NSFOCUS

H1 2017 Cybersecurity Insights

Table of Contents

1 Executive Summary

This year a significant amount of security events such as WannaCry, Petya, and NotPetya occurred adversely affecting a wide variety of social and economic activities. To mitigate threats brought by such events IT and security teams have spared no effort in combating against such attacks for the security and protection of their organizations. It is worth noting that network attack events have resulted in an economic loss of up to $50-billion USD globally. With various new techniques and threat environments rapidly evolving it is necessary to constantly examine various practices, techniques, system configurations, and ecological environments to uphold the greatest security in-depth as possible.

In the era of the Internet of everything (IoE) there is no individual organization that is always 100% secure. Instead of being aggressive to completely prevent penetration and disclosure defenders tend to control the risks within the acceptable level to avoid the "broken window effect" which makes any security measure less effective leading to attacks at a higher success rate. To achieve an enhanced security level, defenders must assess the overall security posture and target systems to align security policies, best practices, and standardization with the assessment results. Moreover, executives and operating teams can use threat intelligence as an auxiliary means to determine their current security posture, observe threat actor motivations, and tune policy architecture accordingly.

IP addresses serve as the cornerstone of the Internet. Malicious IP addresses are those IP addresses found to be associated with certain malicious behaviors such as denial of service (DoS) attacks, intrusions, scanning, and sending of spam emails. Such IP addresses tend to be members of certain botnets and criminal gangs. A botnet army consisting of tens or hundreds of thousands of IP nodes causes destructive damage to any business or organization. It is of great importance for organizations to master the distribution, evolution, and dynamic changes of malicious IP addresses across the Internet to protect key infrastructure.

Data shared by Gartner at the security summit in the Washington D.C suggested that in recent years an astonishing 300 million new malware strains have emerged exploiting dozens of known vulnerabilities. According to monitoring data analyzed during the first half of 2017, the number of exploitations of the top 10 vulnerabilities accounted for 50.8% of the total exploitations.

Struts2 became a focus in the first half of this year as five vulnerabilities in it have been exploited. In the week when the S2-045 vulnerability was released to the wild, NTI discovered 19,396 attack attempts attributed to this vulnerability. Attacks based on Struts2 made up more than 80% of total attacks against all frameworks and applications.

Reflective amplification attacks still maintain a dominant position in DDoS attacks. Reflective amplifiers have become "time bombs" within the network ecology as well as low-cost and low-risk powerful weapons of attackers. Low cost, rapid return, high average revenue per user (ARPU) and low risk ransomware is booming in the black industry.

It should be noted that blackmailers demonstrate flexible business capability by providing different price packages based on the number of files and consumption level. With the rapid evolvement of the Internet of Things (IoT), ransomware, and its variants such as DDoS ransom and database ransom attacks will continue to grab the attention of security teams and be exploited in the media spotlight.

2 Attack Sources

Figure 2-1 Global distribution of attack sources
Source: NTI

According to monitoring data collected by NTI, 60% of malicious global IP addresses are affiliated with the top 10 countries ranked by GDP with the majority in the US, China, India, and Japan.

Country	GDP Place	Ratio of Malicious IP Addresses
USA	1	18.52%
China	2	19.20%
Japan	3	4.18%
Germany	4	1.57%
UK	5	3.40%
France	6	0.80%
India	7	8.53%
Italy	8	0.69%
Brazil	9	1.52%
Canada	10	0.92%

Table 2-2 Distribution of Malicious IP addresses in top 10 countries ranked by GDP

Source: NTI

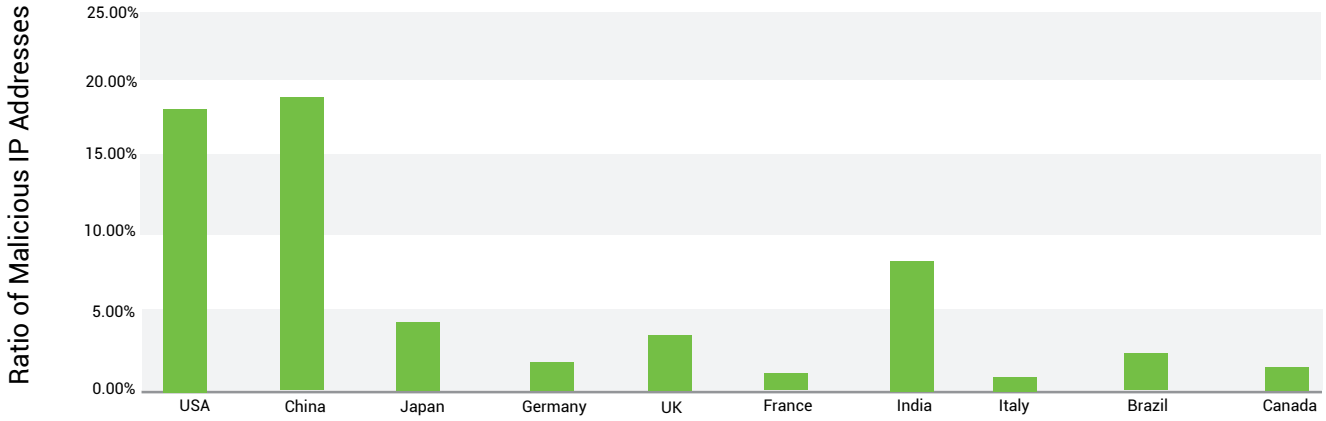


Figure 2-3 Distribution of malicious IP addresses in top 10 countries by GDP

Source: NTI

Distribution of Malicious IP Addresses in Top 10 Countries by GDP

In the network security realm, vulnerability discovery and exploitation are always vital research fields for security teams. NTI closely monitors and analyzes vulnerabilities in popular products from major vendors and purports the following:

1. In recent years, there has been an upward trend in new vulnerabilities revealed each successive year. For the first half of 2017, 4144 new vulnerabilities were disclosed. More vulnerabilities concerning permissions, privileges, and access control are unveiled each year with a significant increase since 2016. From the risk level perspective, the proportion of high-risk vulnerabilities declined, while that of medium-risk has risen.
2. Buffer overflow vulnerabilities have caused greater damage at a more rapid pace since 2015. This kind of vulnerability has gained favor with attackers because they can result in DDoS attacks and remote code execution.
3. Compared with the same period last year, the total number of vulnerabilities has increased by 50% in the first half of 2017, with medium-risk vulnerabilities rising the fastest. Vulnerabilities concerning permissions, privileges, and access control were the greatest in number and gained largest increase.
4. The most noteworthy vulnerabilities in the first half of 2017 are as follows:
    a. Struts2 became a focus with five vulnerabilities being exploited. NTI discovered 19,396 attack attempts based on this vulnerability
    b. The Windows SMB Remote Code Execution Vulnerability (MS17-010) was a highlight in the first half of 2017 due to its exploitation by the Equation Group.
5. For the majority of the exploited vulnerabilities official patches are available.
   In the last three years newly revealed vulnerabilities have denoted an upward trend within the cyber-security arena.

3 Vulnerability Insights

4144 new vulnerabilities were disclosed for the first half of 2017 marking an increase of 50% with that same percentage increase for the preceding years. Of the combined vulnerabilities 2561 were high-risk, 1254 medium-risk, and 329 were considered low-risk. Compared to the same time frame of last year, medium-risk gained the largest increase and accounted for a higher proportion with high-risk classification attributing to the lower end of the overall spectrum.

