WATT
Report

Web Application Threat Trends Report

Trends for the First Half of 2020

Penta Security Systems Inc.
Cloudbric Pte. Ltd.

Penta SECURITY cloudbric

Penta SECURITY cloudbric

Contents

I. Overview

1. Objective of Report

This Web Application Threat Trend Report (WATT Report) is complied with the detection log data from Penta Security's WAPPLES, the web application firewall with No. 1 market share in the Asia Pacific[1], along with the detection log data from Cloudbric, a cloud-based web application firewall. Both WAFs are widely deployed worldwide. This report only contains data that customers have agreed to share, all of which are collected by Penta Security's Intelligent Customer Support (ICS) system and Cloudbric.

The main purpose of this report is to identify web attack patterns through the latest attack trend analysis and reflect the predicted results to WAPPLES/Cloudbric operations. Compared to previous reports, the 2020 H1 WATT Report has two major changes: 1) instead of using data from WAPPLES alone, the report contains data received from both WAPPLES and Cloudbric; and 2) the trend analysis is conducted with Penta Security's self-developed machine learning technology. These changes are expected to improve the accuracy of predictions for future web attacks.

This report is written and distributed for the purpose of providing information on web attack trends to all readers interested in web security trends, including WAPPLES/Cloudbric customers, partners, security managers of companies and institutions, and researchers at academic institutions.

Through this report, readers are provided with various statistical information on major web attacks based on the detection rules of WAPPLES/Cloudbric, trend information on attack types and malicious IPs of major attackers, statistical information on regions where major web attacks originate, and web attack trends by industry and timeframe.

1) Industry Quotient, Frost & Sullivan, 2015.

II. Executive Summary

This report analyzes attack data based on the top 5 rules that are deemed most important amongst all detection rules of WAPPLES and Cloudbric. The analysis is conducted with regards to attack types by industry and country of origin.

1. Web Attack Trend by Rule

Top 5 web attacks detected by WAPPLES and Cloudbric were as follows: Extension Filtering (23.72%), Request Header Filtering (16.73%), SQL Injection (15.21%), Error Handling (7.46%), and URL Access Control (5.71%). Notably, compared to 2018, a new type of attack has emerged, and extension filtering attacks and SQL injection attacks appeared repeatedly every year. Therefore, it is necessary to prepare countermeasures against various web attack, while at the same time, prepare security measures with continuous interest in Top 5 web attacks.

2. OWASP Top 10 Attack Trend by Attack Type

We compared the rules of WAPPLES/Cloudbric and the top 10 web attack types selected by OWASP based on the detection log data from January 1st to June 30th, 2020. The most detected attacks were Injection type, followed by Broken Authentication attack type and Sensitive Data Exposure attack type. This shows that web applications are used more frequently and contain sensitive information (personal, financial, healthcare information, etc.). Therefore, companies must take security measures such as encryption to protect personal information.

3. Web Attack Trend by Objective

We classified and analyzed the attack rules of WAPPLES and Cloudbric by attack objectives. The highest proportion was attacks aimed at information leakage (51.91%), followed by vulnerability scanning. As the frequency of personal information attacks is high, users should constantly monitor carefully to prevent any sort of attacks. In addition, countermeasures such as attempts to further strengthen security measures should be prepared.

4. Major Attacker Trends

We selected the Top 10 major attackers based on the number of web attacks from January 1st to June 30th, 2020. It is worth noting that the rate of web attack trends of major attackers and total web attack trends were shown differently. Major attacker trend is as follows: Directory Traversal (44.74%), SQL Injection (21.86%), Directory Listening (16.05%), Invalid URL (14.10%), and File Inclusion (2.35%) which shows that even if the percentage of web attack trend by rule is lower, or even if does not range within the Top 5 web attacks, it can still cause severe damages.

5. Industrial Trend

We have categorized and presented web attacks that were scouted out by industry sectors. The analysis was conducted by industry, and web attacks were detected in the order of distribution and manufacturing, broadcasting and communication, education, public sectors, and shopping malls. Attacks have occurred mainly in industries that have in-house employees, and a lot of customer information, attacked by major attacks including Cross Site Scripting and SQL Injection.

6. Regional Trend

The ratio of attacks by rule originating from Korea was as follows: Extension Filtering (42.34%), URL Access Control (13.35%), Error Handling (9.44%), Privacy Output Filtering (8.12%), and Request Header Filtering (5.68%). Additionally, by continent, many web attacks occurred in the order of Asia (including South Korea), Europe, America, Africa, and Oceania based on the number of web attacks. In particular, Request Header Filtering attack was the most frequent attack that occurred in Asia, Europe and the Americas.

