 2017, dubbed Rowdy, was delivered over the Internet in China by exploiting vulnerabilities in STBs [5].

In addition, we also notice that some botnet families, typically Dendroid, FlexiSPY, and GMBot, target Android devices. Arguably, botnet is a cyber threat to all platforms.

As we mentioned earlier, attackers keep expanding the scale of botnets by compromising more and more devices to make attacks more effective. Vulnerabilities in IoT devices make these devices ideal tools for DDoS attacks. However, avaricious hackers are far more ambitious than that. According to our observation, some botnets work across platforms. Characterized by self-replication, these botnets can also plant malware of the corresponding platform according to the device type to effectively take control of devices, thus ensuring a more extensive impact. The following are some typical botnets with cross-platform capability.

Characteristics of IoT Devices	Offensive Strength
Rowdy	Linux (x86/x86_64, ARM, ARM4, ARM7, MIPS, MPSL, and so on)
Mirai	Windows, Linux (ARM, EABI4, MIPS, MIPS-I, PowerPC (Cisco 4500), Renesas SH, SPARC, Intel 80386)
Gafgyt.bax	Linux (x86/x86_64, ARM, Mips, PowerPC, SuperH or Motorola 68000)
Darkshell	Windows、linux(x86)
jRAT (remote control)	Relying on Java to spread across platforms, including Windows, Linux, macOS, and FreeBSD

From the programming languages of botnets, we can also see this cross-platform trend. C languages and scripting languages support cross-platform functionality. Whether in an embedded system on the ARM architecture or on a Linux or Windows system, they can demonstrate good adaptability. Botnet malware developed in such a language is therefore able to run and spread across platforms.

Botnet Family	Programming Language
Rowdy	C++
Gyddos	C++
LuaBot	Lua
Aldi_bot	Delphi
yi2.0	E language

Besides, scripting languages are easy to learn and use. A new botnet program can be written in these languages quite efficiently. Easy to construct and promising to make quick money, botnets are attracting more and more hackers, posing an increasing threat to the network.

Balance Between Elusiveness and Control Complexity

Generally, botnets use communication protocols that are closely related to their network architecture. As mentioned previously, botnets need to conceal themselves at any time in order not to be spotted by the defenders. For this reason, botnet designers need to strike a reasonable balance between control complexity and

5 http://blog.nsfocus.net/iot-set-top-box-malware-rowdy-network-analysis-report/

elusiveness.

Typical Family	Main Protocol
AldiBot, Vertexnet, and LokiBot	HTTP
TrickBot	HTTPS
Zeroaccess and Hajime	P2P
Zeus	IRC and Tor
GyDDoS and Rowdy	TCP

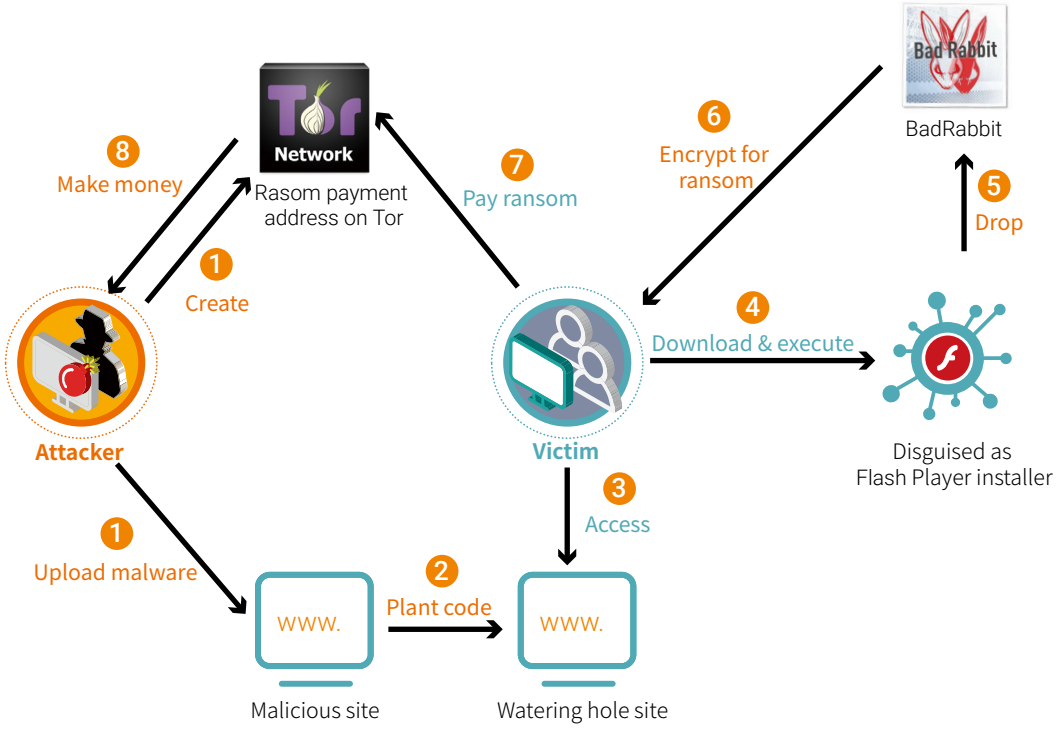
As for the network topology, botnets mainly use a client-server model, in which the C&C server and bots communicate with each other, with the former playing the control role, issuing upgrade or attack commands and the latter uploading local information to the former. In most cases, the communication between hosts is based on custom protocols built on TCP, with the traffic mixed with normal traffic for concealment. Certain botnets implement more complex communication, for example by using IRC, P2P, or Tor. However, such botnets have not become popular yet due to their complicated network architecture.