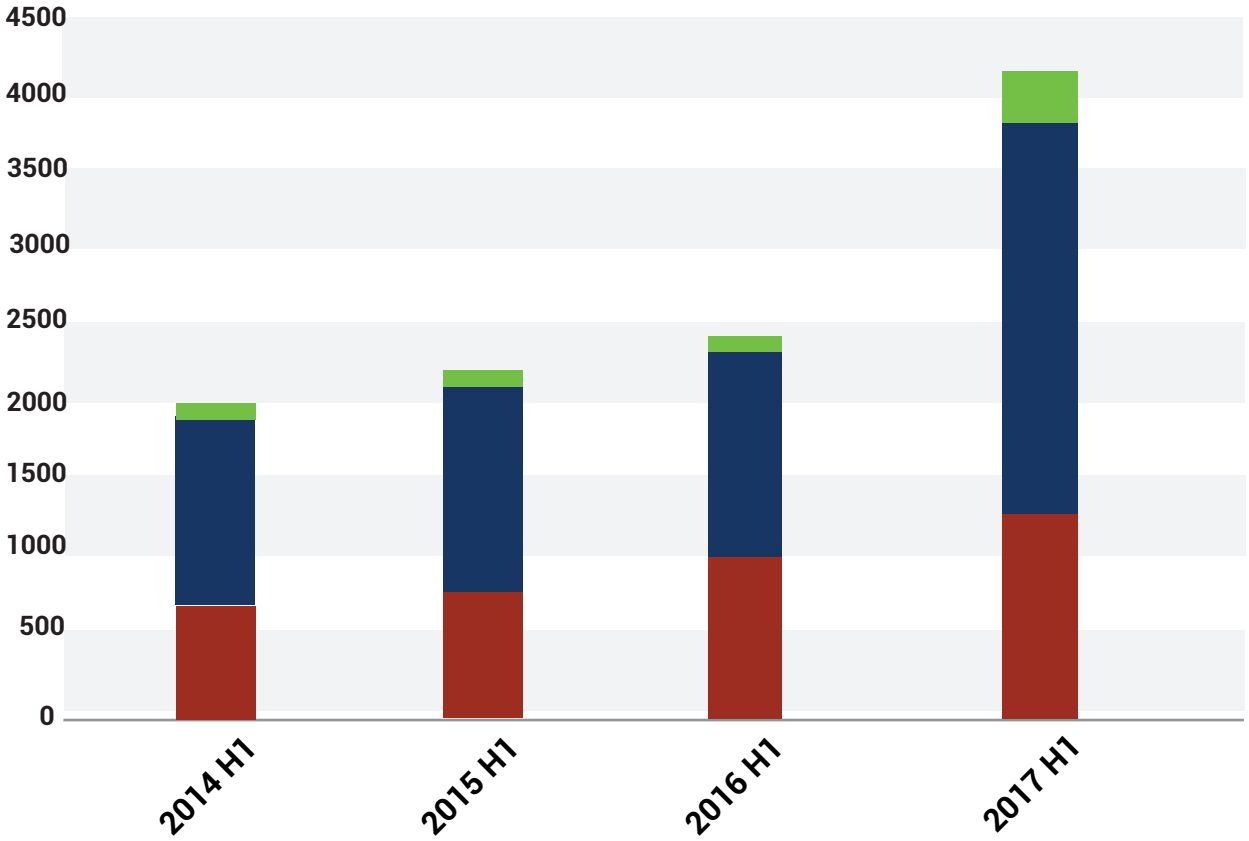


Figure 3-1 Quantity Changes of Vulnerabilities of Various Risk Levels (2014-2017)
Source: NTI

Vulnerabilities concerning permissions, privileges, and access control contributed the largest share, mainly consuming the majority of high and medium-risk vulnerabilities. Buffer overflow vulnerabilities came second, with more than 55.7% being high-risk. Besides, cross-site scripting (XSS) vulnerabilities, cross-site request forgery (CSRF) vulnerabilities, SQL vulnerabilities,
path traversal vulnerabilities, and cryptographic issues were major types of vulnerabilities discovered in the first half of 2017.

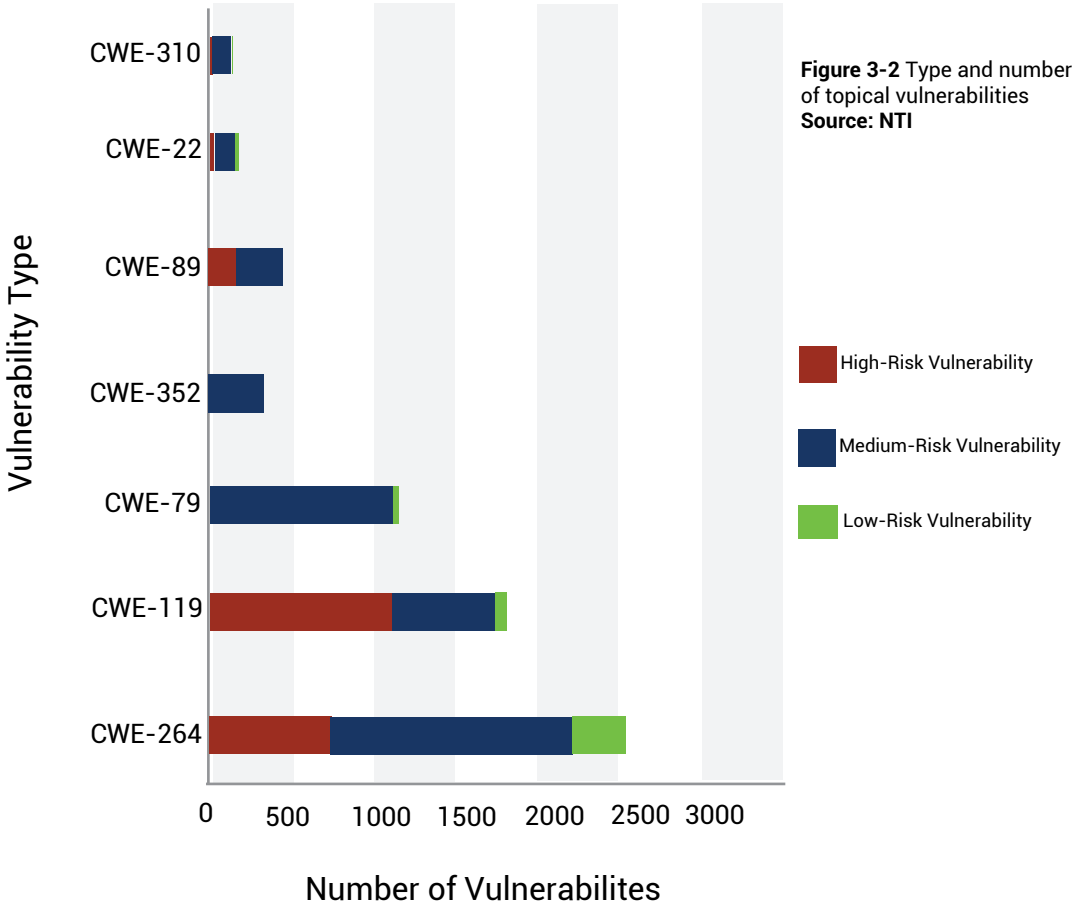


Figure 3-2 Type and number of topical vulnerabilities
Source: NTI

In the last few years there have been several types of vulnerabilities that have gained the greatest momentum to include: account permissions & privileges, access control, buffer overflow's, and XSS vulnerabilities. The remaining application vulnerabilities have not witnessed this steady increase as noted with the former.

Vulnerabilities regarding permissions, privileges, and access control have experienced apparent growth following 2016. Buffer overflow vulnerabilities are on the rise since 2015 and this particular vulnerability has received noticeable recognition among attackers because of the DDoS attribution associated with remote code execution probability.

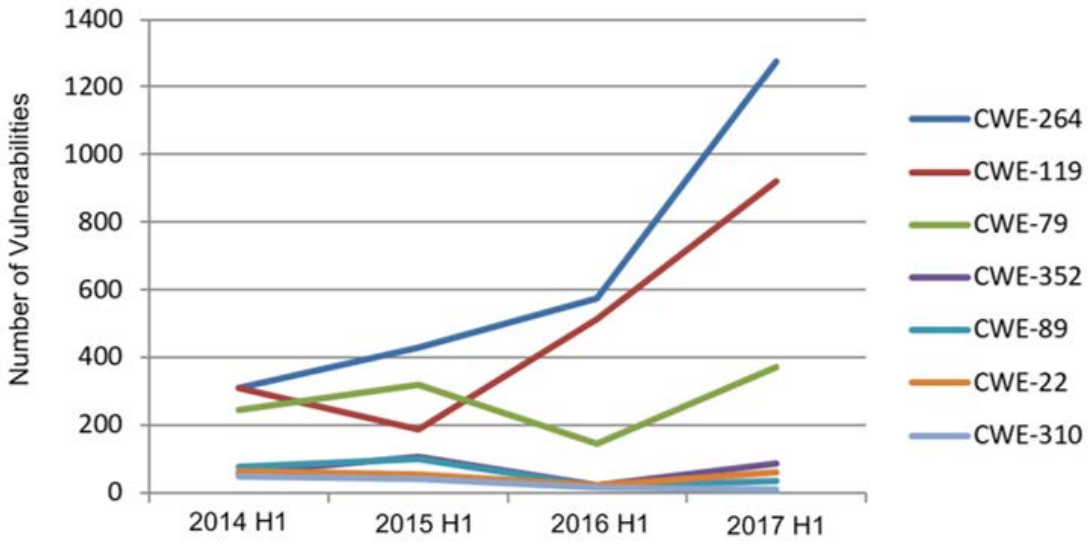


Figure 3-3 Quantity Changes of Various Vulnerabilities (2014–2017)
Source: NTI

CWE ID	Vulnerability Category
CWE-264	Vulnerability relating to permissions, privileges, and access control
CWE-119	Buffer overflow vulnerability (due to improper restrictions on border operations of the memory buffer)
CWE-79	Cross-site scripting vulnerability
CWE-89	SQL injection vulnerability
CWE-352	Cross-site request forgery vulnerability
CWE-22	Path traversal vulnerability
CWE-310	Cryptographic issues

Table 3-2 Mappings between Vulnerability and Common Weakness Enumeration (CWEs')

3.1 Vulnerability- Based Attacks and Exploitation

NSFOCUS data points have indicated that many vulnerabilities that were released many years ago are still very active. The oldest vulnerability (CVE-2002-0649) can be traced back as early as 2002. Most exploitations focus on a few well-known and influential vulnerabilities. According to data shared at the 2017 Gartner Security & Risk Management Summit held in Washington D.C up to 300 million pieces of malware were discovered this year.