7. Variation Trend in No. of Malicious IPs

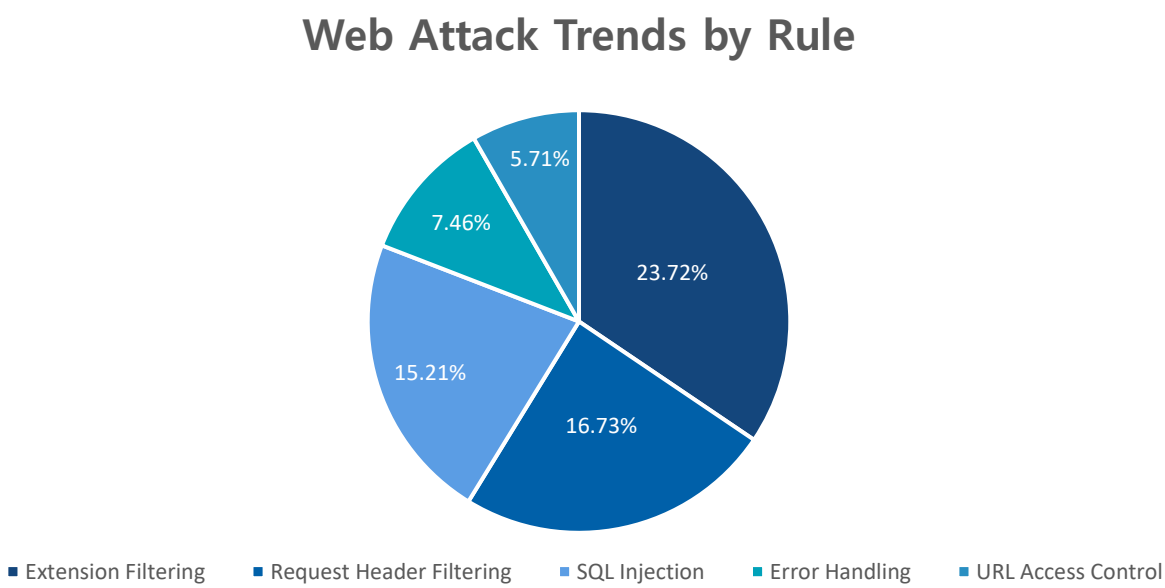
From January 1, 2020 to June 30, attackers with more than 3,000 attack attempts per month were analyzed and designated as Malicious IPs. In particular, April, May, and June were the months with the highest number of Malicious IPs, which were found out to be related to COVID-19 (coronavirus).

III. Trends in Web Attacks for the First Half of 2020

1. Web Attack Trend by Rule

The web attack trend by rule analysis shows which attacks were common throughout the first half of 2020. Based on this, basic web attack response guidelines can be established for security countermeasures against web attacks.

The graph below is an analysis of web attacks through WAPPLES and Cloudbric detection rules in the first half of 2020.



Extension Filtering (23.72%) accounted for the highest number of attack detentions, with Request Header Filtering (16.73%), SQL Injection (15.21%), Error Handling (7.46%) and URL Access Control (5.71%) following behind.

Extension Filtering attack is one of the most frequent web attacks every year, but it had the highest attack frequency in the first half of 2020. Extension Filtering refers to access attempts to configuration files (dll, conf, ini, etc.) rather than the ones in extension formats commonly used by websites. This is a very dangerous attack as it can directly have impact on web server behaviors and web services once exposed to other users.

Request Header Filtering attack is an attack using HTTP Request request sent from a web browser. Unlike normal HTTP Request request, a hacker removes essential elements from the header of the request or writes other elements to make abnormal requests. Such attack can cause secondary damages as the information of the web server could be altered or the web server could be damaged.

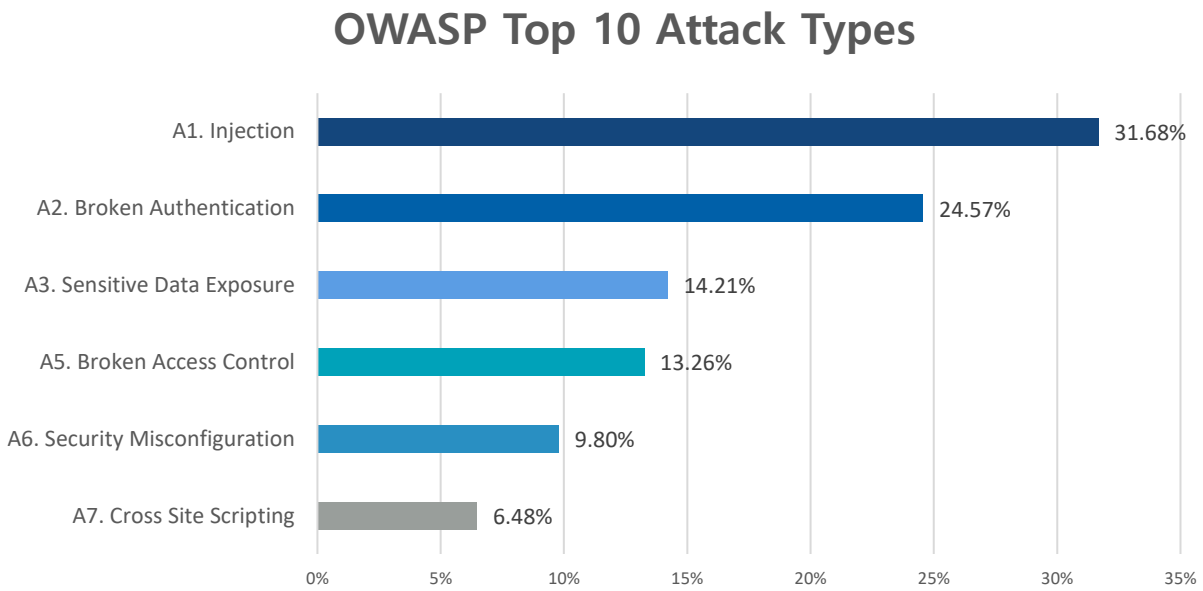
SQL Injection attack is an injection attack technique, which attacks the database by executing SQL statements that are not allowed or unrelated. Although it is one of the most common attacks, it requires a lot of attention because it can end up causing a severe information leakage. As various SQL injection attack methods are already discovered and well-known, it is critical to be prepared for SQL injection attacks.

Attacks such as Error Handling and URL Access Control are also well known which can cause severe damages, so it is critical to establish security measures in advance.

III. Trends in Web Attacks for the First Half of 2020

2. OWASP Top 10 Attack Trend by Attack Type

The graph below classifies the detection cases of WAPPLES and Cloudbric in the first half of 2020, by the attacks that ranked in the OWASP top 10 attack types.



The graph above shows the frequency of attack types that matched the WAPPLES rule detection information with the 10 OWASP vulnerabilities. Injection attacks occurred the most followed by broken authentication and sensitive data exposure.