More Effective Ways of Delivery

Traditionally, attackers need to have malware triggered by tricking users into opening emails that contain malicious attachments, clicking malicious links, browsing web pages implanted with trojans, running legitimate programs with which malicious code is bundled, or performing other operations, thus infecting their systems. Malware delivery in this way relies on users' behavior, so botnets have to be stealthy in order to effectively beguile users besides the defensive mechanism of devices and programs.

The botnet families that were rather active in 2017 are extremely deceptive by disguising themselves as legitimate upgrade and installation programs in the process of delivery, therefore swelling significantly in size. An example of such deceptive malware is BadRabbit, which camouflages itself as a Flash Player installer and prompts users to install the Flash Player plug-in at watering hole sites. After users download and execute the malicious file, their systems will be infected [6].

6 http://blog.nsfocus.net/badrabbittechnical-analysis-protection-scheme/



Another effective way of delivery is to perform scanning, as demonstrated by hackers who have exploited weak passwords and software vulnerabilities to successfully compromise systems. For example, the EternalBlue vulnerability leaked in 2017 by ShadowBroker was integrated as part of the worldwide WannaCry attack. Again, we have to mention the "benefits" brought by the IoT and the massive quantities of mobile smart devices, which stay permanently online without effective maintenance and protection and are very likely to be reduced to bots.

Common Usage of Botnets

- **DDoS**

  The most direct use case of botnets, thanks to their large scale, is seen in DDoS attacks. Most botnets comprise tens of thousands of hosts, which, plus the cheap bandwidth resources and long online hours, explains why there are more and more DDoS attacks based on botnets. According to our observation, botnets such as Mirai and gyddos are rather active and even package their capabilities into services, thereby enabling common users to launch botnet-based DDoS attacks and furthering the damage of botnets.

- **Spam**

  Botnets are often used for spamming. In recent years, people have become more and more aware of the dangers of spam, which involves not only inundation of users' inboxes with advertisements and fraudulent messages but also malware delivery and social engineering-based frauds. Necurs is such an infamous botnet.

- **Cryptocurrency**

  Botnet owners make full use of the wide distribution of bots. The cryptocurrency market, especially Bitcoins, looked up in 2017, which was largely attributable to the involvement of hackers. Like traditional sectors, the cryptocurrency sector is targeted by various attacks, including those against cryptocurrency miners. These attacks were presumably some type of competition that characterizes the cryptocurrency business because, if the victim miner's computing power is compromised during an attack, the chance of mining cryptocurrency will be higher for other miners. Besides, hackers begin to leverage the computing power of botnet clusters for cryptocurrency mining.

IoT Botnets Prevalent in Recent Years

As we mentioned before, the rise of the IoT has a great implication on the botnet trend. For this reason, NTI includes IoT botnets in its monitoring scope. Some most discussed and influential IoT botnets are described in detail as follows.