Vulnerability Name and ID	Percentage of Vulnerability Exploitations
Microsoft Windows ASP.NET Denial-of-Service Vulnerability (CVE-2009-1536)	12.1%
Microsoft SQL Server 2000 Resolution Service Remote Heap Corruption Denial-of-Service Vulnerability (CVE-2002-0649)	8.8%
Microsoft Network Policy Server RADIUS Denial-of-Service Vulnerability (MS16-021) (CVE-2016-0050)	8.3%
Microsoft Internet Explorer ASLR Security Restriction Bypass Vulnerability (MS15-009) (CVE-2015-0051)	3.8%
OpenSSl SSLv2 Weak Encryption Communication Method DROWN Vulnerability (CVE-2016-0800)	3.5%
Apache Struts Remote Command Execution Vulnerability (s2-008)	3.4%
Microsoft mshtml.dll Library GIF Image Processing Remote Denial-of-Service Vulnerability (MS04-025)	3.0%
Struts2 Remote Command Execution Vulnerability (s2-045) (s2-046) (CVE-2017-5638)	2.7%
Squid Proxy DNS Name Resolver Remote Denial-of-Service Vulnerability (CVE-2005-0446)	2.7%
GNU Bash Environment Variables Remote Command Execution Vulnerability (CVE-2014-6271)	2.5%

Table 3-2 Top 10 Vulnerabilities by exploitation percentage
Source: NTI

3.2 Monitoring of Topical Vulnerabilities

In April 2017, the Shadow Brokers publicly released a trove of specially crafted state-sponsored hacking tools and various confidential documents stolen from the infamous NSA's Equation Group. Some of the published documents had been initially auctioned by Shadow Brokers for millions of dollars.

The leaked files consist of three primary sections to include: Windows, Swift, and Odd with the hacking tools exploiting the Windows directory and making use of the IIS 6.0 remote vulnerability. SMBv1 exploits that were not publicly known prior to Shadow Brokers have been used to attack Windows systems with port 445 opened and successfully attempting to escalate privileges. Moreover, the remote vulnerability exploit in the RDP service can be used to attack Windows machines with port 3389. The following table lists vulnerabilities unveiled in the first half of 2017 (all by Shadow Brokers) and the affected ports and services.

Vulnerability ID	Vulnerability Source	Affected Product
CVE-2017-3881	Vault 7	Cisco Cluster Management Protocol
CVE-2017-0143	ETERNALBLUE	SMBv1 server
CVE-2017-0144	ETERNALBLUE	SMBv1 server
CVE-2017-0145	ETERNALBLUE	SMBv1 server
CVE-2017-0146	ETERNALBLUE	SMBv1 server
CVE-2017-0147	ETERNALBLUE	SMBv1 server
CVE-2017-0148	ETERNALBLUE	SMBv1 server
CVE-2017-8487	ENGLISHMANSDENIST	OLE
CVE-2017-0176	ESTEEMAUDIT	RDP
CVE-2017-7269	EXPLODINGCAN	IIS 6.0

Table 3-3 Vulnerabilities Discovered 1H 2017
Source: NTI

According to attack monitoring data of NTI, Equation Group vulnerability-based attacks underwent an exponential growth in May and June of this year. We believe that this is directly related to the recent wide-scale deployments of WannaCry and NotPetya ransomware malware.

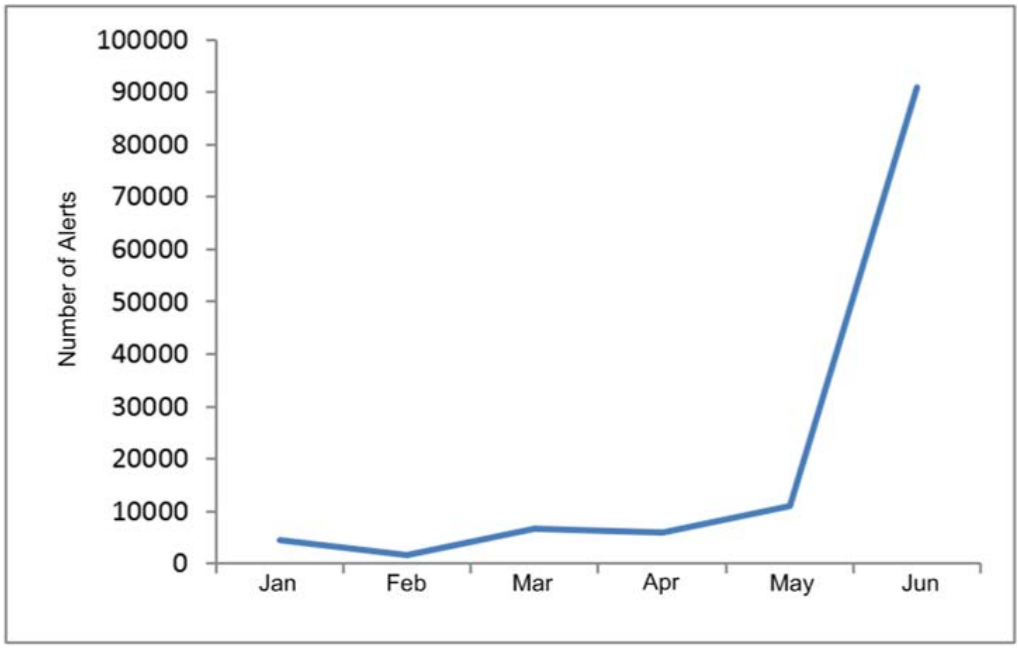


Figure 3-4 Vulnerability Alerts Related to Equation Group Information Release

NSFOCUS discovered four major key findings from our website security protection monitoring data:

1. Website application attacks remain most prevalent among exploited areas of attack
2. SQL injections are still the most commonly exploited attack vector
3. 80% of compromised assets are due to old vulnerabilities and un-patched systems
4. Struts2 is frequently exploited and continues to be recognized as the most vulnerable in web frameworks and applications

4 Website Security Trend

4.1 Distribution of Website Attacks

As per data accumulated from first half of 2017, website application attacks remain at the top of most targeted platforms with the primary attack vectors being:

- SQL Injections
- Known Vulnerabilities
- Path Traversal
- Cross-site Scripting
- Illegal Upload
- Remote Command Execution

Moreover, the monitoring of various websites found that:

- 82% websites fell victim to multiple web attack types
- 79.3% were old un-patched web vulnerabilities
- 45.9% were path traversal attacks
- 44.3% of attacks contributed to SQL injections