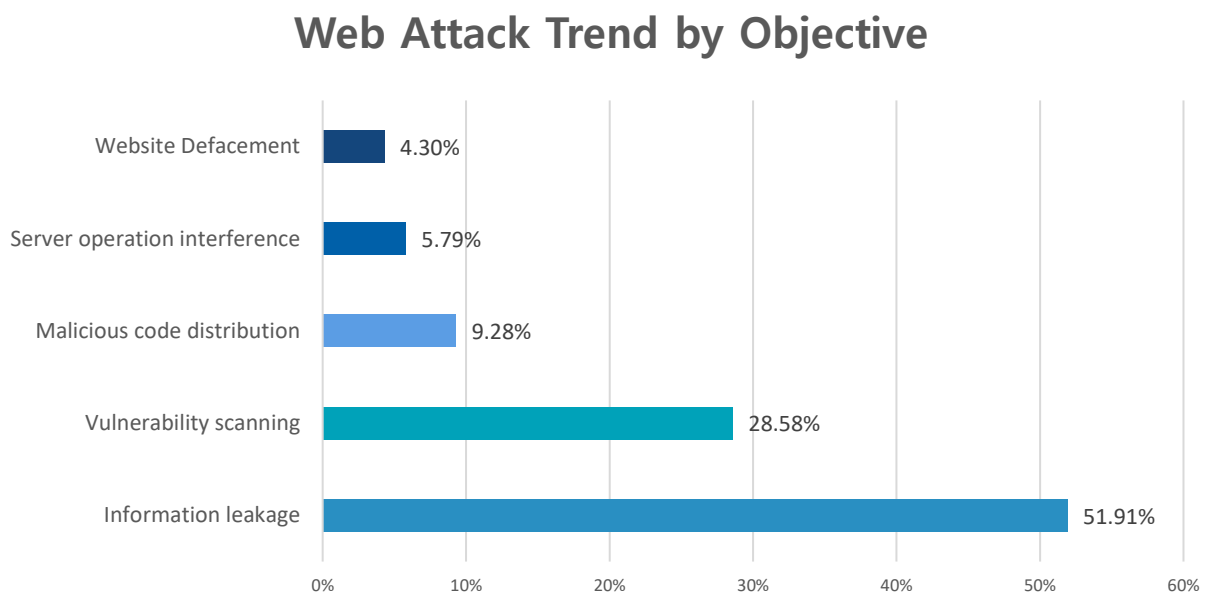
In particular, the Sensitive Data Exposure attack was ranked 6th in the OWASP Top 10 Attacks in 2013, however, it had ranked 3rd place in 2017 with much higher risks. In other words, web applications and APIs (finance, health, personal information, authentication information, etc.) have been deployed with insufficient protection for sensitive data over the time and it shows how corporates must take security measures to protect data via encryption.

OWASP Top 10 Attack Types	No. of Detections
A1. injection	17,022,983
A2. Broken Authentication	13,204,227
A3. Sensitive Data Exposure	7,632,723
A5. Broken Access Control	7,123,249
A6. Security Misconfiguration	5,265,267
A7. Cross Site Scripting	3,484,083

< Top 10 Web Attack Trend based on OWASP >

III. Trends in Web Attacks for the First Half of 2020

3. Web Attack Trend by Objective



The graph above is an analysis of web attack detection data for the first half of 2020, classified by objectives. The percentage of attacks originating from South Korea was in the order of information leakage (51.91%), vulnerability scanning (28.58%), malicious code distribution (9.28%), server operation interference (5.79%), and website defacement (4.30%).

More than about 50% of the attacks were aimed at information leakage, unauthorized modification and manipulation of the website by unauthorized users such as website defacement that causes unauthorized alteration of a designated web page. Additionally for SQL Injection that steals or manipulates user information by adding malicious code to the SQL server. There is also File Upload which uploads .exe, .jsp, .php, etc. that can be executed on the web server and Include Injection technique that injects dangerous scripts, files, and malicious codes.

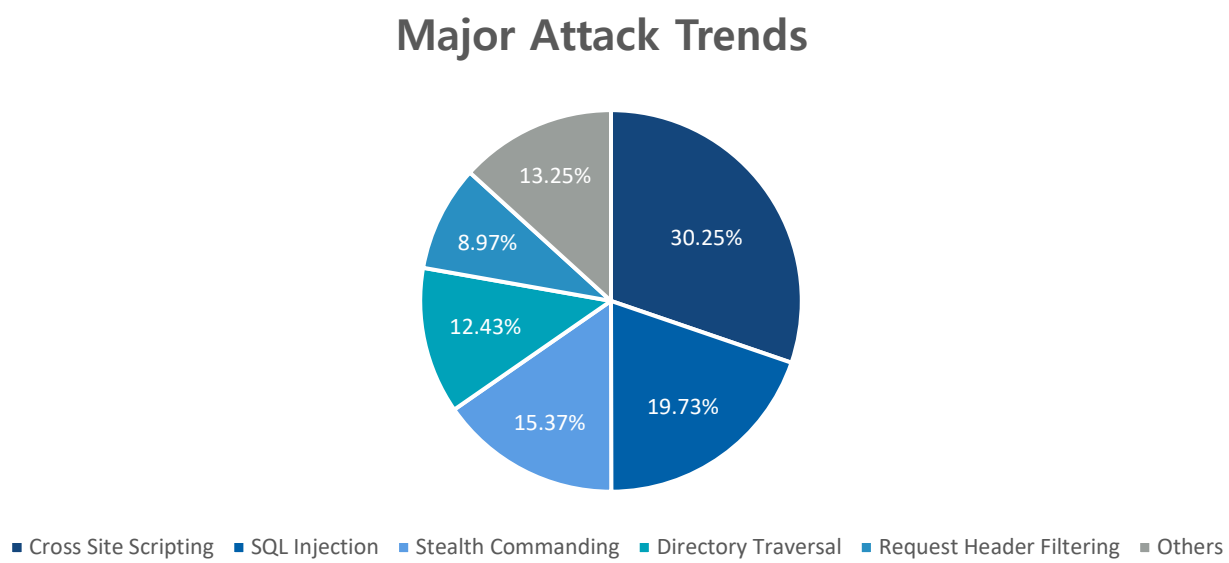
The second most common objective is vulnerability scanning (28.58%). It uses an automated tool to make a request or response out of the standard of HTTP (Invalid HTTP), request a URI outside the format defined in RFC (Invalid URL), or expose directory contents of a website), error handling, etc. to determine which vulnerabilities exist on the website. Attacks are also attempted based on prior information obtained from these actions.