Mirai

This is a very influencing IoT botnet that emerged in 2016. Following is a review of the Mirai event [7] :

1. On August 31, 2016, researchers, after reverse engineering, published a detailed Mirai analysis report on MalwareMustDie, which listed C&C servers and enraged Anna-Senpai, the hacker behind this malware.
2. On September 20, 2016, KrebsOnSecurity.com, owned by the well-known security journalist Brian Krebs, was subject to a massive DDoS attack, with traffic peaking at 665 Gbps. Brian Krebs speculated that this attack was launched by means of the Mirai botnet.

7 http://www.freebuf.com/articles/terminal/117927.html

3. On the same day, French web host OVH suffered a record-breaking DDoS attack, also from Mirai, at a rate of 1.1 Tbps, which then peaked at 1.5 Tbps.
4. On September 30, 2016, Anna-Senpai disclosed source code of Mirai on Hack Forums and mocked at previous researchers' incorrect analysis.
5. On October 21, 2016, US domain name service provider Dyn was hit by a massive DDoS attack, which was believed to originate largely from the Mirai botnet.

Mirai is now still active in the cyberspace. By December 2017, its new variant dubbed Satori had infected over 280,000 IP addresses. In January 2018, a researcher with the screen name of unixfreaxjp discovered the first time ever in the history of computer engineering a piece of Linux malware designed to infect ARC CPU and dubbed this new Linux ELF malware Mirai Okiru. By that time, no antivirus product had ever detected this malware.

Rowdy

In August 2017, NSFOCUS's DDoS situation awareness platform detected anomalous bandwidth usage over a customer's network, which, upon analysis, was confirmed to be a distributed denial-of-service (DoS) attack. The attack was characterized by different types of traffic, including TCP flood, HTTP flood, and DNS flood. Tracing source IP addresses, we found that the attack originated from STBs, a type of terminal device of cable TV (CATV). Then we captured a sample for further analysis of the attack behavior pattern. According to our evaluation, Rowdy had created quite a large botnet in only a few months, infecting devices from five vendors based in China. What is the installed base of STBs in China? According to the *Statistical Communique of the People's Republic of China on the 2016 National Economic and Social Development* released by the National Bureau of Statistics in February, the actual number of STB users had reached 223 million by the end of 2016, while in the *2017 Midyear OTT Operations Big Data Blue Paper* by AVC, the number stands at 240 million. Rapid infiltration into such a huge network by Rowdy will lead to disastrous consequences.

DarkCat

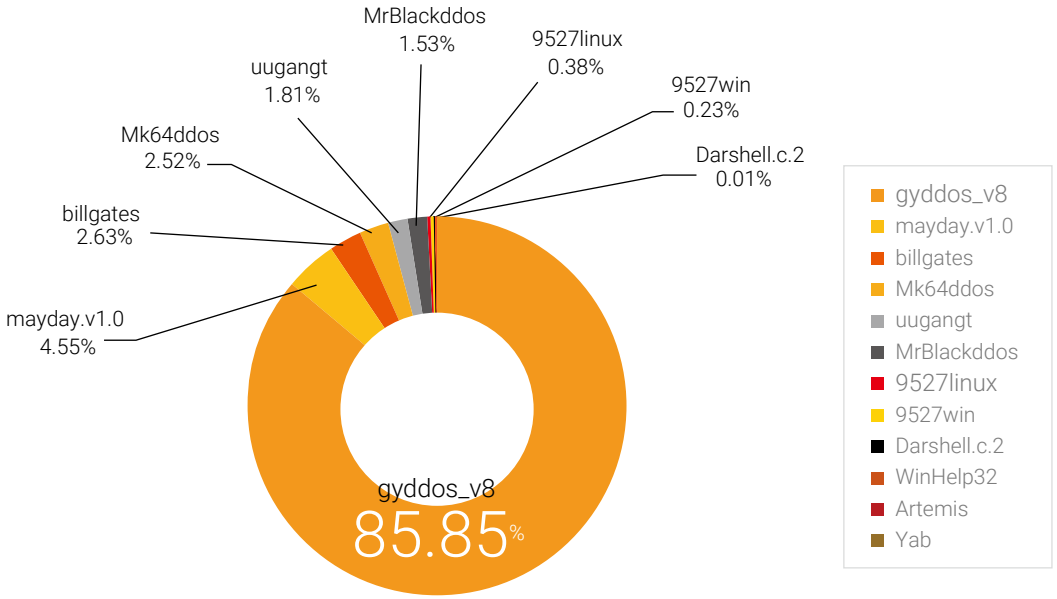
Network terminals, such as STBs, fiber modems, and routers, run the embedded Linux system based on the Microprocessor without Interlocked Pipeline Stages (MIPS) architecture in most cases. They are managed via web portals and usually also support remote management protocols like Telnet and Secure Shell (SSH). Moreover, most devices support execution of common shell commands via the built-in BusyBox, including ps, netstat, ls, and cat. Worse still, some devices use default or weak passwords for management purposes. At the end of 2017, NSFOCUS's emergency response team received successive feedback from a host of carrier customers on the anomalous traffic detected in users' fiber modems. After analyzing the captured packets, we found that these devices were infected with a worm. The naming convention of this virus program is "cat + five random characters", for example, catburhk. For this reason, it was dubbed DarkCat.

