Asian Cyber Security
Vendor of the Year

Penta SECURITY
cloud · iot · enterprise

Web Application Threat Trend Report

Trends for 2017

Penta Security Systems Inc.

Contents

I. Overview

The Web Application Threat Trend (WATT) Report is an annual report compiled by Penta Security Systems. The report details attack trends and patterns analyzed by Penta Security System's Intelligent Customer Support (ICS) team after thorough analysis of customer and detection data from WAPPLES, Penta Security's Web Application Firewall (WAF), which holds the largest market share in the WAF industry for the Asia-Pacific region.[1,2] The report focuses on the analysis of web attack patterns, tracking trends to both identify new web attack patterns and predict future ones to enhance WAPPLES operations.

Each year the report is distributed to WAPPLES customers and partners, corporate and institutional security managers, research organizations, and any individuals or organizations interested in web security trends.

Readers are encouraged to use this report to get a better understanding of the current threat landscape, including trends specific to different contexts like region, time of day, industry, and more, in order to better fine-tune defenses for meeting the security needs of their unique environments. It is important to note, however, that the majority of WAPPLES appliances are located in the Asia-Pacific region, resulting in a data lean towards countries located in Asia. Hence, readers located in Asia-Pacific may find this report especially useful.

[1] All customer and detection data have been extracted with express consent.
[2] Industry Quotient, Frost & Sullivan, 2015.

II. Executive Summary

Major findings in the 2017 WATT report are as follows:

- Of the top five attacks, Cross Site Scripting (XSS) accounted for the highest proportion of attacks at 33.31%. Throughout the year, this attack maintained a stable percentage of close to 20% of detections each month. However, SQL Injection attack ratios grew continuously month to month.

- Penta Security's ICS team maintains a classification system based on specific threat factors that define particular IP addresses to be "Black IPs" or blacklisted IPs. Criteria for classification as a Black IP include attackers that launched more than 200,000 web attacks over the course of 2017, and have a threat score of 80 or above. These IPs are identified as primary attackers for the purpose of this report. Primary attackers favored attacks like Stealth Commanding (41.04%) and Directory Traversal (37.59%) over other common attacks.

- The industries surveyed and analyzed in 2017 can be segmented as follows:

  1. Broadcasting and Communications (25.96%)
  2. Public Administration (25.29%)
  3. Financial Services (17.43%)
  4. Education (16.28%)
  5. Science and Technology (4.02%)
  6. Retail and Manufacturing (3.45%)
  7. Other (7.57%)

- Attacks took place at all hours of the day, but a large portion of attacks occurred between 11:30 and 12:30, as well as 17:00 to 18:30, noting that significant increases in attacks tend to be observed during break times and hours nearing the end of a shift.

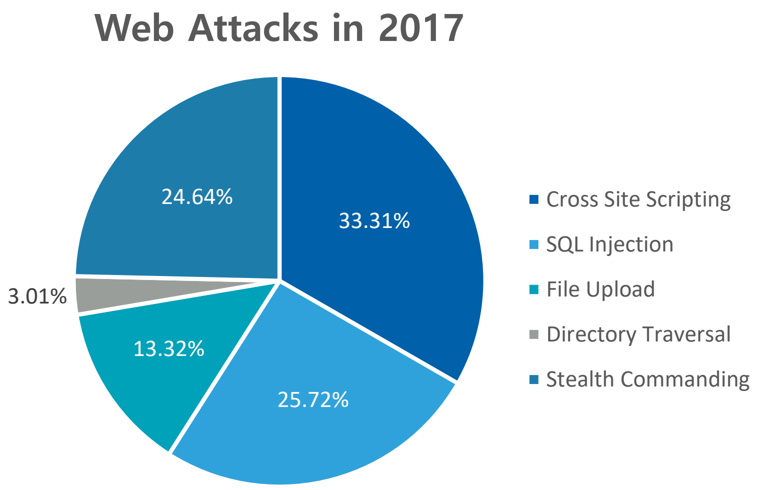
All organizations that possess valuable or sensitive information, regardless of industry, country, or other circumstances, must be able to respond to and manage both common and uncommon, large-scale threats. The objective of this report is to provide data-driven insights into web attacks attempted in 2017, and to encourage organizations to place optimizing security protocols high on their agendas.

III. 2017 Web Application Threat Trends

1. Overall Trends (1/2)

Web attacks detected over the course of the year are analyzed based on which of WAPPLES' detection rules they triggered. Looking at the distribution of attacks, general trends can be drawn about the most commonly attempted attack techniques. This analysis will guide the establishment of more effective web attack prevention and response strategies.

The following chart displays the distribution of positive detections by WAPPLES in 2017.



At 33.31%, Cross Site Scripting accounted for the highest number of attack detections, with SQL Injection (25.72%), Stealth Commanding (24.64%), File Upload (13.32%), and Directory Traversal (3.01%) following behind.

Cross Site Scripting (XSS) attacks ranked second in the 2016 roundup but took the top spot in 2017, making up nearly one-third of all attacks detected. With XSS, application servers aren't the only targets of attack, but end-users of the application as well. Giving attackers the ability to extract both administrator privileges and sensitive user information, this technique of infiltration is rising in popularity among hackers. When XSS attacks proceed undetected, direct implications can include cookie or session ID data leakage, exposure of administrative credentials, as well as malicious code download. Leveraging this information, secondary attacks can be launched to obtain classified or confidential information, be it national intelligence or corporate secrets.

Of special note, cyber attacks determined to have originated from North Korea rose significantly over the past year. Investigations confirmed an attack launch exploiting the IMG tag XSS vulnerability present in Internet giant Daum's email service on September 19, 2017.[3]

These types of XSS attacks are launched using a range of script tags. Doing so, attackers are able to extract data from web application end-users as well as execute special commands, allowing for attackers to steal credit card or bank account information, passwords, etc. Websites can also be manipulated to proliferate self-replicating worms, or if attackers are able to take control of site resources, they can severely slow down website speeds.