The third is aimed at malicious code distribution. It identifies the weaknesses of the server and distributes malicious codes such as Trojan and various viruses. Hackers use a method of displaying user information by entering malicious script code (Cross Site Scripting) to execute malicious commands and obtain information (Stealth Commanding), or through an abnormal approach (Suspicious Access) by attacking the server through sending malicious codes.

In addition, attacks aimed at server operation interference and website defacement have also occurred. Most common attacks were related to information leakage, which explains why users and corporates need precise attention and strengthened security measures.

III. Trends in Web Attacks for the First Half of 2020

4. Major Attacker Trends



The table above is the result of selecting the top 10 web attackers from January 1 to June 30, 2020 and analyzing their web attack trend. It is important to keep an eye on their web attack trend as their attack patterns are likely to cause real damage in the future.

Web attacks used by major attackers based on the 2020 web attack trend analysis were Cross Site Scripting (30%), SQL Injection (19.73), Stealth Commanding (15.37%), Directory Traversal (12.43%), and Request Header Filtering (8.97%).

Cross Site Script (XSS) and SQL Injection attacks are common attack techniques. In particular, XSS attacks are presumed to have risen due to an attempt to steal not only the web application server but also the user and system administrator privileges and credential information all at once. When XSS attacks are performed, primary damage such as stealing cookie/session ID information, system administrator privileges, and downloading malicious codes can lead to serious secondary damages such as severe corporate/state confidential information leakage.

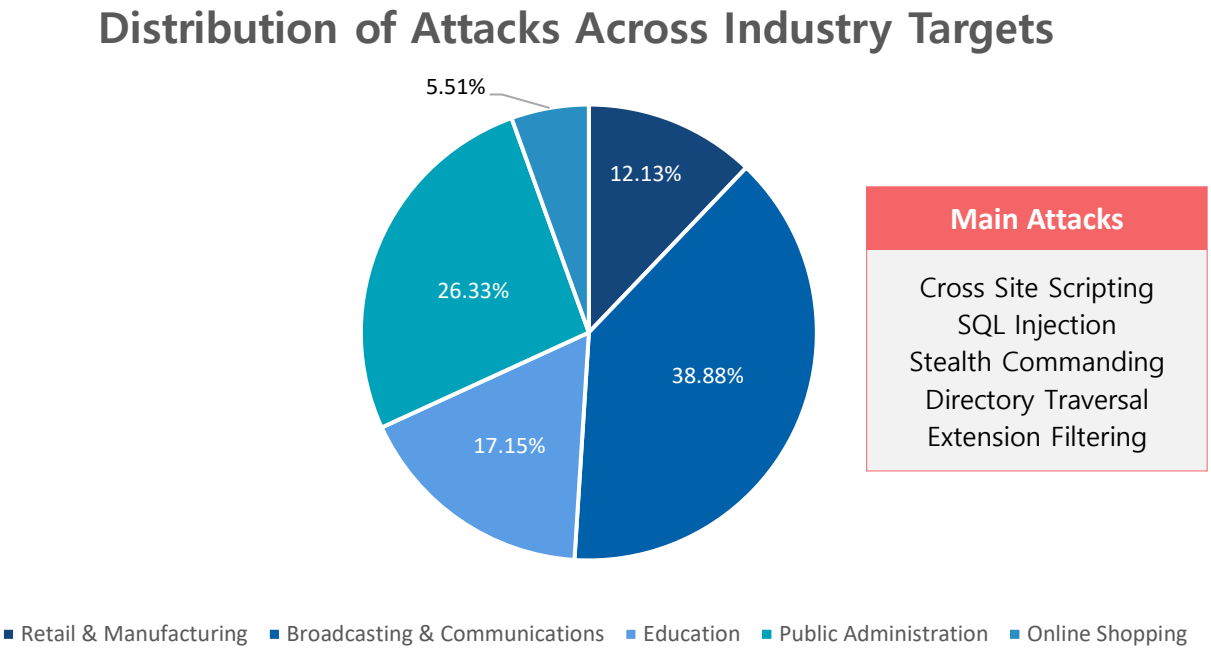
Stealth Commanding, the second most common attack technique, occurs mainly when a web application receives an HTTP request and passes that information to the outside. When an attacker injects malicious commands into a part of the information, the web application passes this information to an external program for execution. An attacker could use these vulnerabilities to plant a Trojan horse virus or execute malicious code. This is a dangerous attack that can lead to cyber terrorism such as data deletion and information theft.

Lastly, there are Directory Traversal attacks and Request Header Filtering attacks that access and verify/execute Directory or File, and both attacks are dangerous attacks that can lead to personal information leakage.

The main objective for these attacks is that it takes advantages of the vulnerabilities to steal information or to attack the web for the purpose of taking over the server. It is strongly recommended to prepare a guideline to prevent these attacks.

III. Trends in Web Attacks for the First Half of 2020

5. Industry Trend



The graph above shows the percentage of web attacks by industry as detected by WAPPLES and Cloudbric. In addition to the "Web Attack Trends by Rule", this analysis provides further insights for each specific industry on how to stay prepared.