3. Most Active Botnet: gyddos

Gyddos is an active and influential botnet in China, which is developed on Windows platforms. In the recent botnet activity monitoring, we saw a whirlwind of gyddos activities. This botnet family has been around for years, with a number of variants and a quite mature commercial operations model. Therefore, special attention should be paid to and special measures should be taken against this botnet.

High Activity

When monitoring some botnet families active in China, we discovered that the gyddos family was the most rampant in terms of the frequency and number of instructions. Of all C&C hosts, those of gyddos-v8[8] alone issued 85.85% of communication instructions, putting it on top of the list.

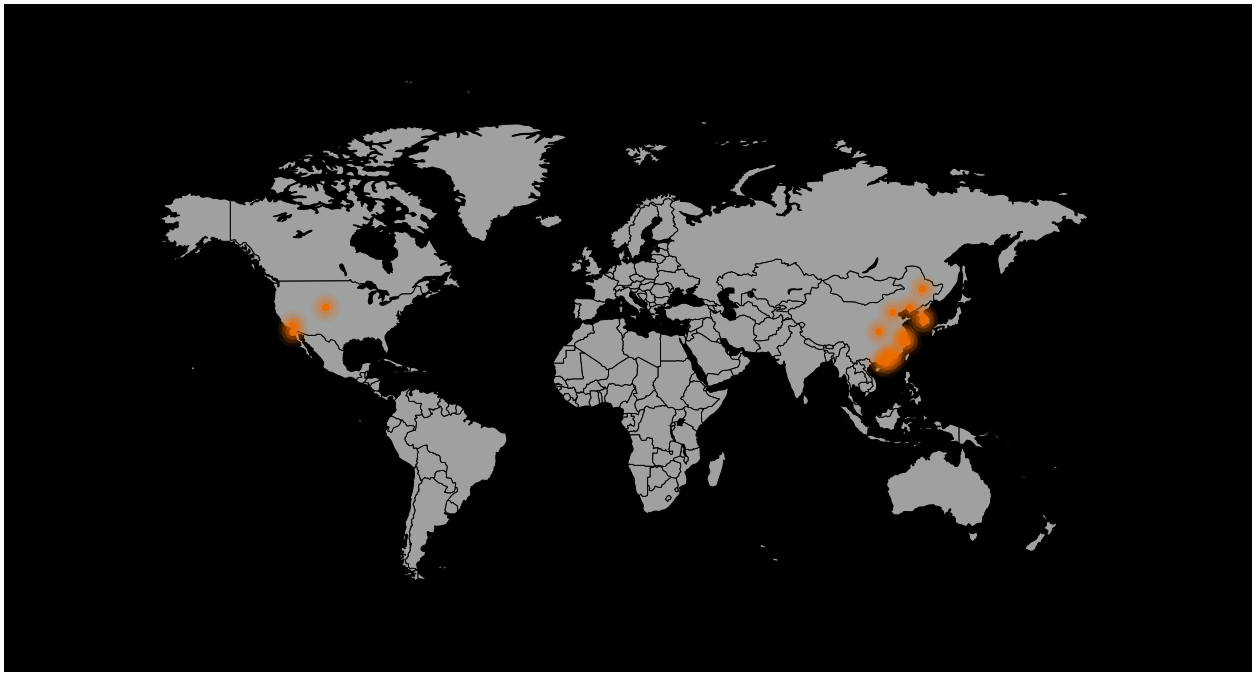


At its heyday, gyddos-v8 was found to be responsible for 31,264 attacks.

8 We have captured 10 variants of gyddos samples and dubbed them gyddos-v1, gyddos-v2, ⋯, gyddos-v9, and gyddos-X1 respectively.