The following measures can help prevent XSS: 1) Update attack patterns swiftly and accurately to block bypass methods; 2) Implement whitelists or pop-up blocking to handle special characters used in scripts; 3) Block HTML entirely; 4) Implement input value restrictions or input substitutions to prevent script injections.

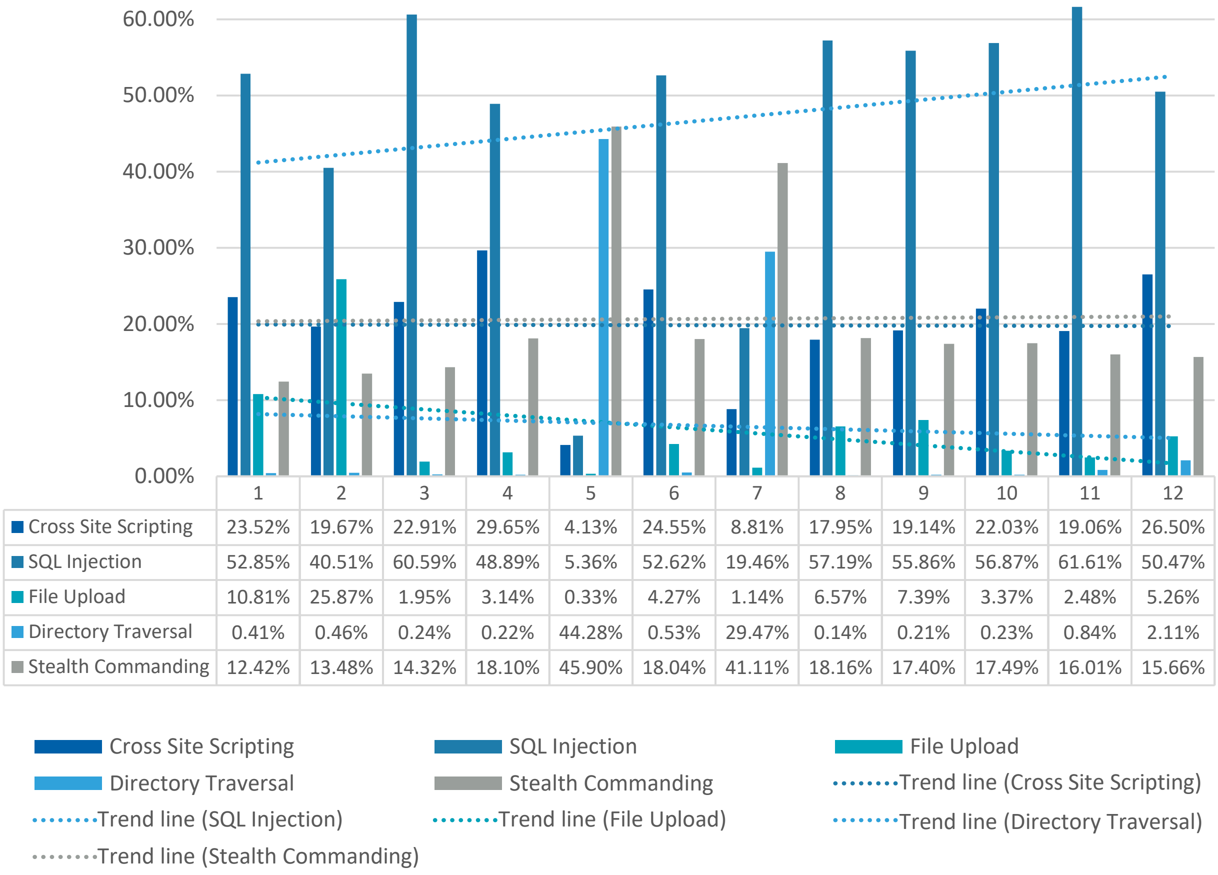
Other attack types, including SQL Injection can also cause significant harm and need to be actively prevented with appropriate security measures.

[3] Boan News, http://www.boannews.com/media/view.asp?idx=57180. September 25, 2017

III. 2017 Web Application Threat Trends

1. Overall Trends (2/2)

Breakdown of Attacks by Month



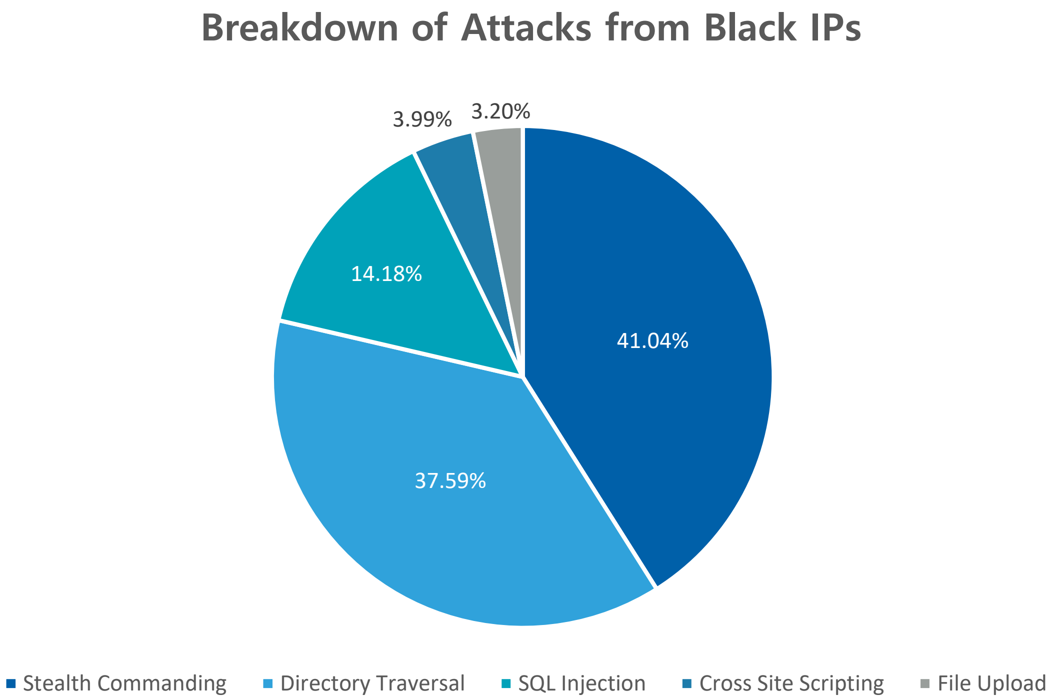
	1	2	3	4	5	6	7	8	9	10	11	12
Cross Site Scripting	23.52%	19.67%	22.91%	29.65%	4.13%	24.55%	8.81%	17.95%	19.14%	22.03%	19.06%	26.50%
SQL Injection	52.85%	40.51%	60.59%	48.89%	5.36%	52.62%	19.46%	57.19%	55.86%	56.87%	61.61%	50.47%
File Upload	10.81%	25.87%	1.95%	3.14%	0.33%	4.27%	1.14%	6.57%	7.39%	3.37%	2.48%	5.26%
Directory Traversal	0.41%	0.46%	0.24%	0.22%	44.28%	0.53%	29.47%	0.14%	0.21%	0.23%	0.84%	2.11%
Stealth Commanding	12.42%	13.48%	14.32%	18.10%	45.90%	18.04%	41.11%	18.16%	17.40%	17.49%	16.01%	15.66%