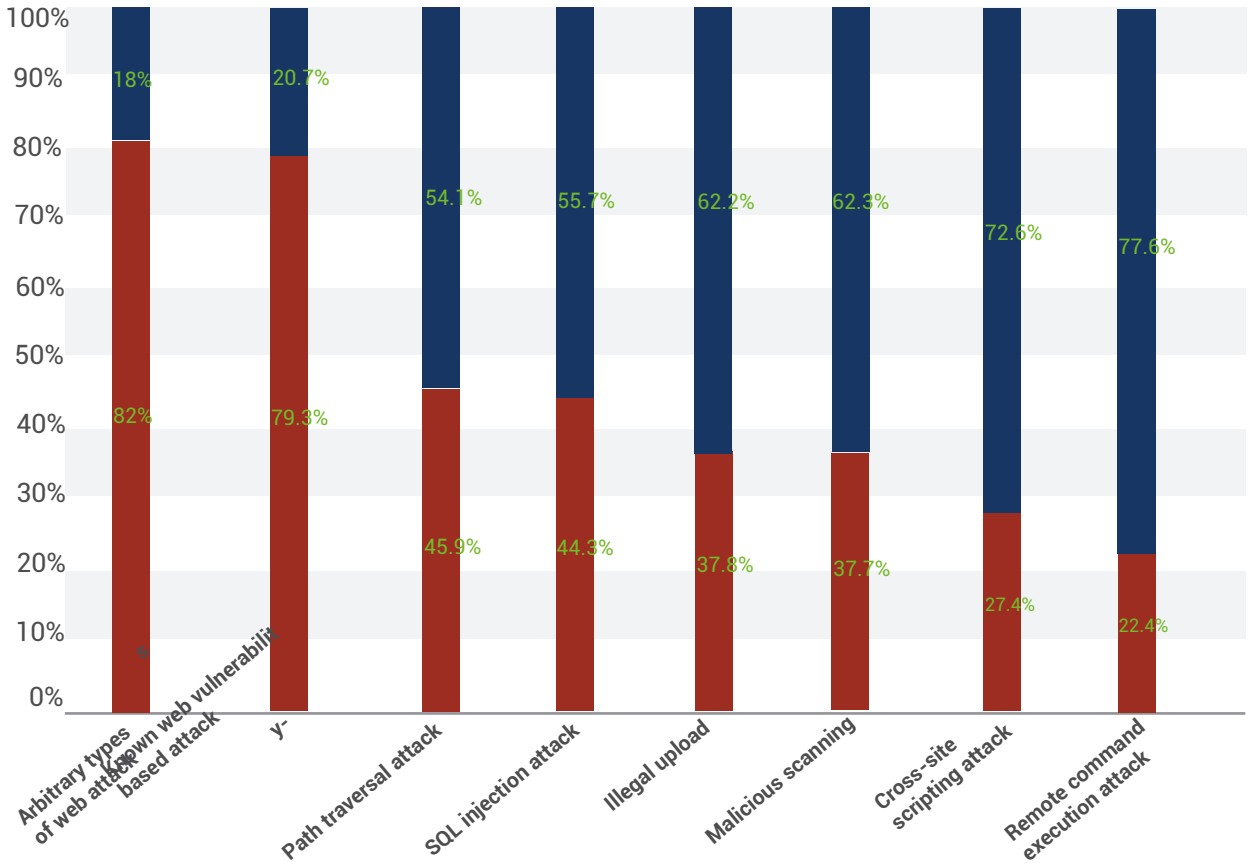


Figure 4-1 Distribution of attacked websites in H1 2017

Source: NSFOCUS Managment Security Service (MSS)

Website Security Trend

Traditionally, most web application attacks rely on several common vulnerabilities. Web attacks can be launched at a low cost with basic attack methods and vulnerability exploits embedded and integrated into various attack tools such as China Chopper and SQLmap. These contributing factors make it easy to launch successful web application attacks.

Websites are ripe to attack for several reasons. These include web service hosting, affiliated web service system architecture, and multiple web applications running to support multiple congruent web services. These elements combined with complicated software architecture promotes easily exploitable vulnerabilities. Meanwhile, the technology between websites are highly homogenized and each attack method can impact global website services considerably.

Additionally, for new vulnerabilities script kiddies regularly employ scanning techniques utilizing search engines such as Google to gain a considerable amount of web shell ability in a short time. Together with open network scanning engines such as Shodan this facilitates targeted attacks by exploiting web service vulnerabilities.

Let's take Apache Struts2 (the most popular Java web server framework) as an example. Five vulnerabilities (S2-045–S2-049) were detected in a six month time-frame impacting Struts2.3 through Struts2.5. The S2-045 vulnerability (CVE-2017-5638) revealed in March appeared to be the most detrimental. The Jakarta Multipart parser plug-in of Apache Struts2 is prone to a remote code execution vulnerability that can be triggered if the attacker uses this plug-in to upload files and change the Content-Type value of the HTTP header.

According to NSFOCUS monitoring data related to this vulnerability, many vulnerable websites are distributed globally with the majority residing in economically developed regions such as US, China, Japan, and Europe. As shown in Figure 4-2, in the week following after the vulnerability was released a total of 19,396 attacks based on this vulnerability were detected with an average of 2771 attacks each day. The most attacks occurred on March 10th totaling 8925. It was also discovered that attackers exploited the S2-045 vulnerability for ransom receiving a total of 84 Bitcoins (equivalent to USD 100,000).

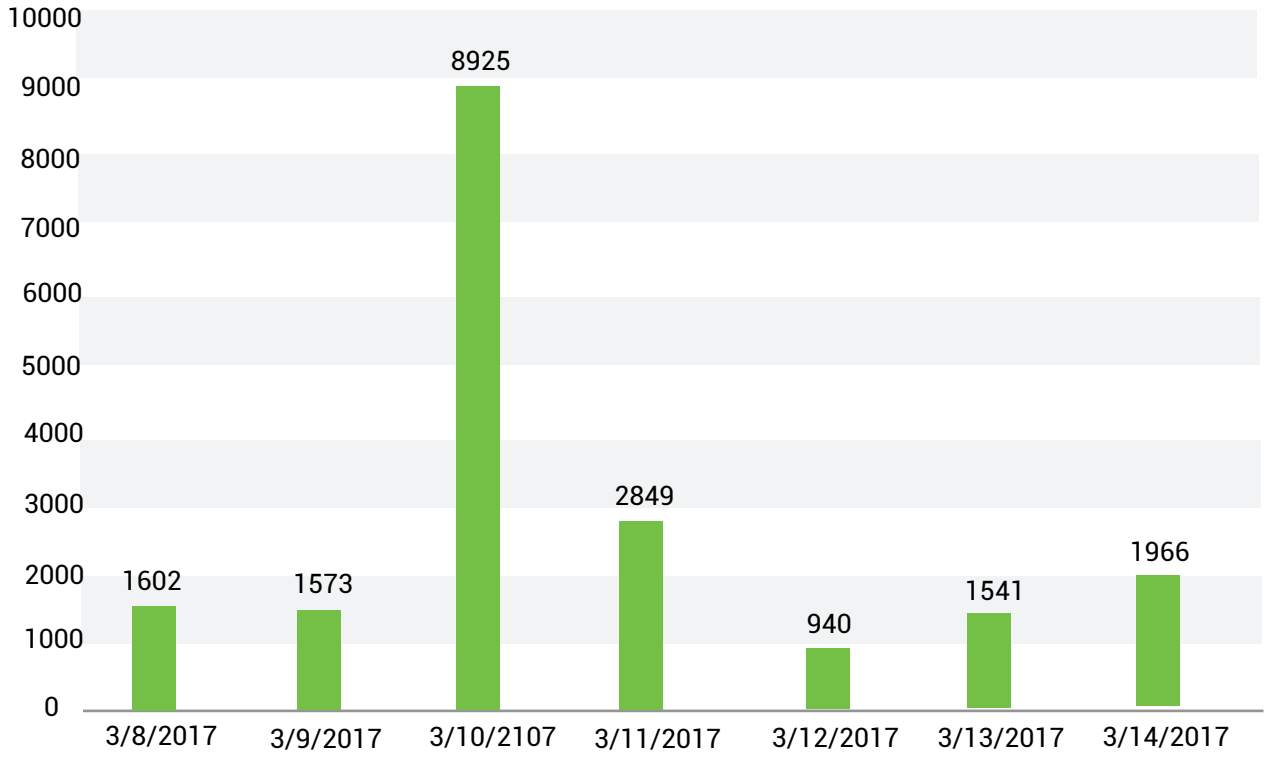


Figure 4-2 Attacks against monitored websites after Struts2 (S2-045) vulnerability release
Source: NSFOCUS MSS

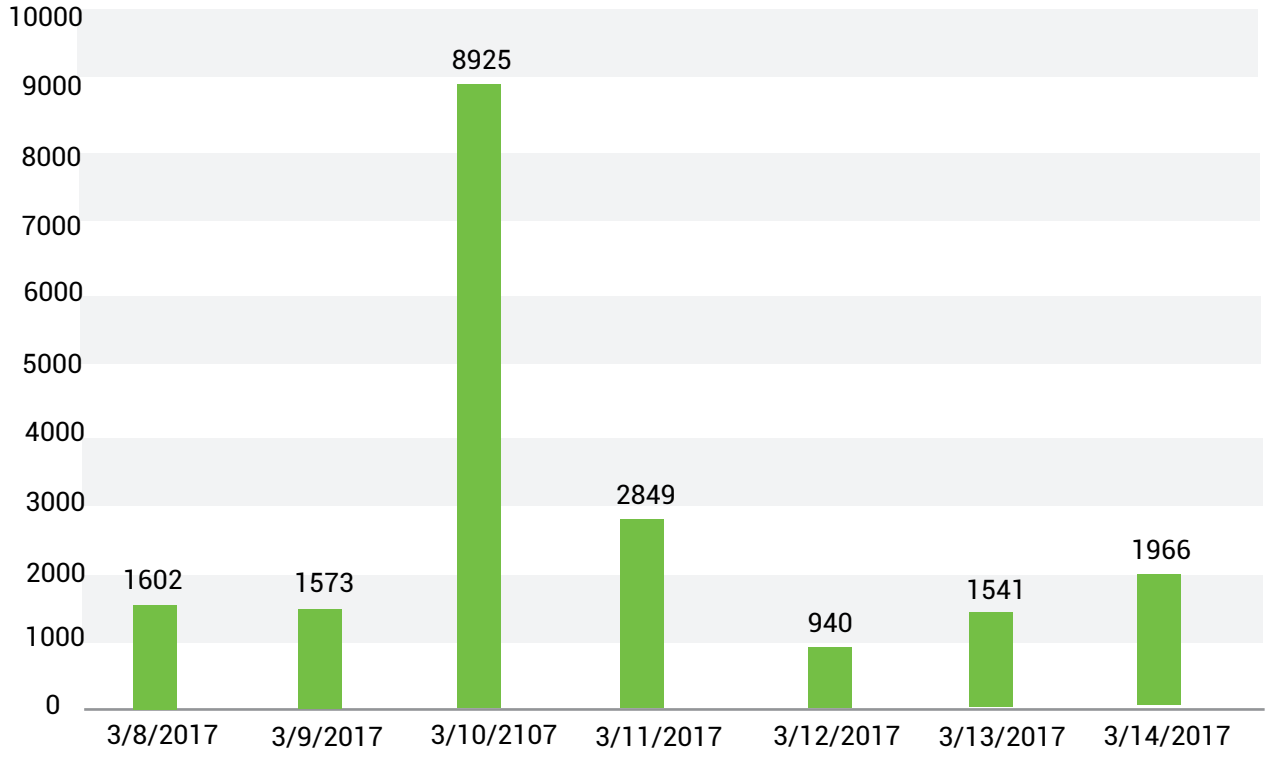


Figure 4-2 Attacks against monitored websites after Struts2 (S2-045) vulnerability release
Source: NSFOCUS MSS

4.2 Web Attack Type Distribution

In terms of attack types SQL injection is still the most common attack method accounting for 40.8% of all total cyber-security attacks.