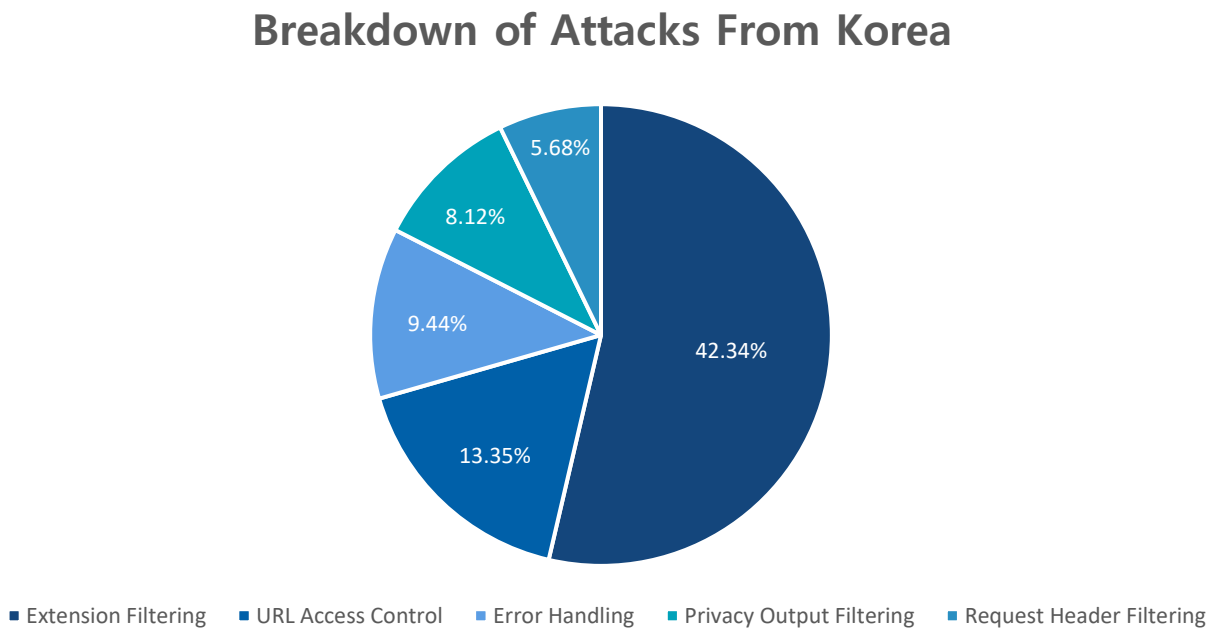
Attacks were distributed across the following industry targets: retail and manufacturing, broadcasting and communications, education, public administration, and online shopping. For the retail and manufacturing industry, which suffered more than 12% of all web attacks, the tremendous customer databases are highly tempting targets for hackers. This makes it crucial for retail and manufacturing firms to protect the personal data of their customers.

The broadcasting and communications industry and the education industry are also facing frequent web attacks. Due to the COVID-19 pandemic, consumption of online media and usage of online lectures have grown significantly. Security personnel must pay close attention and establish multiple security measures to protect sensitive personal information from the hands of hackers.

The danger is not only limited to personal information. Each industry contains sensitive and valuable data from financial statements and contracts to intellectual property and trade secrets, all of which must be protected with adequate security measures.

III. Trends in Web Attacks for the First Half of 2020

6. Regional Trend (1/3)

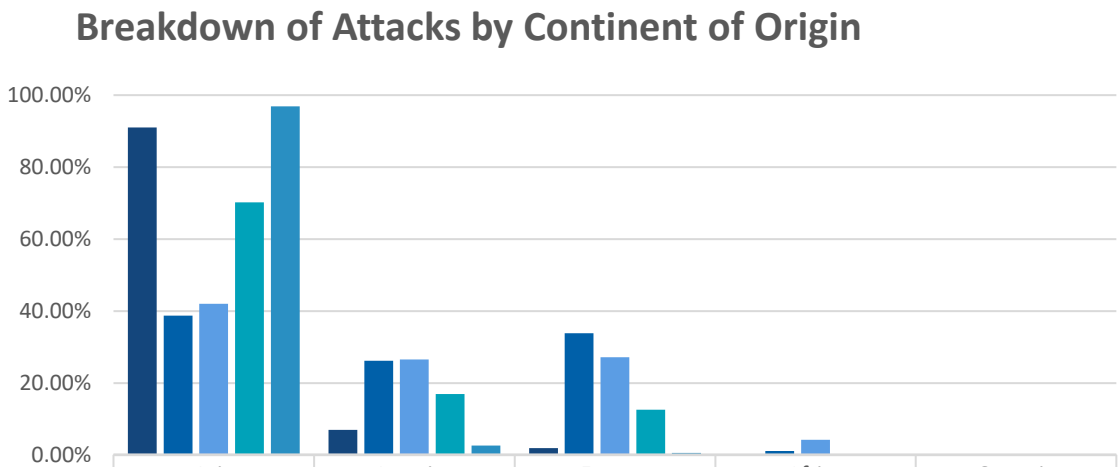


In the first part of this segment, attacks originating from South Korea were analyzed separately as seen in the graph above. The reason Korean data is presented separately is because South Korea is home to many of WAPPLES' users and subscribers of the WATT Report. Thus, a separate analysis on the attack rules originating from South Korea is provided.