The above graph shows the monthly frequencies of the top five web attacks of 2017 and their respective trend lines.

SQL Injections showed a consistent upward trend throughout the year, while Cross Site Scripting stayed at a stable rate of close to 20% each month. From these observable differences in attack frequencies, it is evident that even though XSS has become more prominent overall in 2017, SQL Injections are also on the rise. These nuances in overall trends will help security administrators forecast which areas of security require greater investment of resources.

It is important to note, however, that there are always outliers. For example, in the months of May and July, Directory Traversal and Stealth Commanding showed sharp increases. Hackers often use different web attack techniques selectively, and may resort to less frequent attack methods to gain what they want. Directory Traversal and Stealth Commanding attacks are typically aimed at obtaining personal information and giving hackers unfettered access within the web application server. Although they may not make up a large portion of the total attacks, the consequences suggest that even uncommon attacks should not be ignored.

2. Trends in Primary Attacker Behavior



The above graph shows attacks by primary attackers (Black IPs) detected from January 1, 2017 to December 31, 2017. Primary attackers are categorized as such because of their threat score (80 or above), and their high likelihood of causing significant damage. At least 200,000 attacks have been launched from the IPs of each primary attacker over the course of the year.

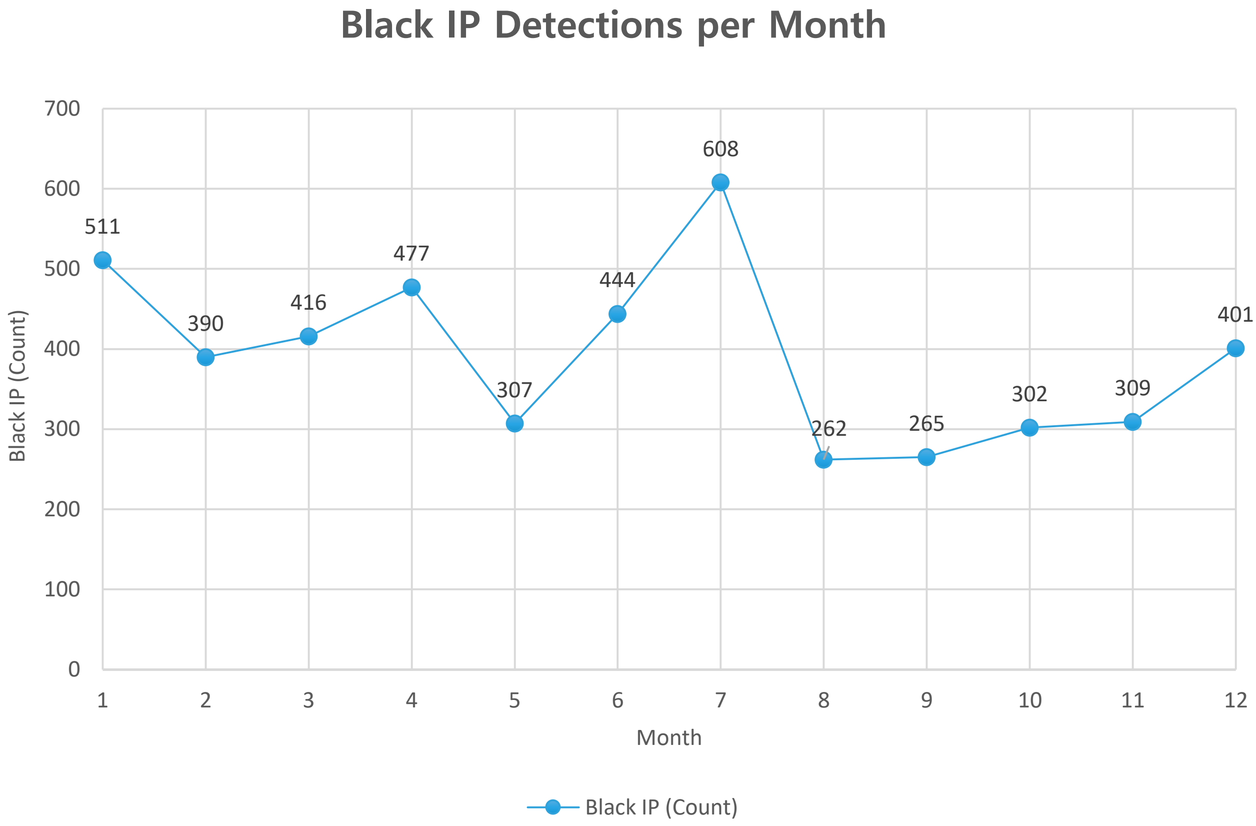
Stealth Commanding showed to be the most popular form of attack launched by primary attackers. The distribution of attacks is as follows: Stealth Commanding (41.04%), Directory Traversal (37.59%), SQL Injection (14.18%), Cross Site Scripting (3.99%), and File Upload (3.20%).