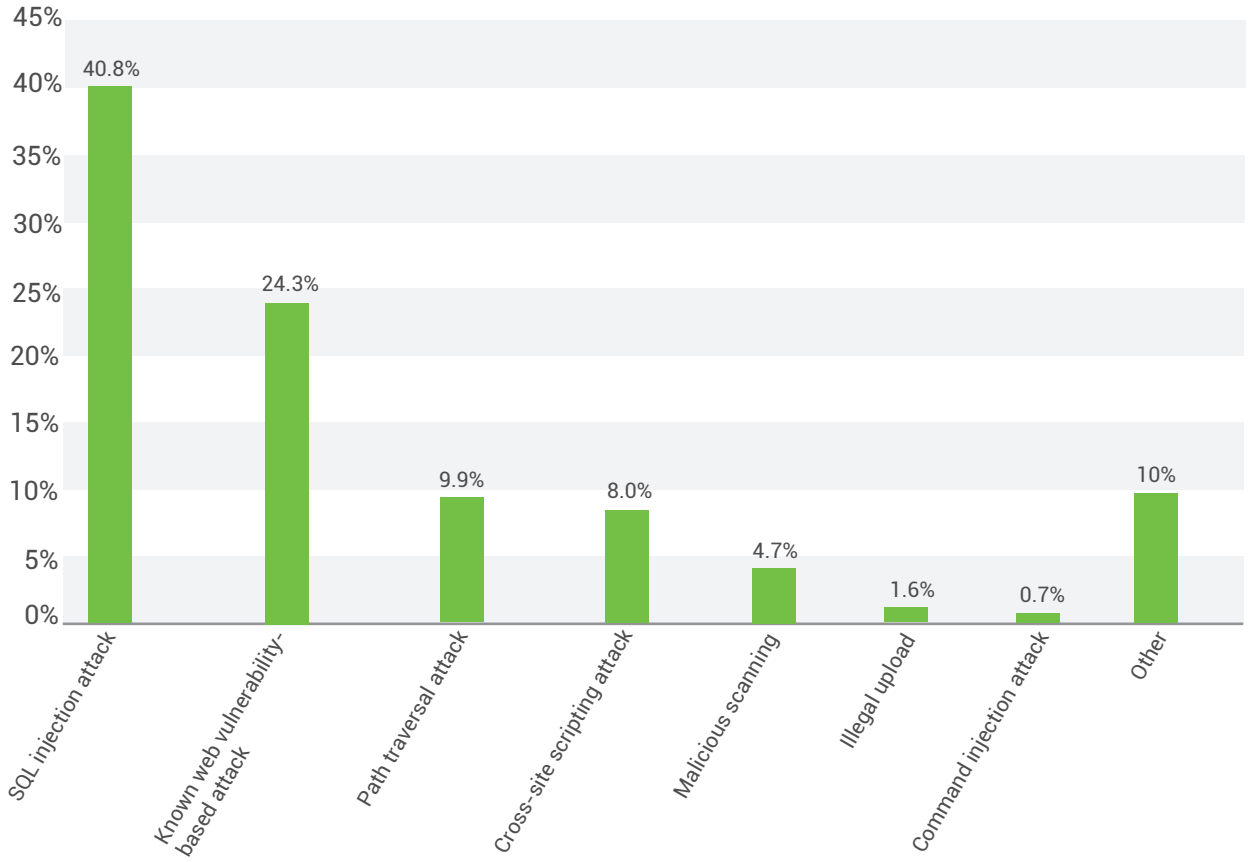


Figure 4-3 Web attack type distribution in H1 2017
Source: NSFOCUS MSS

4.3 Web Vulnerability Exploitation

From the perspective of exploitation, previous vulnerabilities discovered in the past contributed to the largest portion among various scanning attack attempts with more than 60% of top 10 vulnerabilities being exploited. This solidifies the importance of prioritizing vulnerability and patch management programs.

Vulnerability Name	Release Date	Percentage
Tomcat Directory Traversal Vulnerability (CVE-2008-2938)	2008	21.7%
IIS File Upload Vulnerability (CVE-2009-4445, CVE-2009-4444)	2009	13.9%
Lighttpd Source Code Exposure Vulnerability (CVE-2006-0814)	2006	6.0%
Nginx File Traversal Vulnerability (CVE-2009-3898)	2009	5.4%
IIS CGI Program Name Parsing Error Leading to File Execution Vulnerability (CVE-2000-0886)	2000	5.4%
IIS File Extension Name Parsing Error Leading to ASP Code Disclosure (CVE-1999-0253)	1999	2.6%
Tomcat Directory Traversal Vulnerability (CVE-2008-5515)	2008	2.4%
Apache Header Data Length Anomaly Leading to Server Resource Consumption (CVE-2011-3192)	2011	2.1%
IIS Script File Name Parsing Vulnerability (CVE-2009-4444)	2009	1.8%
IIS Unicode Character Decoding Error Leading to Remote Command Execution (CVE-2000-0884)	2000	1.5%

Table 4-1 Top 10 vulnerabilities in web servers with disclosure dates

Source: NSFOCUS MSS

For attacks against the web frameworks and applications, the Struts2 code execution vulnerability was the most exploited accounting for 80% of this attack type:

Vulnerability Name	Release Date	Percentage
Struts2 Remote Code Execution Vulnerability (CVE-2013-1966)	2013	48.7%
Struts2 Remote Code Execution Vulnerability (CVE-2013-2251)	2013	26.9%
Struts2 Jakata Plug-in Remote Code Execution Vulnerability (CVE-2017-5638)	2017	5.9%
Struts2 ClassLoader Operation Vulnerability (CVE-2014-0094)	2014	2.9%
Struts2 Malicious Ognl Expression Leading to Remote Code Execution (CVE-2016-3081)	2016	2.7%
Struts2 REST Plug-in Remote Code Execution Vulnerability (CVE-2016-4438)	2016	2.4%

Table 4-2 Top 10 vulnerabilities in web frameworks with disclosure dates
Source: NSFOCUS MSS

In addition, the following table lists other website application vulnerabilities that were frequently exploited:

Vulnerability Name	Release Date	Percentage
ElasticSearch Sandbox Bypass Leading to Remote Code Execution Vulnerability (CVE-2015-1427)	2015	2.7%
PHPCMS2008 page size Parameter Validation Leading to Command Execution	2011	2.0%
ThinkPHP lite Mode Remote Code Execution Vulnerability	2013	1.2%
DedeCMS 5.7 SQL Injection Vulnerability	2013	0.6%
phpCMS V9.1.9 and Earlier Does Not Strictly Check the Uploaded ID Parameter, Causing the Local File Include Vulnerability	2013	0.2%
PHPCMS V9 Arbitrary File Reading Vulnerability	2012	0.1%

Table 4-3 Misc vulnerabilities in web servers with disclosure dates
Source: NSFOCUS MSS

5 DDoS Trend

5.1 DDoS Attack Count and Total Traffic

Compared to 2016 H2, NSFOCUS detected a total of 100,000 DDoS attacks with a decrease 30% for 2017. Moreover, the total attack traffic was approximately 16,000 TB with a decrease of 38.4%. NSFOCUS attributed this statistic to the decrease of reflection attacks that occurred at the beginning of 2017.

Compared to 2016 the overall attack trend in H1 2017 significantly halted but began to increase by Q2. Moreover, we witnessed an increase of 39.3% from Q1 to Q2 with an overall total traffic output of 10.3%. This is validation that historically "DDoS attacks slow down at the beginning of the year but become active in the middle of the year".