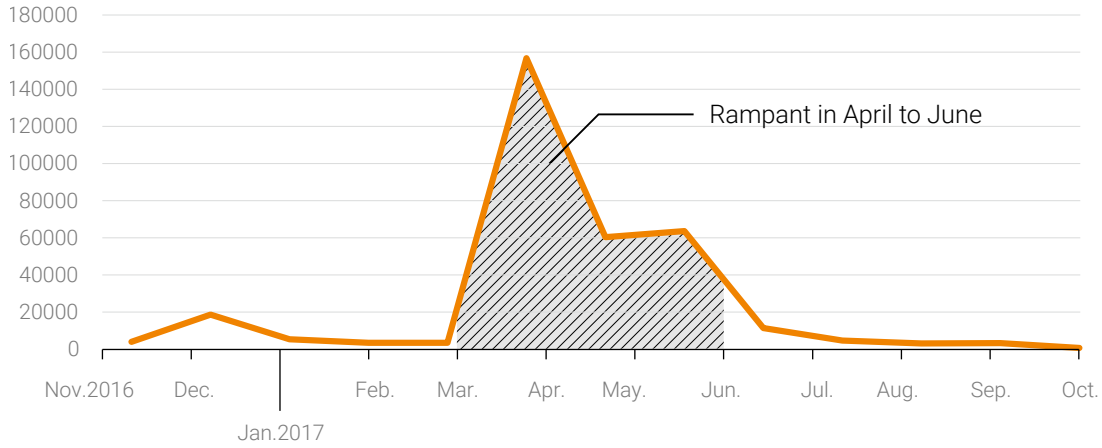
Our statistics show that most C&C hosts of gyddos are in China, the USA, and South Korea. As for China, coastal areas in the southeast were most affected by this botnet.

Figure 8. Geographic distribution of C&C servers of gyddos-v8



As shown in the following figure, gyddos-v8 was most active from April to June in terms of the number of communication instructions issued by C&C hosts.

Figure 9. Monthly change in the number of instructions issued by C&C servers of gyddos-v8



Early Appearance

This botnet was first discovered and named Nitol by Microsoft in September 2012. From the names of malicious files it generated[9], some researchers speculated that Nitol was the early version of the gyddos family developed by the gyddos workshop. In September 2012, Microsoft discovered that computers sold by some retailers were loaded with counterfeit versions of Windows software embedded with harmful malware, including Nitol, most of whose C&C servers were on the 3322.org domain. Subsequently, the US District Court for the Eastern District of Virginia granted a temporary restraining order to allow Microsoft to host the 3322.org domain through its newly created domain name system, enabling Microsoft to block all malicious communication with this domain. This effectively reduces the impact of network activities carried out by multiple botnet families, including Nitol.[10]

Lots of Variants

Currently, gyddos has at least 10 versions, each of which has more functions than the previous one. At the same time, DDoS attack techniques are continuously upgraded. Now it has become mature enough to launch volumetric attacks, to spread across a large area, and to support different business operation models.

- **gyddos v1-v4**

  Capable of issuing basic instructions and launching common attacks like TCP flood and UDP flood attacks.

- **gyddos v5**

  Adds the Ultimate Packer for eXecutables (UPX) option to compress the volume of files at the controlled end.

  Adds a CC attack module (by reference to the source code of ImDDoS).

  Adds the lpk.dll hijacking function, making it possible to use any exe file to reactivate gyddos.

  Adds the intranet IPC$ propagation function (brute-force guessing of passwords).

  Adds the DNS flood module.

  Adds the network interface card (NIC) information in the go-live package.

- **gyddos V6**

  Adds the DownloadFile flood module.

  Fixes the bug of the same bot repeatedly going live (using mutex)

  Adds a mechanism that prevents the LPK infection module from being detected by antivirus software.

- **gyddos V7**

9 http://www.freebuf.com/articles/network/147591.html

10 https://blogs.technet.microsoft.com/microsoft_blog/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain/

Adds remote control functions (for execution of CMD shell commands, file transfer, bulk restart/shutdown, ...).

Adds a function that allows users to define the packet structure for TCP flood and UDP flood attacks.

- **gyddos V8**

  Adds a multitask polling module (enabling bots to conduct pulsing denial-of-service attacks or switch the attack method whenever necessary).