The most common web attack rules originating from South Korea are Extension Filtering (42.34%), URL Access Control (13.35%), Error Handling (9.44%), Privacy Output Filtering (8.12%), and Request Header Filtering (5.68%). This breakdown is very similar to the general breakdown of "Web Attack Trends by Rule". South Korea is one of the most economically active countries, meaning that it has a lot of personal and sensitive data that hackers are looking for. As such, security managers in South Korea must be extra cautious for Extension Filtering (42.34%), which accounts for over 40% of total web attacks. Techniques like scripting, performing abnormal function, with data leakage and follow-up attacks are constantly expected, making it necessary to always stay on high alert.

III. Trends in Web Attacks for the First Half of 2020

6. Regional Trend (2/3)



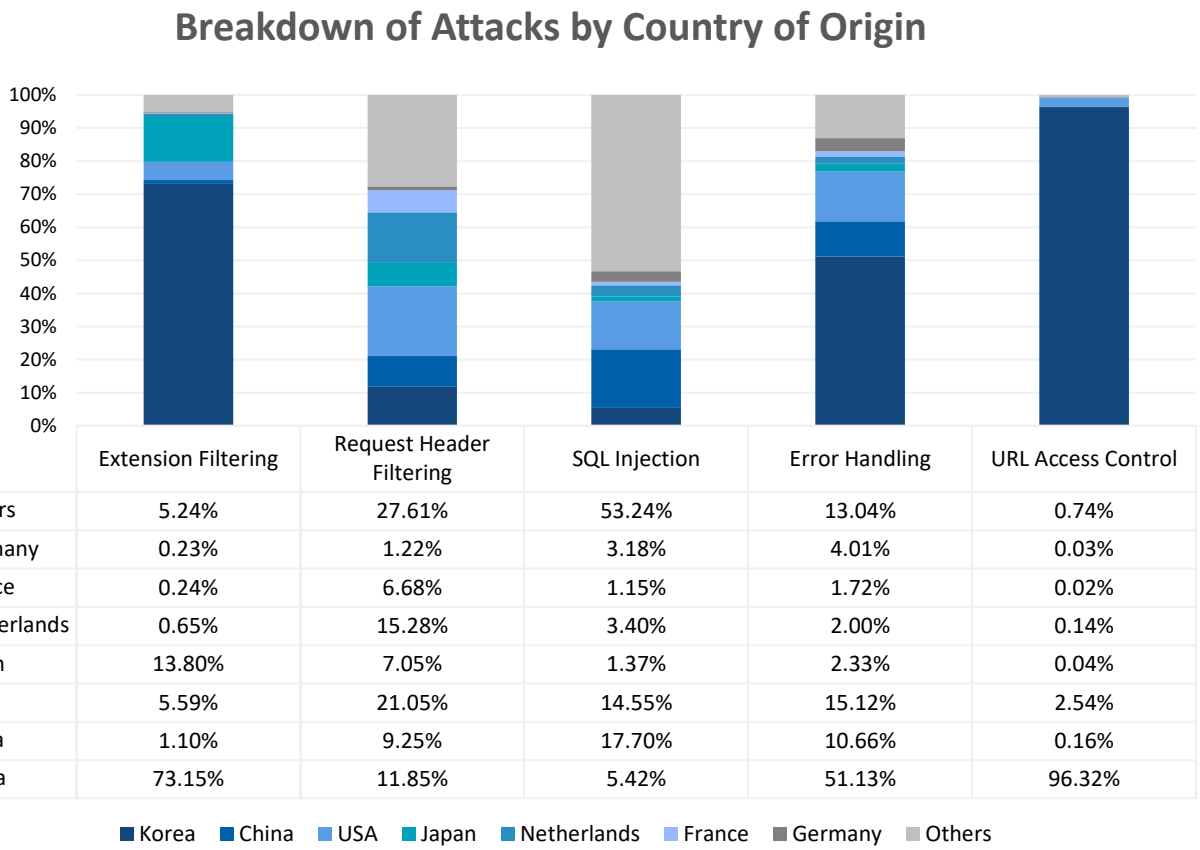
	Asia	America	Europe	Africa	Oceania
Extension Filtering	90.98%	6.95%	1.95%	0.09%	0.04%
Request Header Filtering	38.75%	26.16%	33.84%	1.09%	0.16%
SQL Injection	41.98%	26.58%	27.13%	4.20%	0.12%
Error Handling	70.21%	16.95%	12.62%	0.12%	0.09%
URL Access Control	96.84%	2.58%	0.56%	0.01%	0.01%

The graph above exhibits the breakdown of the web attack rules by their continent of origin. Similar to the breakdown last year, the continent where most web attacks were originated in is Asia, followed by the Americas, Europe, Africa, and Oceania. Compared to last year, the percentage of web attacks coming out of Europe has decreased, while those originating from Asia and the Americas rose. Even though the prevalent types of attacks have changed, hackers have been utilizing countries with active economic activities and frequent intercontinental information exchanges as the origin of web attacks. Security managers should focus their preparations on attacks that originate from Asia, the Americas, and Europe.

In addition, when looking at the count of all web attacks by continent, Extension Filtering accounted for the largest percentage, followed by Request Header Filtering, SQL Injection, Error Handling, and URL Access Control. Looking a step closer, Extension Filtering is prominent in Asia, while SQL Injection attacks are common across all three continents. Security managers across the world should prepare for web attacks based on such regional trends. Particular attention should be paid to attacks like Extension Filtering and Request Header Filtering, both highly common.

III. Trends in Web Attacks for the First Half of 2020

6. Regional Trend (3/3)



	Extension Filtering	Request Header Filtering	SQL Injection	Error Handling	URL Access Control
Others	5.24%	27.61%	53.24%	13.04%	0.74%
Germany	0.23%	1.22%	3.18%	4.01%	0.03%
France	0.24%	6.68%	1.15%	1.72%	0.02%
Netherlands	0.65%	15.28%	3.40%	2.00%	0.14%
Japan	13.80%	7.05%	1.37%	2.33%	0.04%
USA	5.59%	21.05%	14.55%	15.12%	2.54%
China	1.10%	9.25%	17.70%	10.66%	0.16%
Korea	73.15%	11.85%	5.42%	51.13%	96.32%

The graph above illustrates the top seven countries where the highest proportions of of web attacks originated from.