Stealth Commanding attacks often occur when a web application receives an HTTP request and forwards that information externally. If the attacker inserts malicious protocols into that information, the web application passes that protocol over to the external program as is. An attacker could then exploit these vulnerabilities to introduce Trojan horse viruses or execute malicious code. In cases of cyber terrorism, Stealth Commanding can be used for the purpose of data deletion or information hijacking.

Directory Traversal also accounted for a large portion of attacks. This attack method allows an attacker to access the standard password file through a relative path like ../../etc/passwd. Using special characters like "../" or "..₩" it is possible for attackers to navigate to other directories and files on the file system. Particularly, if the administrator's credentials get exposed, all system and server information may become accessible to the attacker. Customer information may be at risk and data breach incidents can lead to hefty losses for companies.

III. 2017 Web Application Threat Trends

3. Black IP Fluctuations



The graph above shows how the number of primary attackers detected (Black IPs) fluctuated month to month. While it may be difficult to take the number of Black IPs as a direct indicator of the number of actual hackers attempting a web attack (as a single hacker may utilize multiple IP addresses or launch repeated attacks in other months), the number of Black IPs detected each month can help gauge which part of the year saw the greatest volume of advanced attacks.

Furthermore, when the fluctuations in the data coincide with abnormalities observed in Section A's breakdown of attacks by month, further insight may be drawn about specific events or breaches that occurred in 2017, such as the fifth release of exploit tools from the NSA's Equation Group in April which included the Eternal Blue exploit.

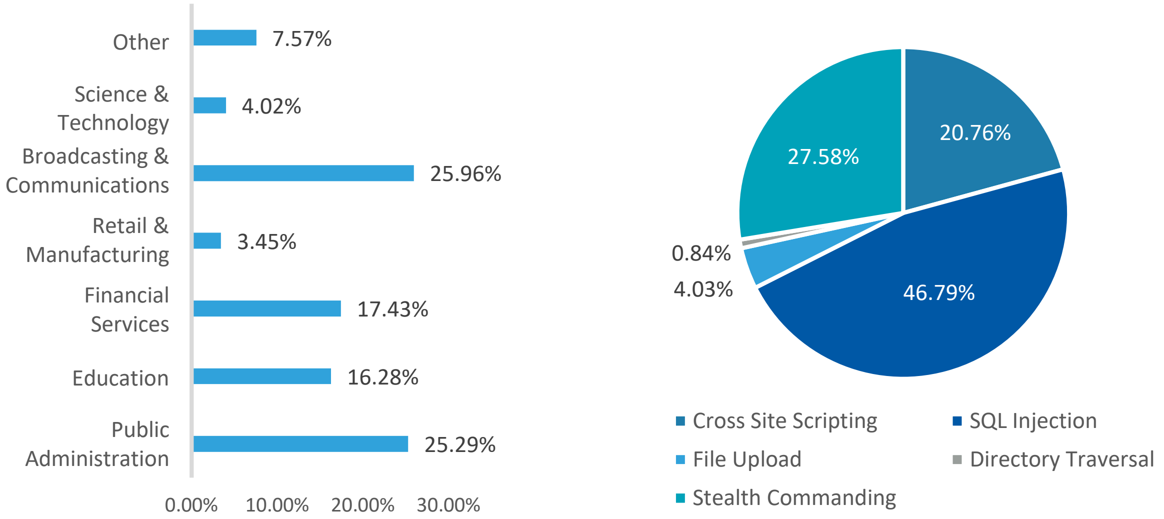
A monthly average of 391 Black IPs had been detected in 2017, with notable increases observed in January, April, June, July, and December.

These months saw a number of incidents involving 1) hacking and data leaks for cryptocurrency exchanges, 2) DDoS and SQL Injection attacks on the financial sector resulting in service interruptions, and 3) cyberactivism aimed at political figures. Certainly, there are limits to determining correlation between fluctuations in the numbers and particular events. However, it is useful to analyze Black IP numbers separately from trends in general attackers as attacks launched have more severe consequences and may be utilizing new techniques that require special caution and swift responses. Therefore security managers can benefit from keeping up with significant social or political events that are likely to coincide with spikes in Black IP activity.

III. 2017 Web Application Threat Trends

4. Industry-specific Trends

Distribution of Attacks Across Industry Targets



The chart on the left illustrates which industries are most often targeted by web attacks. The chart on the right specifies which attacks were most commonly detected on all industry-associated WAPPLES devices. Data from devices installed in industries labeled "Other" or non-industry sectors have been excluded for this second segment.

Attacks were distributed across industry targets as follows: Broadcasting and Communications (25.96%), Public Administration (25.29%), Financial Services (17.43%), Education (16.28%), Science and Technology (4.02%), and Retail and Manufacturing (3.45%). In particular, SQL Injection accounted for the highest proportion of attacks, which not surprisingly targeted industries likely to possess larger amounts of customer data, such as Broadcasting and Communications, Public Administration, Financial Services, or Education. Attackers are likely to go after the data stored in databases connected to front-facing websites of companies in those industries. Security administrators should therefore put more focused attention into protecting customer information.

A significant example of an attack targeting one of the abovementioned industries is the breach suffered by BSNL, one of India's state-owned telecommunications companies.[4] Although the attack was launched benignly by a French security researcher to bring attention to the SQL Injection vulnerability in BSNL's intranet website, this case shows that businesses in critical industries like communications are still unprepared against breach attempts. Obtaining the personal information of 47,000 BSNL employees, including those of senior officials, could potentially lead to a secondary offensive utilizing social engineering to gain more privileged access or launch phishing scams.