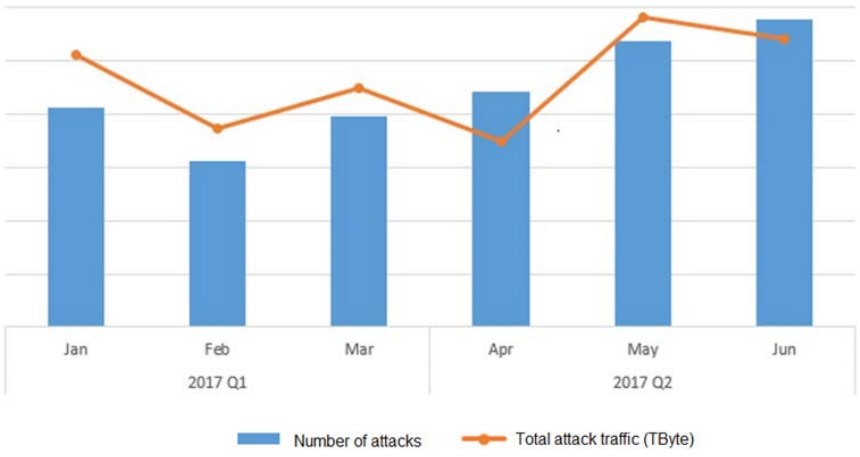


Figure 5-1 Number of attacks and traffic in each month
Source: NSFOCUS Global DDoS Attack Trend Monitoring system (ATM)

5.2 Percentages of DDoS Attacks of Various Types and Traffic

The top 3 DDoS attacks by count were all reflection attacks: NTP, SSDP, and CHARGEN reflection floods accounted for 81.7% of all total attacks. From the perspective of traffic volume, SYN and UDP flood attacks were still the attacks with the heaviest traffic accounting for 56% and 23.3% respectively. Compared to 2016 the traffic of SYN flood attacks increased significantly by 7% and UDP flood attacks declined by 6.3%.

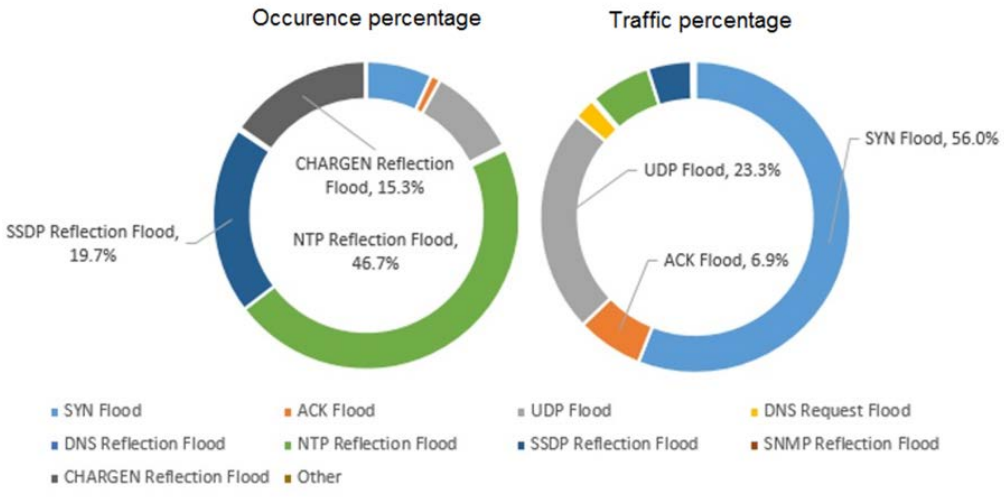


Figure 5-2 Percentages of various type of DDoS attacks by count and total traffic

Source: NSFOCUS Global DDoS Attack Trend Monitoring system (ATM)

5.3 Percentages of DDoS Attacks by Duration

Long-lasting attacks increased while short-lived attacks slightly decreased for 2017. Compared to 2016 H2, attacks ending within 30-minutes accounted for 53.5% of all DDoS attacks, down by 8.9%; those lasting for more than 3-hours are on the rise accounting for 33% with a decrease of 5.7%.

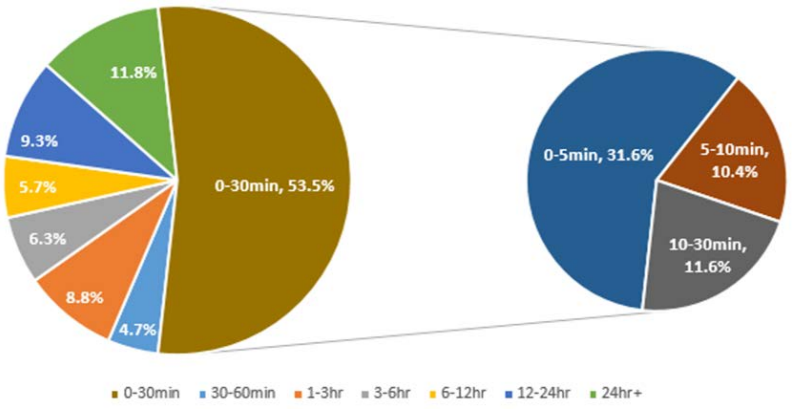


Figure 5-3 Distribution of attack durations
Source: NSFOCUS Global DDoS Attack Trend Monitoring System (ATM)

5.4 Distribution of Source Countries of DDoS Attacks

Currently China still has the most controlled DDoS attack sources contributing to a total percentage of 46.5% globally. USA and Russia came in distant second and third places in terms of attack count with 3.0% and 2.0% of attacks launched respectively.

Source Country	Percentage
China	46.6%
USA	3.0%
Russia	2.0%
Canada	1.9%
Japan	1.9%
Germany	1.8%
UK	1.7%
Netherlands	1.6%
Brazil	1.5%
South Korea	1.5%
Other	36.5%

Figure 5-4 Distribution of source countries of DDoS attacks and top 10 source countries
Source: NSFOCUS Global DDoS Attack Trend Monitoring system (ATM)

5.5 Distribution of Target Countries of DDoS Attacks

For 2017, China has been victim to the most amount of DDoS attacks at 64.6% globally. Closely following we see USA at 18.1% and Canada at 2.5%.

Source Country	Percentage
China	46.6%
USA	3.0%
Russia	2.0%
Canada	1.9%
Japan	1.9%
Germany	1.8%
UK	1.7%
Netherlands	1.6%
Brazil	1.5%
South Korea	1.5%
Other	36.5%

Figure 5-5 Top 10 DDoS Target Countries
Source: NSFOCUS Global DDoS Attack Trend Monitoring System (ATM)

6 DDoS Extortion

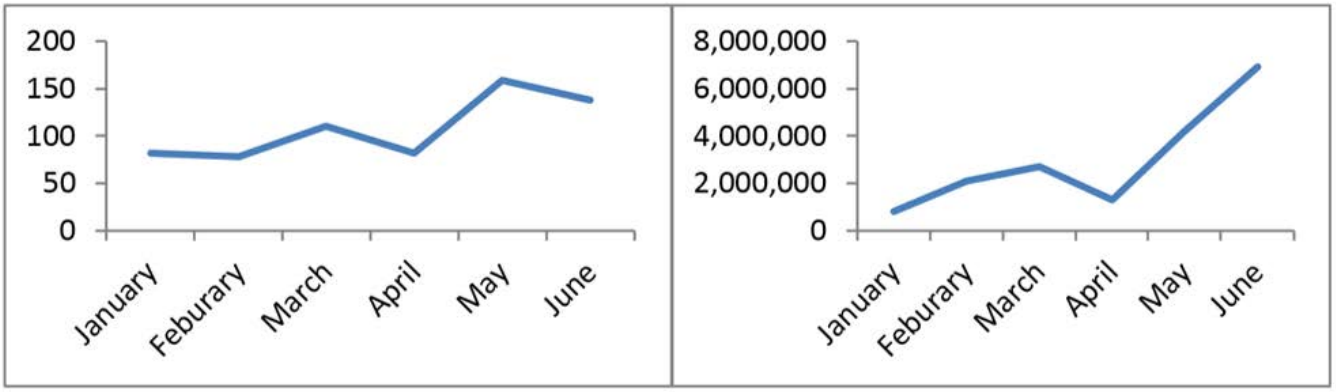
Cyber extortion has been a large contributor to overall cybercrime activity for 2017. According to the monitoring and analysis of various extortion activities NSFOCUS determined that:

- The number of ransomware attacks and capabilities has steadily increased in amount and sophistication
- Ransomware replicates and spreads automatically by exploiting system vulnerabilities
- As the ransomware industry matures such cyber threats will continue to grow in persistence
- DDoS and database extortion is frequently occurring which may become new favorite for attackers

6.1 Ransomware

From a technical perspective ransomware has been active since the inception of all major malware strains. However, it has become a cybercrime that Internet users and the security industry are most concerned about because of its capability of encrypting files, which may lead to data loss and the paralysis of mission-critical services resulting in more devastating consequences to victims.

2017 experienced major ransomware events to include WannaCry and Petya/NotPetya. There has also been an increase in the quantity of new ransomware with a total of 649 new strains as of June 30th. For the past six months new ransomware events were reported almost every week (for details, see Figure 6-2). Of the reported ransomware attacks analysis of the code determined that a large portion were upgraded or simply reassembled versions of previous ransomware while others were brand new with new techniques.