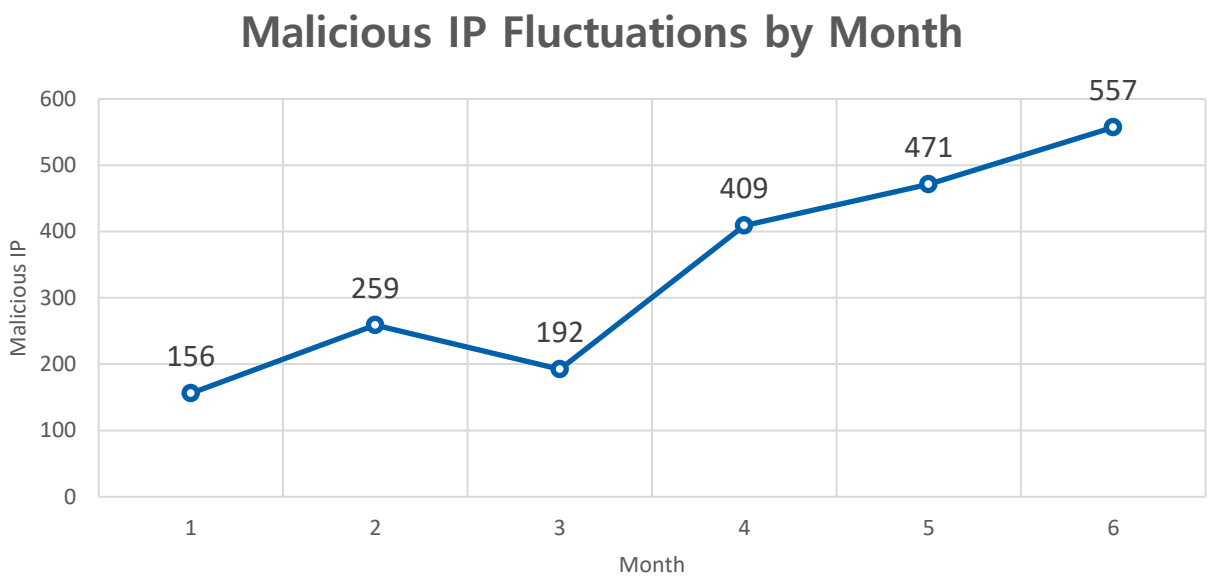
Compared to the previous report, France and the Netherlands are new to the list. As always, South Korea, China, USA, and Japan maintained their top spots on the list.

As seen in the graph, Extension Filtering and Request Header Filtering are two most common web attacks overall regardless of their country of origin. The graph also shows that most web attacks come from countries with high economic outputs, meaning that security managers in these countries must enhance their web security measures to stay safe.

There are a lot of countries that belong to the "Others" category. Especially in the case of SQL Injection, over 50% of these attacks occurred in countries that are not on the top 7 list, meaning that all countries should be aware of SQL Injection attacks. In sum, there is no country that is completely safe from web attacks, meaning that everyone should have adequate web security measures in place.

III. Trends in Web Attacks for the First Half of 2020

7. Variation Trend in No. of Malicious IPs



The graph above shows the fluctuations in the number of detected malicious IPs, the ultimate weapon used for web attacks. The reason we look at the number of malicious IPs is because they are a fair indicator of the frequency and severity of web attacks. Nevertheless, it is not meant to be a reliable indicator because there are times when a single attacker uses multiple malicious IPs, and other times when a single malicious IP causes significant damage.

We define malicious IP as one that engages in attacks for more than 3,000 times a month. By analyzing the relationship between the fluctuations of malicious IP and specific incidents in the first half of 2020, we could identify the attack patterns and strengthen the respective web security measures to defend against similar attack patterns in the future.

The number of detected malicious IPs fluctuated between 156 and 557 per month, averaging at 340 per month over the first half of 2020. During this period, COVID-19-themed cyberattacks significantly increased, especially after April, when it became a global pandemic. Some of the common attacks included 1) phishing scams with COVID-19 related information, 2) hacking aimed at workers working from home, and 3) hacking of healthcare providers and organizations, including the WHO.

Indeed, the number of malicious IP isn't necessarily related to each specific web attack trend. But they do tend to move in similar directions. Again, it is important to prepare for and inspect the risks of various web attacks and prepare to respond quickly and accurately according to the manual in case of attacks.

IV. APPENDIX

1. Method of Analysis

1) Data Collection Method and Duration

The data reported in this WATT Report is collected from the logs of WAPPLES, a web application firewall widely distributed in the Asia Pacific region, and Cloudbric, a cloud-based web application firewall (WAFaaS) distributed worldwide. The data collection duration is between January 1, 2020 and June 30, 2020.

2) Key Differences from Previous Reports

Different from the previous WATT Reports, the 2020 H1 WATT Report included data from Cloudbric, a cloud-based web application firewall distributed around the world. Additionally, Penta Security's newly developed machine learning technology allowed for more accurate prediction of future attacks. In addition, by analyzing web attacks based on their objectives and based on OWASP Top 10, a more advanced report was created.

The WATT Report, which will now be published semi-annually, is prepared with both industry professionals and casual readers in mind. On the professional end, it provides insights for security managers, many of them being users of WAPPLES and Cloudbric. On the casual end, it is an easy read for general readers like those involved in research institutions who are interested in web security trends. In the future, we plan to update information through continuous research and analysis and publish a report semi-annually to identify and compare the latest trends.