Another example in the Korean context is the attack on popular accommodation service app "Yeogi-Eoddae."[5] In March of 2017, details of nearly 4000 of its 3 million account holders had been leaked from the parent company WITH Innovation Corp. By exploiting vulnerabilities in the database, the hacker launched an SQL Injection attack to obtain administrator credentials. Using those credentials, the hacker then infiltrated a public-facing service management page to extract customer information. While these cases may pertain to businesses that handle large volumes of personal information, these kinds of SQL Injections may target a range of other industries as well.

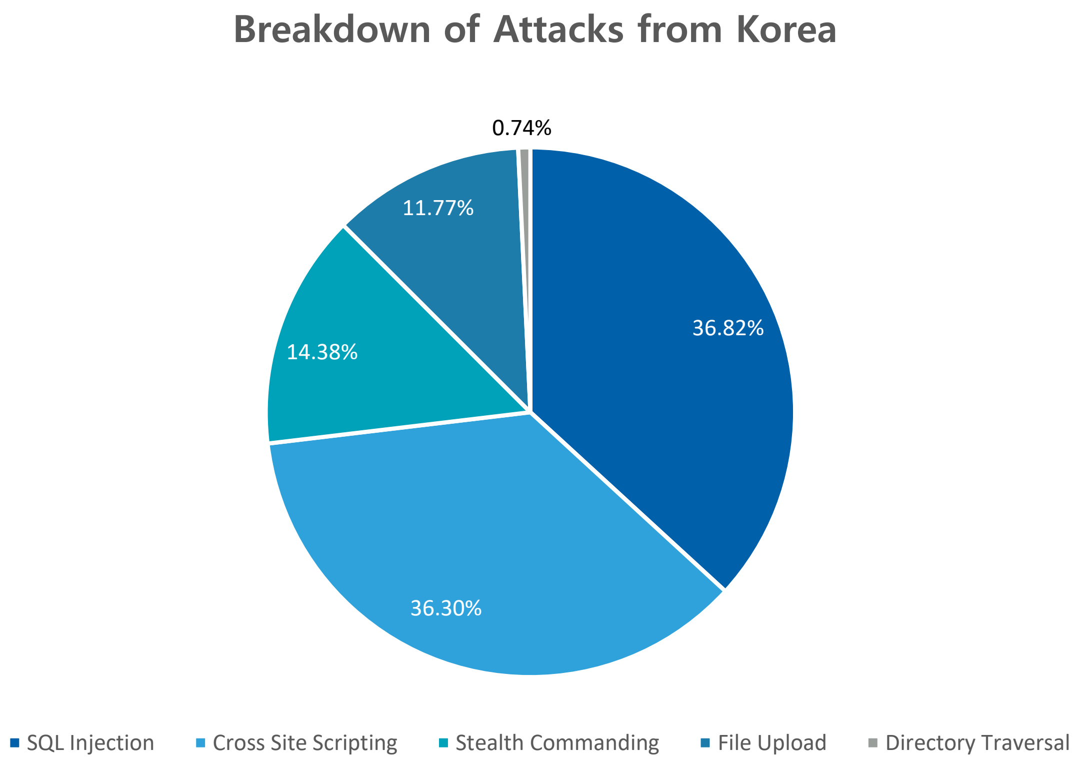
In the case of the Financial Services and Education industries, special attention should be paid to File Upload attacks. By successfully uploading malicious files, attackers can gain access to server systems or distribute malicious files to an infected website's users, attacking their PCs and other endpoint terminals. The scale of impact for such an attack is hard to contain and therefore preventing File Upload attacks should be an important consideration especially in these two industries.

[4] Computer Weekly, http://www.computerworld.in/news/security-researcher-hacks-bsnl-intranet-leaks-details-47000-employees. March 05, 2018

[5] Hankyorae, http://www.hani.co.kr/arti/economy/it/787941.html. March 24, 2017.

III. 2017 Web Application Threat Trends

5. Regional Trends (1/3)



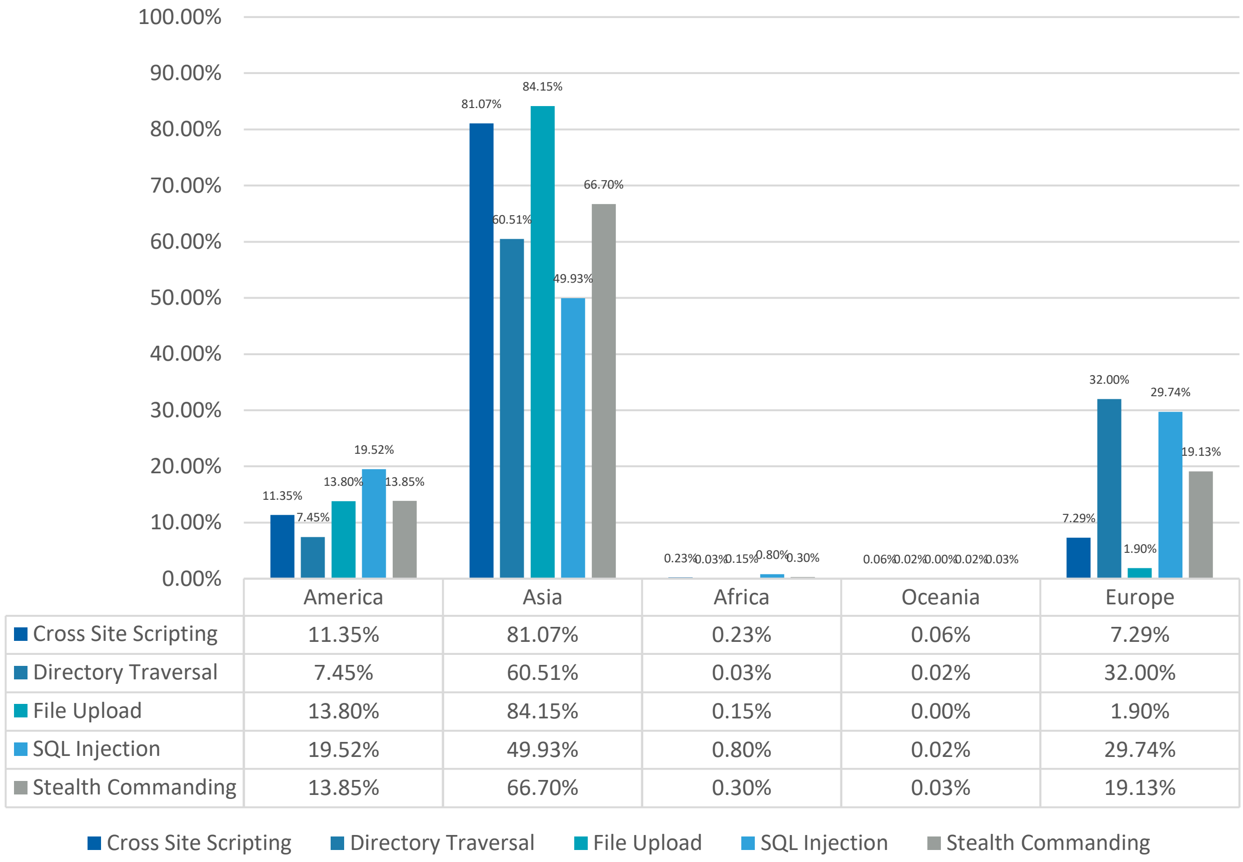
In the first part of this segment, attacks originating in Korea were analyzed separately. The chart above shows what kinds of attacks were most frequently launched from Korea in 2017. The choice of this particular segmentation was made in recognition that among the security administrators who use WAPPLES products and other readers subscribing to the WATT Report, many provide web services in Korea.