Quantities of new ransomware found in H1 2017

Topicality of ransomware in news reports in H1 2017

Figure 6-1 Quantities of new ransomware and topicality of ransomware in news reports in H1 2017
Source: NTI

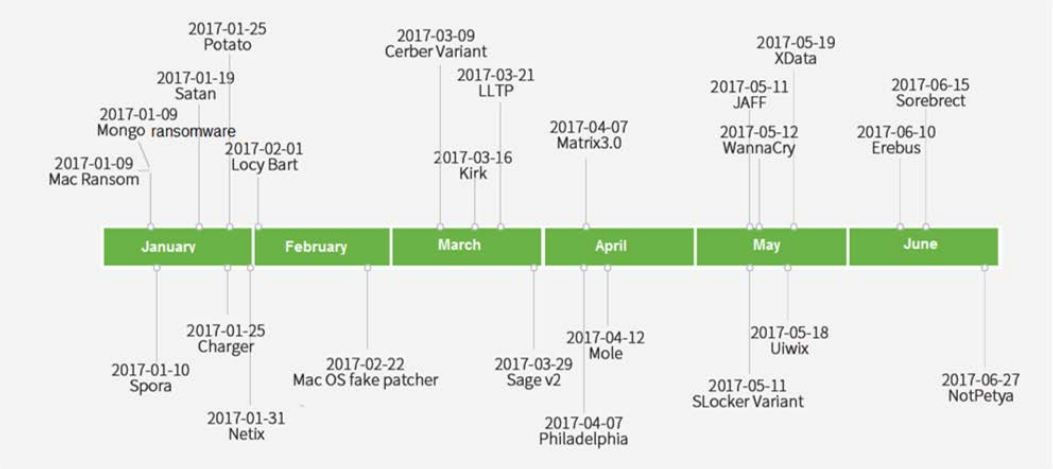


Figure 6-2 Timeline of Ransomware Reports in H1 2017
Source: NTI

Our technical analysis of ransomware in H1 2017 discovered that:

- To evade detection previously popular ransomware has been constantly upgraded to appear in networks as new variants and the emergence of open-source ransomware makes it easier to develop new ransomware types

- The compilation quality and encryption mechanism of ransomware are maturing with a significant decrease in design flaws making it less possible to decrypt encrypted files without the primary decryption key

- The reverse analysis of software reveals that some malware does not have the decrypting capability, which means that encrypted data cannot be decrypted even if victims pay the demanded ransom. Disguised as ransomware, this type of malware wipes or irreversibly destroys users' files for which the attacker asks for exorbitant prices as a ransom to intimidate victims

In terms of the delivery method, most ransomware is deployed via

- spamming or spear phishing emails that contain attachments
- inject Trojans into corrupted web pages and applications

Advanced ransomware has also emerged to exploit vulnerabilities in Microsoft Office and Adobe as well as capitalizing on local privilege escalation vulnerabilities. Such ransomware can spread by exploiting weak passwords and other remote execution vulnerabilities and therefor poses a more serious threat to organizations and individuals.

The most eye-catching pieces of ransomware are WannaCry and Petya/NotPetya, which are delivered in the form of worms that exploit vulnerabilities in Microsoft SMBv1. Additionally, TOR or onion routing, a technique for providing protected communication on the internet, has become a common method adopted by ransomware attack campaigns.

In terms of ransom targets Windows users experience the greatest amount of compromises. Although, there are also some frequently targeted Mac and Linux distributions to include Android Charger, SLocker, Lockdroid, Netix, MacRansom, Erebus, and KillDisk.

It is worth noting that a certain type of business has formed in the underground market that is referred to as Ransomware as a Service (RaaS). This service is sold by means of a temporary or permanent license and the seller makes money by asking for lump-sum payments or commissions. Some ransomware even has exhaustive advertisements that list RaaS services of different versions and varying prices with the cheapest commercial ransomware selling at only $60 USD. Many script kiddies can generate different versions of ransom programs by making some simple configurations with a generator and then spread them by using conventional methods such as sending emails, injecting Trojans, and tricking users into downloading the malware through social engineering

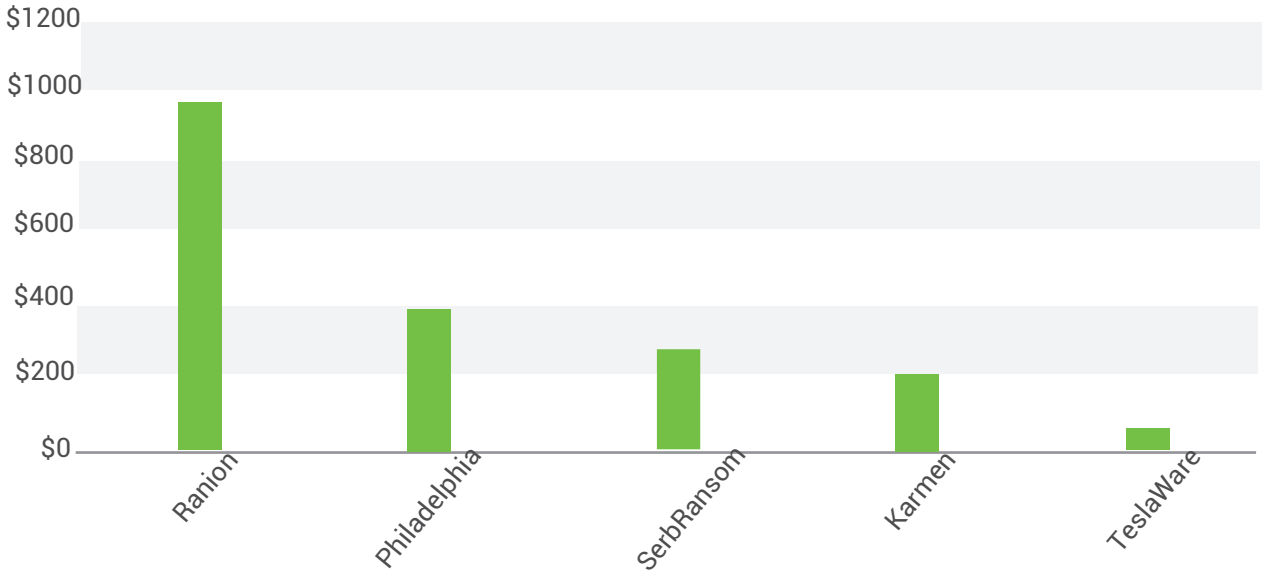


Figure 6-3 Ranking of RaaS services by unit price **Source:** BleepingComputer

The maturity of the Bitcoin industry has also contributed to the rise of ransomware and the anonymity of Bitcoin makes it the most favored means of payment for blackmailers. According to the exchange rate of Bitcoin, victims often pay thousands of US dollars for each compromised host. An advanced ransomware virus infection can force a business to pay Bitcoin ransom worth thousands or even millions of US dollars to the hacker. For the underground market this is a very profitable industry. Additionally, NSFOCUS has observed that:

- The ransom demanded by most ransomware victims ranges between $100-500 USD. However, there are some ransomware strains that demand a payment of more than $1000 USD this includes: Sage, KIRF, Jaff, and Cerber. Currently, Jaff has demanded a ransom as high as $3700 USD.

- From statistics about the enterprises stated by media sources the highest ransom paid by an enterprise in total has reached $1million USD (South Korea-based Nayana).

- RaaS services are individualized and available in offerings of different levels and prices depending on the number of files and the level of consumption at the locality of victims. The service tends to be incredibly user-friendly by providing detailed instructive steps.

- Ransomware has gained momentum and rapid growth because of its low cost, promise of fast money, and low risks. As a result, more users will be targeted by and fall victim to ransomware attacks.