  Optimizes the DNS flood module.

- **gyddos V9**

  Adds a module that allows other attackers to lease bots.

  Adds a bot statistics module (number, system, and geographic distribution of bots).

- **gyddos X1**

  Adds an SSDP amplification attack module.

  Adds an NTP reflection attack module.

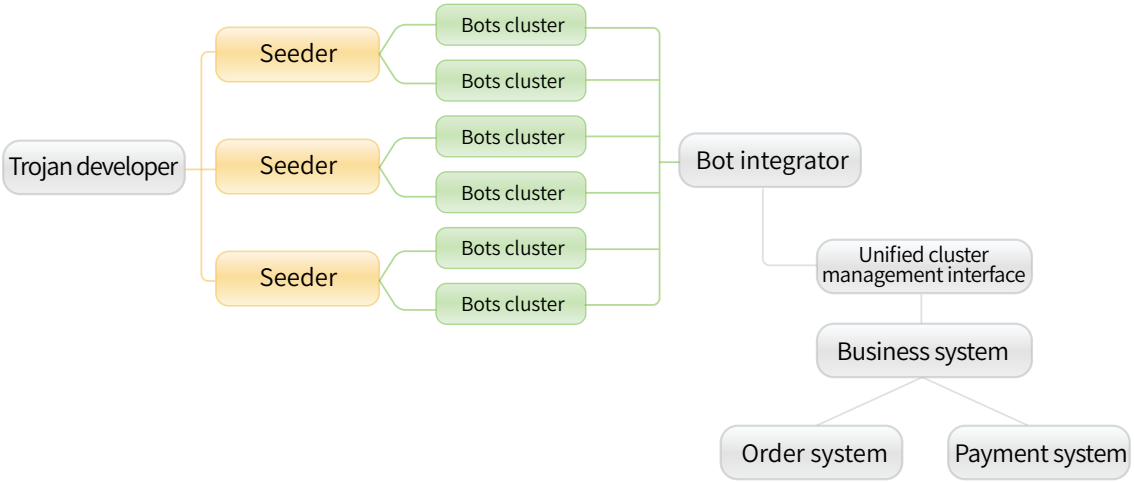
Long Life

Our earliest detection of gyddos's activities can be traced back to November 2013, when we tracked and monitored more than 100 C&C servers. Up to now, more than four years have passed, and most C&C servers detected back then, and botnets controlled by these servers are still alive, tenacious of life.

During routine monitoring, NTI detects attacks launched by this family from time to time. This indicates that it is a widely distributed and highly influential botnet family.

Commercialized Operation Model

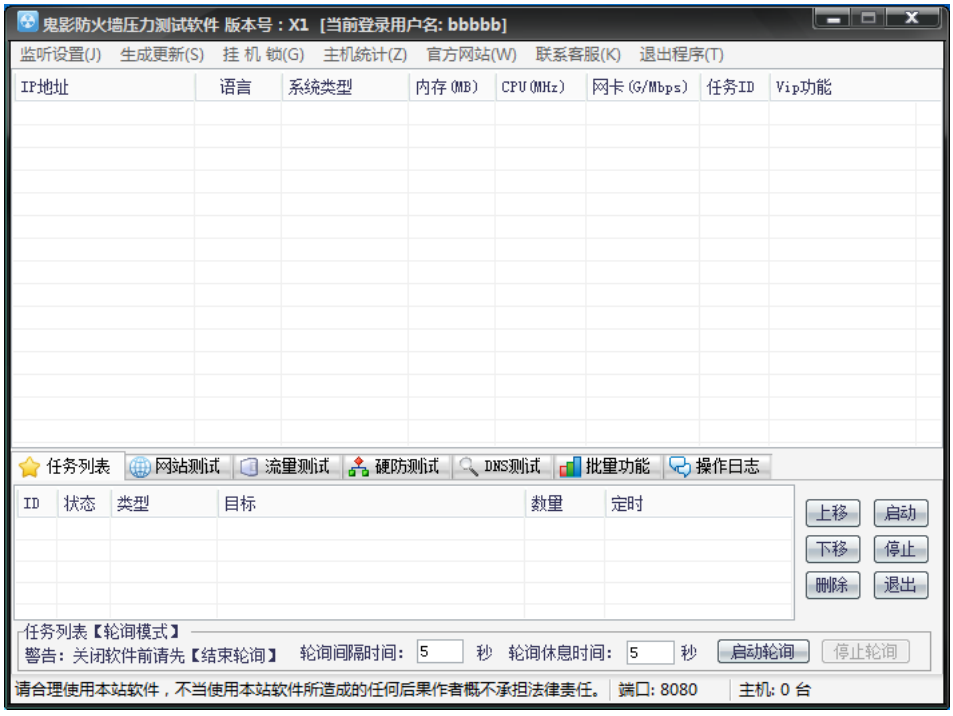
Using botnets to infect other devices has become quite a mature method characterized by a relatively fixed process composed of multiple stages, which involve different roles in the black industrial chain that are keen on making easy money.