Attacks originating in Korea were segmented as follows: SQL Injection (36.82%), Cross Site Scripting (36.30%), Stealth Commanding (14.38%), File Upload (11.77%), and Directory Traversal (0.74%). The ratios were similar to the overall attack ratios of 2017 and likewise, security managers based in Korea or in companies targeting Korean consumers should pay close attention to SQL Injection and Cross Site Scripting especially since these attacks made up over 70% of all attacks. With the rising occurrence of cryptojacking incidents in 2017, wherein web browsers are hijacked to generate cryptocurrency for the hacker, the prominence of Cross Site Scripting and SQL Injection attacks used to install mining malware are likely to increase in 2018.

III. 2017 Web Application Threat Trends

5. Regional Trends (2/3)

Breakdown of Attacks by Continental Origin



	America	Asia	Africa	Oceania	Europe
■ Cross Site Scripting	11.35%	81.07%	0.23%	0.06%	7.29%
■ Directory Traversal	7.45%	60.51%	0.03%	0.02%	32.00%
■ File Upload	13.80%	84.15%	0.15%	0.00%	1.90%
■ SQL Injection	19.52%	49.93%	0.80%	0.02%	29.74%
■ Stealth Commanding	13.85%	66.70%	0.30%	0.03%	19.13%

The chart above follows the attack trends in regions according to where attacks originated. Similar to patterns seen in 2016, the highest number of attacks originated from Asia, followed by North and South America combined, Europe, Africa and Oceania. Known to be hubs for intercontinental exchanges and vibrant economic activity, Asia, Europe and the Americas are highly targeted for web attacks, especially by attacks from within the respective regions.

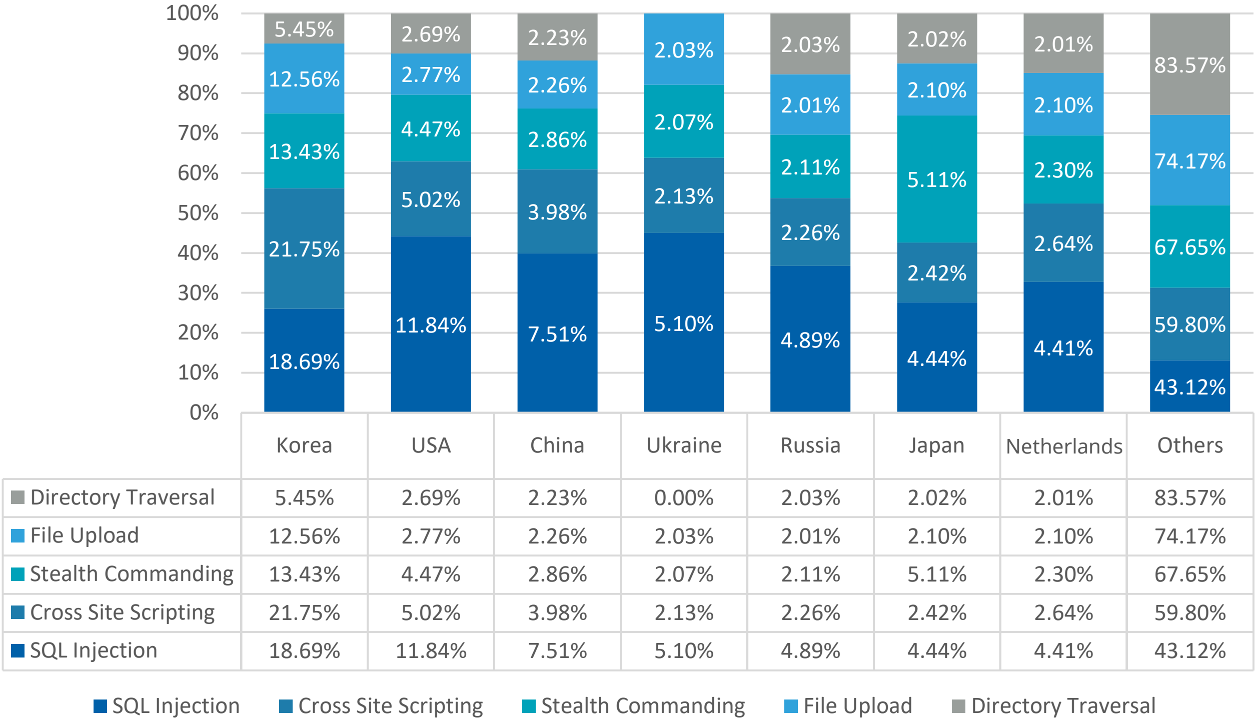
Asia was observed to be a major source of File Upload, Cross Site Scripting, and Stealth Commanding attacks. Attacks originating from Europe tended to be either Directory Traversal, SQL Injection, or Stealth Commanding attacks. Attacks from the Americas, on the other hand, were primarily SQL Injections.