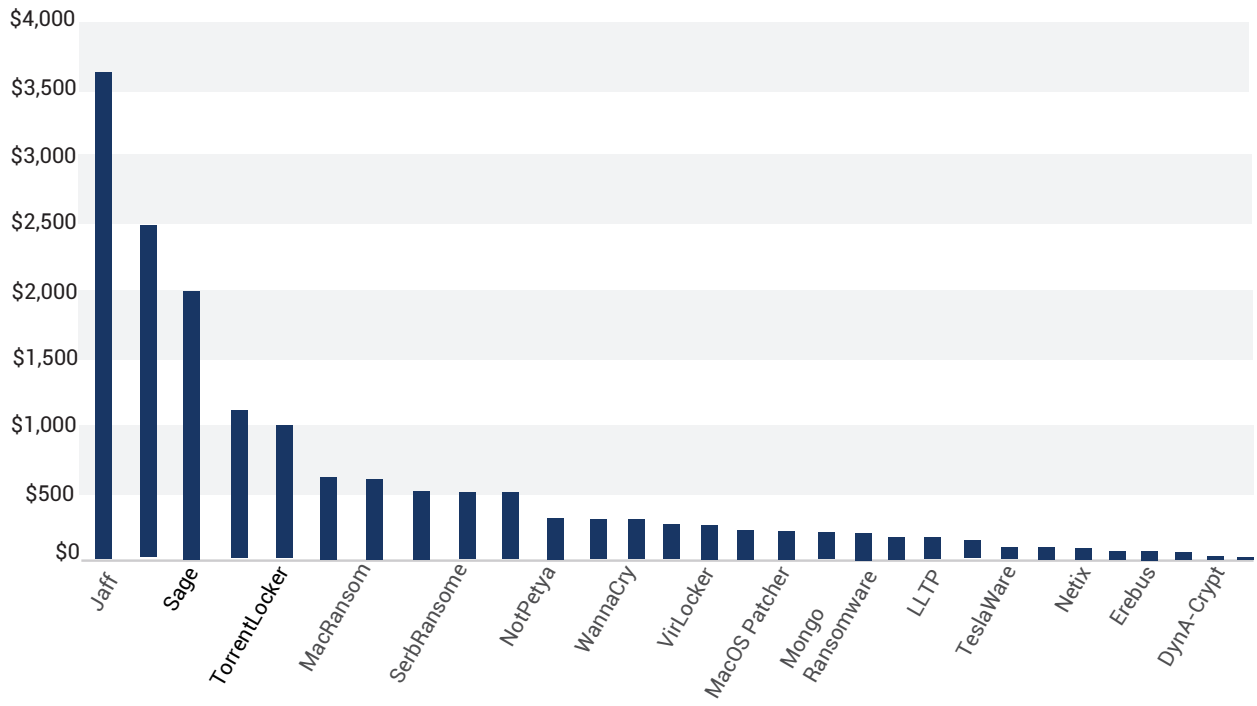


Figure 6-4 Ranking of new ransomware in H1 2017 by ransom payment

Source: BleepingComputer

6.2 DDoS for Ransom

DDoS attacks are another tactic for demanding ransoms and are often achieved by means of launching DDoS attacks against a victim's networks. Various ransomware strains are bundled with a DDoS attack capability such as 'FireCrypt'. However, it is not uncommon to also utilize botnet armies to launch DDoS attacks on the target.

Examples of recent DDoS attacks using botnet armies include but not limited to: Mirai, Imeij, Hajime, DeltaCharlie, Necurs, Amnesia, and Rakos. Thanks to the maturity of the black market for botnet based DDoS attacks and the availability of DDoS as a Service (DaaS), the business model for ransom driven DDoS attacks has gradually improved making it convenient and cost-efficient to launch such an attack. The following table lists major DDoS ransom events in H1 2017.

Date	DDoS Ransom Event
2017-01-23	Lloyds Banking Group receives an email demanding payment of 100 Bitcoins (£75,000 or $94,000) as a ransom during a DDoS attack.
2017-04-26	The XMR squad charges German companies €250 ($275) for "DDoS tests".
2017-06-26	After Nayana's paying ransom for unlocking its system, other banks receive the Armada Collective hacking group's ransom demand of $315,000 for avoiding DDoS attacks.

6.3 Database Ransom

A database ransom attack is implemented by illicitly taking control of a database to encrypt or damage data for demanding a ransom from its victims. Many databases have read-only interfaces directly exposed to the Internet and do not have complete access control policies permitting database manipulation facilitated by weak or empty password policies.

Date	Database Ransom Event
2017-01-03	A hacker by the name of Harak1r1 steals and replaces data in a MongoDB database that was not configured in strict accordance with security requirements. A demand of 0.2 Bitcoin (approximately $200) ransom. It starts as a small emergency event, but subsequently more attackers participate, including a hacking group Kraken that specializes in blackmailing victims (according to publicly available information, this group has attacked at least 21,600 databases and earned more than $7700 from ransom payments). As of January 15th available data shows that over 32,380 databases have been compromised and 21 hacking groups have been involved. It is found that 1,994,422 MongoDB databases are exposed to the Internet (for the geographical distribution, see Figure 6-5) at the time of the attack. Such a large number of devices provide a huge potential for database ransom attacks.
2017-01-13	Following MongoDB databases, ElasticSearch servers become another hacking target for which victims are required to pay 0.2 Bitcoin (approximately $200) ransom to the attacker.
2017-01-18	CouchDB and Hadoop databases successively had data wiped.
2017-01-24	A white hat hacker finds that Cassandra databases exposed to the Internet can also become attack targets.
2017-02-25	MySQL databases are held hostage for 0.2 Bitcoin ransom.

Source: NTI

Figure 6-5 Distribution of Internet-facing MongoDB databases in January 2017
Source: NTI

7 Other Major Events

The first half of 2017 witnessed a significant increase in information theft and disclosure events to include the following:

Month	Event
February 2017	A new type of Android banking Trojan 'Marcher' appears tricking users into downloading malware via phishing attacks based on SMS or MMS to gain privileges and collect account data from scores of banks. Additionally, 20 different antivirus software applications are unable to remove or un-install the malware.
March 2017	A security team outside of China finds an upgraded version of the banking Trojan Dridex, namely "Dridex V4".
April 2017	Payday Loan, a reputable company in the UK, is confirmed to suffer a data breach event and issues a security advisory to its customers.
April 2017	Kaspersky Lab discovers a new strain of ATM-targeting malware 'ATMitch'.
May 2017	The banking Trojan 'TrickBot' is used to launch a new wave of cyberattacks on private banks, private fortune management enterprises, investment banks, life insurance, and annuity management agencies in the UK, Australia, and Germany.
May 2017	A hacking gang uses the malware dubbed 'Cron' to infect over 1-million Android phones in Russia and steals over 50-million rubles (approximately $833,440 USD) from bank customers.
May 2017	O2-Telefonica in Germany has confirmed to Sddeutsche Zeitung that some of its customers have had their accounts hijacked by hacker group SS7 who exploited flaws to steal money.
June 2017	A security researcher discovers a piece of ATM-targeted malware titled 'Rufus'.
June 2017	Staff at Indian outsourcing company *Tata Consultancy Service* uploads a huge trove of financial institutions' source code and internal documents to a public GitHub repository leading to code disclosure.
June 2017	Security researchers at McAfee Labs discover a new strain of banking malware 'Pinkslipbot' (also known as QakBot or QBot) that uses a complicated multistage proxy for HTTPS-based control server communications.

Source: NTI

Conclusion

It's no surprise that cyber-attacks are still on the rise. What is changing slightly is what type of cyber-attack dominate or which ones are up and coming.

DDoS is still very popular even though there was a reduction earlier this year. Yearly trends still show DDoS attacks slow in the winter and pick up in the spring.

China still has the highest percentage of malicious IP addresses in the Top 10 countries based on GDP with the United States a close second. Yet, China is both the most attacked country and the most attacking country by GDP.

The number of vulnerabilities in applications has increased 50% over same time last year most being of medium risk. Thanks to Shadow Brokers, exploitation of vulnerabilities also saw a marked increase after the release of WannaCry/Petya/NotPetya. This also contributed to the increase in successful ransomware attacks earlier this year and the fallout from that may still have more to come.

Website application attacks remain most prevalent among exploited areas of attack with SQL injection still the most commonly exploited attack vector. Worse is the 80% of compromised assets are due to old vulnerabilities and un-patched systems. Struts2 is frequently exploited and continues to be recognized as the most vulnerable in web frameworks and applications.

And there is lots of malware and more is coming. Most common and successful distribution mechanisms for malware are spam/phishing and malicious software uploaded to vulnerable websites directed to from those sites usually due to cross-site scripting (XSS).

Organizations and individuals must stay vigilant and augment investments in cybersecurity to enhance protection against cyber threats. Cybersecurity development requires long-term efforts as attackers never cease to seek easy-to-exploit targets. Internet-facing applications and services as well as nodes with default configurations with lack of protective security measures are like defenseless cities that can easily fall prey to attackers and unknowingly become an attackers' accomplice.

High-risk vulnerabilities that are small in quantity but can cause serious damage is favored by attackers. To address this situation organizations and individuals need to assess security threats, identify and track the running status of mission-critical assets, and prioritize vulnerabilities for remediation before taking appropriate measures to gain a defensive advantage. Moreover, the application and adoption of new security information technologies and services provide convenience for attackers to launch various cyber- attacks to include the recent rise in ransomware attacks. To adapt to the evolving cybersecurity arena, organizations and individuals must raise their awareness and upgrade their capabilities in identifying, detecting, and defending against unknown and known threats.

Threat intelligence provides a valuable reference for security teams to develop effective security protection policies and courses of action that permits for reduced time of exposure to vulnerabilities and thus maximize the return on investment for defenders. In this process, NSFOCUS would like to collaborate with organizations (including regulatory authorities, security vendors, and businesses) and individuals from all walks of life to tackle cyber threats and build a secure cyberspace.