More often than not, multiple roles are assumed by the same organization or individual. However, to provide a clear picture of the ecosystem of the underground botnet market, we assign different tasks to different roles in the preceding industrial chain. Trojan developers make money mainly by selling code, without direct involvement in hacker activities. Quite a few developers claim that they are developing hacking tools for testing purposes, which are in reality for sale on the black market for profit. The real "dirty work" is done by seeders, who are responsible for spreading malware as extensively as possible to expand the infection base for the ultimate end of selling hosts under their control to bot integrators. A bot integrator, after integrating bot resources, manages large-scale bot clusters in a centralized manner, which features a client program or web interface for users to conveniently customize attacks. Then users complete the transaction by paying tokens[11] via the payment system. Moreover, as a downstream player in the value chain, integrators exert themselves to promote the botnet business through various marketing activities.

Over years, gyddos has continuously been optimized and added management functions, making the cluster control capability more stable and reliable and preparing the software for service commercialization on the black market. Bot integrators of gyddos have tried every means to promote the DDoS service through instant message groups and forums. They offer a client program for users to log in to schedule resources for targeted attacks.

11 Tokens are a virtual form of currency like game cards and Bitcoins. Tokens can be converted to real currency at a certain exchange rate. Trading with tokens can be conducted with unreal names, thus making it possible to hide the real identity of those engaging in the trade.



Our long-time observation suggests that entities expecting to launch DDoS attacks are mostly operators of porn, gambling, lottery, private server, perverted game, and porn game websites. Their major motive is to defeat competitors in the same industry. These users, though without hacking skills, can launch volumetric attacks, with no fear of exposing their true identities thanks to the covert nature of online transactions. Low costs, low risks, and ideal effects are three main factors that have contributed to the rapid development of the DDoS service across the globe.

4. Defenses Against Botnet Attacks

Botnets have long established themselves as a substantial cyber threat. Now they are proved to be even more menacing in new network environments. With the constant development of the Internet, botnets keep expanding in size and improving adaptability, posing more challenges to the defensive side. Botnet activities can be used as an indicator to assess the overall security of the Internet. In the ongoing monitoring of botnets, we have found that the Internet environment in China is imbued with complicated dynamics, which adds to the difficulty of management (for enterprises) and governance (for governments). Nowadays, technologies are evolving day by day, so are botnets. Attackers are using them to detect vulnerabilities in new devices and new software applications, and continuously employ new attack tools and techniques to expand their sizes. Botnets grow side by side with the Internet, managing to survive in an immature network environment. The propagation of botnets tells us that large quantities of misconfigured or vulnerable devices on the Internet are the hotbed of large botnets. Our projection is that this situation will persist for a long time or even become more intense over time. Enterprises or individual Internet users should do a good job in proactive protection for two purposes: First, they should configure devices and software properly and update them in a timely manner, and take necessary security measures, such as installing antivirus software and deploying mature security solutions, to effectively prevent devices from being reduced to bots, thus nipping botnets in the bud; second, they should keep an eye on the botnet development trend, understand the real-life threats of botnets, and deploy security measures accordingly, to effectively maintain the normal operation of business.

NTI will conduct ongoing monitoring of the botnet development trend and regularly release intelligence regarding botnet activities, in hopes of helping enterprises defend against related attacks and providing them with a valuable insight into this ever-changing trend.

NSFOCUS

THE EXPERT
BEHIND GIANTS

Over years, NSFOCUS has been committed to defense researches in the cybersecurity realm, providing most competitive security products and solutions for governments, carriers, and financial, energy, Internet, education, and medical sectors, ensuring customers' business continuity. To these customers, NSFOCUS lives up to the reputation of a trustworthy expert.

www.nsfocusglobal.com