With insight into continental attack trends, targeted adjustments can be made to strengthen security policies. In particular, special attention should be paid to handling SQL Injection and Cross Site Scripting attacks which have remained dominant throughout past reports as well.

III. 2017 Web Application Threat Trends

5. Regional Trends (3/3)

Breakdown of Attacks by Country of Origin



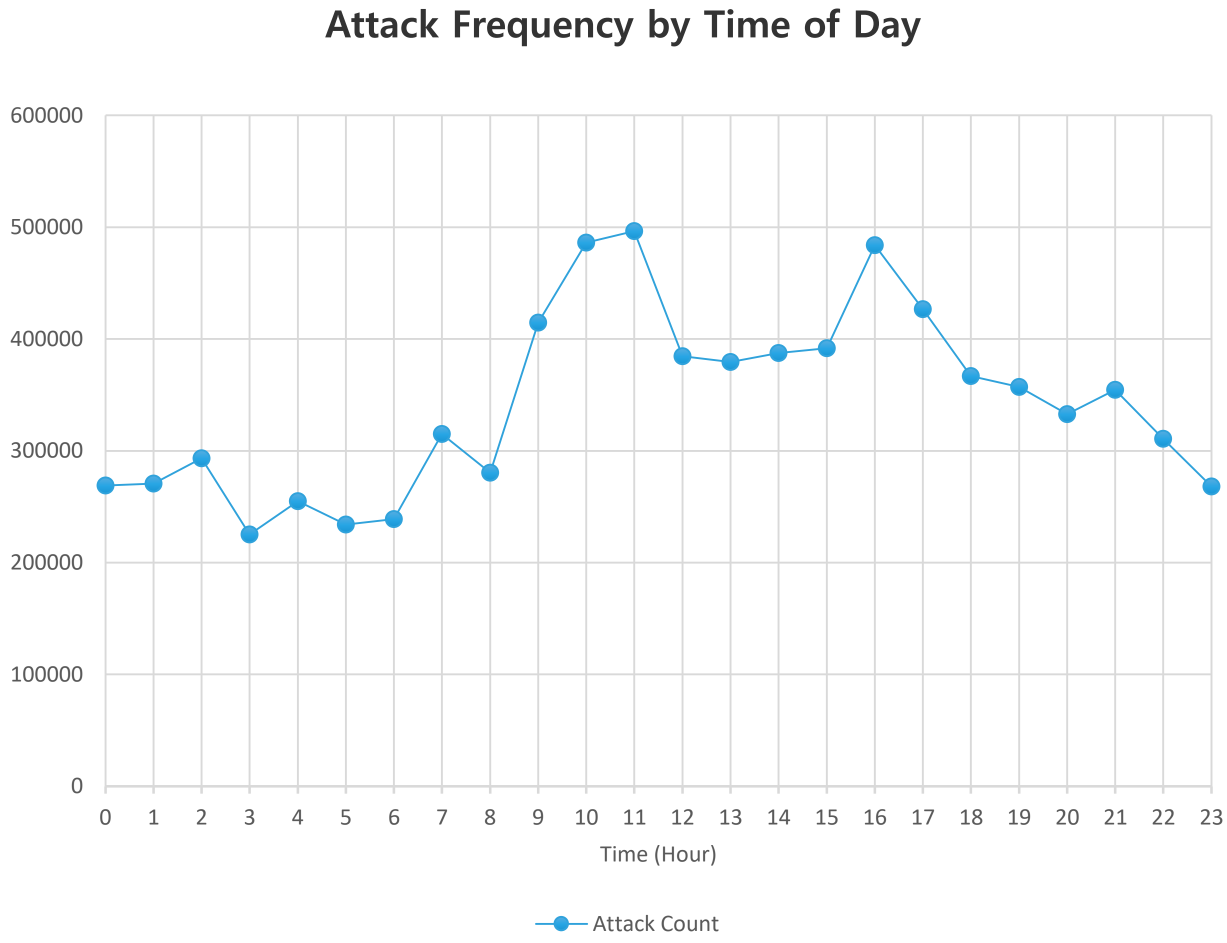
	Korea	USA	China	Ukraine	Russia	Japan	Netherlands	Others
■ Directory Traversal	5.45%	2.69%	2.23%	0.00%	2.03%	2.02%	2.01%	83.57%
■ File Upload	12.56%	2.77%	2.26%	2.03%	2.01%	2.10%	2.10%	74.17%
■ Stealth Commanding	13.43%	4.47%	2.86%	2.07%	2.11%	5.11%	2.30%	67.65%
■ Cross Site Scripting	21.75%	5.02%	3.98%	2.13%	2.26%	2.42%	2.64%	59.80%
■ SQL Injection	18.69%	11.84%	7.51%	5.10%	4.89%	4.44%	4.41%	43.12%

Seven countries have been identified to contribute the highest percentage of attacks. The chart above shows the distribution of attack types within these countries.

Ukraine and the Netherlands gained prominence over the past year as new entrants into this list of top attack origins. On the other hand, USA, China, Russia and Japan remained in the top spots they occupied in the 2016 report. While there may be some shifts in rankings, overall the top few origin countries identified above remain the source of continuous web attacks.

A relatively high percentage of attacks in each country were made up of SQL Injection and Cross Site Scripting attacks, although Japan had a significant percentage of Stealth Commanding attacks. As expected, nations like the USA, China and Russia occupied top spots, most likely because of their powerful political and economic status. Therefore defense against web attacks from these countries need to be stepped up.