3) Glossary

▪ Extension Filtering

File extensions serve the purpose of indicating the file type. Extension filtering refers to the act of using malicious/abnormal extensions for malicious purposes, such as to induce file download or file execution.

Potential Consequences: Execution of abnormal functions through scripting

▪ File Inclusion

File Inclusion mainly targets PHP applications. By exploiting the "Include Script" function of PHP, the threat actor delivers malicious scripts to the servers and executes malicious codes through the server webpage. By doing so, the hacker could access, modify, or delete files that contain sensitive information.

Potential Consequences: Compromise of sensitive files and data, execution of abnormal functions through scripting

▪ Invalid HTTP/URL

Invalid HTTP/URL usually occurs during the process of delivering information to the outside after receiving HTTP requests. Attackers would inject malicious commands into the information delivered, after which the web application would deliver the whole command to the external program. By exploiting this vulnerability, attackers could plant trojans or execute malicious codes into the programs.

Potential Consequences: Compromise of sensitive file and data

I. APPENDIX

▪ Request Header Filtering

When an HTTP request gets sent from the web browser, attackers would interfere by removing necessary elements from the header or replace it with a different element, resulting in the request to be sent in the wrong form. It is commonly used in automated attack tools. This type of attack can tamper the information of the web server and can end up causing damages to the server.

Potential Consequences: Web server information tampering, abnormal behavior of server

▪ Error Handling

By using the code included in the packet that the server responds to, the processing result gets communicated to the client. In the case of a specific error message, the type and version of the web server, web application, and DBMS are included in the message. The lack of detection and blocking policies may lead to information leakage and cause significant damage.

Potential Consequences: Compromise of sensitive files and data, secondary attacks

▪ Directory Traversal

Directory traversal is a form of HTTP attack where hackers gain access to restricted directories and obtain sensitive files of which the system administrator keeps private from the users.

Potential Consequences: Access to system files and source code

▪ SQL Injection

SQL injection is when attackers interfere with the SQL query made by an application to its database server, hence allowing them to attack the database server and view, modify, and exfiltrate sensitive data.

Potential Consequences: Compromise of sensitive files and data, bypass of system authorization

IV. APPENDIX

4) OWASP and WAPPLES/Cloudbric Detection Rules

OWASP(Open Web Application Security Project) creates a list every three years of the most exploited and dangerous web application vulnerabilities, commonly referred to as the OWASP Top 10. Below is a list of the latest OWASP Top 10 and the respective WAPPLES/Cloudbric Rules used to protect them.

TOP	OWASP TOP 10	WAPPLES/Cloudbric Rules
1	injection	SQL Injection
		Stealth Commanding
		Cross Site Scripting
2	Broken Authentication	Cookie Poisoning
		Directory Traversal
		Cross Site Request Forgery
		SQL Injection
3	Sensitive Data Exposure	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Content Filtering
		Response Header Filtering
		Error Handling
4	XML External Entities	User Defined Pattern
5	Broken Access Control	Parameter Tampering
		Invalid URL
		Directory Traversal
		URL Access Control
6	Security Misconfiguration	Directory Listing
		Error Handling
		Response Header Filtering
7	Cross Site Scripting	Cross Site Scripting
8	Insecure Deserialization	Insecure Deserialization
9	Insecure Deserialization	User Defined Pattern
		Custom Rule
10	Using Components with Known Vulnerabilities	Detection Log Monitoring and Sync

* One WAPPLES/Cloudbric Rule could be matched to multiple OWASP TOP 10 vulnerabilities.

IV. APPENDIX

5) TOP 40 Attacker IP List

Rank	Attacker IP	Country of Origin
1	175.21.X.X	China
2	175.21.X.X	China
3	34.74.X.X	USA
4	175.21.X.X	China
5	103.66.X.X	Unknown
6	129.21.X.X	USA
7	195.123.X.X	Ukraine
8	45.192.X.X	Seychelles
9	210.140.X.X	Japan
10	107.6.X.X	Netherlands
11	210.159.X.X	Japan
12	38.108.X.X	USA
13	185.143.X.X	Netherlands
14	175.21.X.X	China
15	45.135.X.X	Unknown
16	221.8.X.X	China
17	17.58.X.X	USA
18	125.198.X.X	Japan
19	152.99.X.X	Korea
20	35.200.X.X	USA
21	45.227.X.X	Unknown
22	182.47.X.X	China
23	78.47.X.X	Germany
24	39.110.X.X	Hongkong
25	195.206.X.X	UK
26	45.227.X.X	Panama
27	42.49.X.X	China
28	42.3.16.X.X	Hongkong
29	175.21.X.X	China
30	211.253.X.X	Korea
31	210.175.X.X	Japan
32	185.221.X.X	Russia
33	5.188.X.X	Ireland
34	45.227.X.X	Panama
35	125.130.X.X	Korea
36	45.227.X.X	Panama
37	210.175.X.X	Japan
38	211.43.X.X	Korea
39	210.175.X.X	Japan
40	211.46.X.X	Korea

Penta SECURITY
enterprise · iot · blockchain

KOREA	www.pentasecurity.co.kr
GLOBAL	www.pentasecurity.com
JAPAN	www.pentasecurity.co.jp
CHINA	www.panqi.tech

cloudbric

KOREA	www.cloudbric.com
JAPAN	www.cloudbric.jp

Cyber Security Awards Application Security 2020

IoT-based Smart Security Innovation Award 2020

Member of the International Transport Forum CPB

TU-Automotive Awards Best Auto Cybersecurity Product/Service 2019

Cybersecurity Excellence Awards Winner 2018

Hot Company in Web Application Security for 2016

SC Magazine Europe Best SME Solution

Recognized on the Gartner WAF Magic Quadrant

ICSA Labs Certified WAF

The First and Only CCEAL4 Certified WAF

PCI-DSS Compliance