6. Trends Across Time of Day



The graph above shows the sum of attacks detected according to time of day (local time). Segmented by one-hour intervals, the distribution of web attack occurrences throughout an average day can be analyzed to find out the most targeted time of day.

Evidently, more than 200,000 attacks took place at all hours of day and therefore continuous protection is needed. In particular, special attention should be paid during the typical lunch and dinner times of 11:00 to 12:30 and 17:00 to 18:30, as well as after usual work hours. At these times, quickly undertaking web security countermeasures can be especially difficult as shifts may be in the process of changing.

Security might already be an imperative in certain organizations that are able to deploy resources for continuous monitoring 24 hours a day. However, there may still be multiple opportunities for attackers to attack, such as during mealtimes, shift changes, or when security protections are paused temporarily to conduct system inspections.

The data shows that it is important to continuously monitor for web attacks and prepare an emergency manual for responding to any attacks that may occur. Conducting regular training for security administrators to familiarize them with the emergency manual will also help to build response capabilities against web threats. To this end, analyzing detection data as done in this report will provide the basis for shaping response strategies adapted to current web attack trends.

IV. APPENDIX

1. Methods of Analysis

1) Data Collection Method and Duration

The data from this report is based on log analyses from WAPPLES taken from January 1, 2017 through December 31, 2017. All customer and detection data have been extracted with express consent.

2) Key Differences from Previous Reports

Like the ICS Reports published up to 2015 and the 2016 WATT Report, this report is based on true-positive logs of WAPPLES' detection rules collected on the ICS server. The report is compiled each year in order to extend information to all interested parties including customers who use WAPPLES, security administrators of various companies and organizations, national and private research institutions, as well as university laboratories interested in web security trends. Penta Security Systems publishes the WATT Report annually, detailing observed trends so they may be used as a comparative reference for annual data trends. The 2017 report included a larger proportion of data from the Asia-Pacific region, resulting in an amplification of detections from the Asian continent. Readers are advised to note this change.

3) Glossary

The technical terms presented below are vulnerabilities and attack techniques that can lead to information leakage and/or service failure.

- **Cross Site Scripting (XSS)**

Overview : An attack technique involving the insertion of malicious scripts into forum posts or emails to cause other users to perform some involuntary action. For example, if a hacker posts a message that includes code which will behave maliciously in the server, the moment a user views the message, the code will be automatically executed to extract user information for the hacker.

Expected consequence : Cookie hijacking, session hijacking, abnormal function through malicious script.

- **SQL Injection**

Overview : An injection technique capable of compromising databases by allowing an attacker to manipulate client input values or variables in poorly secured web pages to execute unauthorized SQL queries. Besides being one of the most common forms of attack, SQL Injection attacks can also cause massive data leaks.

Expected consequence : Unauthorized data access, manipulation, or tampering, compromised system authority, data leakage.

- **File Upload**

Overview : An attack that involves a hacker uploading a malicious file to the web server using the file upload function of the web application or website. After which, the hacker will be able to connect to the website and remotely execute system operating commands from the server computer's system.

Expected consequence : Uploading and executing a web-shell to run commands, browsing system files and local resources without authorization, attacking other servers, file renaming/copying/deletion/creation.

IV. APPENDIX

▪ Directory Traversal

Overview : An attack technique that involves unauthorized filename manipulation to move up directory hierarchies for the purpose of accessing directory files and data that system administrators intended to keep hidden.

Expected consequence : Access to system files and leakage of source files located in parent folders.

▪ Stealth Commanding

Overview : An attack technique that obtains information by attaching a server side script to an input to execute malicious commands. The system executes the attack by injecting a command into the parameter and turning them into protocols.

Expected consequence : Abnormal behavior of the server, data leakage.

4) Black IP List

Ranking	IP Address	Country	Threat Score
1	62.210.X.X	France	97.32
2	195.154.X.X	France	96.68
3	149.56.X.X	United States	95.75
4	112.216.X.X	Korea	95.69
5	5.10.X.X	Netherlands	95.09
6	107.150.X.X	United States	94.59
7	14.63.X.X	Korea	92.42
8	91.200.X.X	Ukraine	90.80
9	39.118.X.X	Korea	89.88
10	72.246.X.X	United States	89.37
11	221.234.X.X	China	88.85
12	50.63.X.X	United States	88.72
13	177.185.X.X	Brazil	88.38
14	177.12.X.X	Brazil	88.01
15	72.246.X.X	United States	87.75
16	209.17.X.X	United States	87.65
17	91.223.X.X	Ukraine	87.53
18	184.168.X.X	United States	87.21
19	91.151.X.X	United Kingdom	87.07
20	43.248.X.X	Hong Kong	86.91
21	98.19.X.X	United States	86.78
22	211.252.X.X	Korea	86.35
23	64.87.X.X	United States	86.29
24	110.4.X.X	Malaysia	86.16
25	52.78.X.X	United States	85.80
26	88.202.X.X	United Kingdom	85.69
27	61.111.X.X	Korea	84.93
28	152.99.X.X	Korea	84.68
29	61.111.X.X	Korea	84.16
30	210.102.X.X	Korea	84.00
31	205.144.X.X	United States	83.78
32	72.246.X.X	United States	83.67
33	212.247.X.X	Sweden	82.98
34	119.203.X.X	Korea	82.95
35	121.127.X.X	Hong Kong	82.84
36	211.39.X.X	Korea	81.91
37	211.252.X.X	Korea	81.69
38	61.111.X.X	Korea	81.19
39	210.102.X.X	Korea	80.98
40	61.111.X.X	Korea	80.75

Asian Cyber Security
Vendor of the Year

thank you

Penta SECURITY

KOREA	Yeouido, Seoul	www.pentasecurity.co.kr (HQ)
U.S.A	Houston, Texas	www.pentasecurity.com
JAPAN	Shinjuku-Ku, Tokyo	www.pentasecurity.co.jp