Web Application Threat Trend Report

2018

Penta Security Systems

Contents

I. Overview

1. Purpose

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 2018 WATT report is an analysis of attack data in accordance with the Top 5 rules which are web attack trends by rule, trends in primary attacker behavior, industry, region, and time specific trends.

1. Web Attack Trends by Rule

The top 5 web attack trends detected by WAPPLES are as follows: Extension Filtering (32.71%), Error Handling (17.22%), Cross Site Scripting (6.99%), Request header Filtering (6.27%), Stealth Commanding (5.77%). A new attack was detected in 2018 which requires further attention, however, Cross Site Scripting and Stealth Commanding attacks that also ranked in top 5 in 2017 were consecutively detected.

2. Trends in Primary Attacker Behavior

Criteria for classification as a 'Black IP' include attackers that launched more than 1 million web attacks over the course of 2018, and have a threat score of 80 or above. The primary web attack trend of Black IP differ from the average web attack trends, which explains the critical reason why it requires particular attention through continuous monitoring. Primary attackers favored attacks like Request Header Filtering (69.81%), SQL Injection (13.21%), Stealth Commanding (9.36%), Cross Site Scripting (3.70%), and Error Handling (2.11%). Additionally, the attacks occurred 942 times a year in average (maximum 1861 and minimum 87 times) and especially occurred more often in January, May, and June in 2018.

3. Industry-specific Trends

The industries surveyed and analyzed in 2018 were classified in different industries including education, broadcasting and communications, retail and manufacturing, organizations, public administration, and entertainment. Main attacks were as follows: Cross Site Scripting, Include Injection, File Upload, SQL Injection, Stealth Commanding, Directory Traversal.

4. Regional Trends

The ratios of attacks originating in Korea were as follows: Extension Filtering (44.90%), Request Header Filtering (24.06%), Error Handling (19.31%), Cross Site Scripting (8.20%), Stealth Commanding (3.53%). In addition, by continents, Asia accounted for the highest number of attack detections with North and South America combined, Europe, Oceania, and Africa following behind. Extension Filtering occurred the most especially in Asia, Europe, and North and South America combined.

Moreover, by country, Korea accounted for the highest number of attacks originated from Asia, with North and South America combined, China, Malaysia, Russia, Japan, and Germany following behind.

5. Trends Across Time of Day

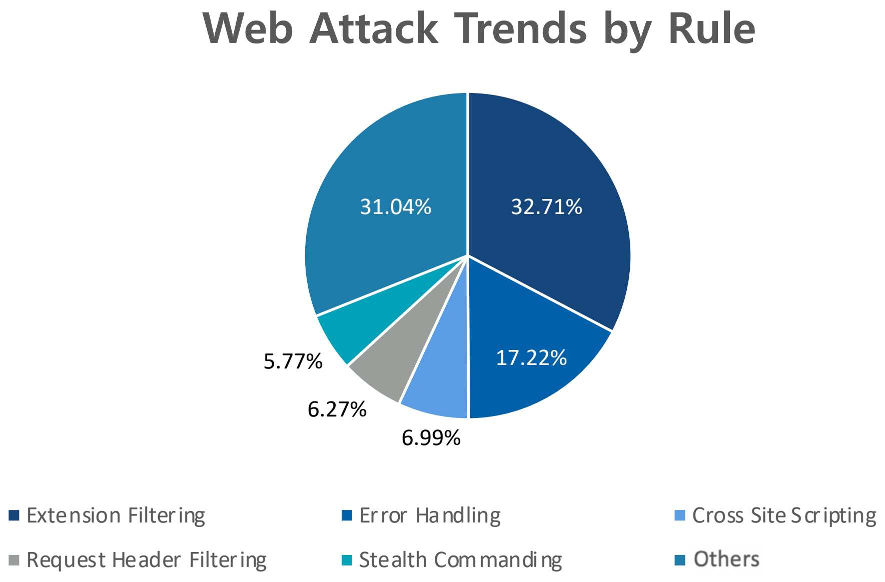
More than 600,000 web attacks took place at all hours of day. Particularly from 10:30 to 12:30 and 15:00 to 17:00, which can be seen as opportunities due to change of shifts (meal time, etc.) and when security protections are paused temporarily to conduct system inspections. Therefore it is important to pay special attention during the abovementioned hours.

III. 2018 Web Application Threat Trends

1. Web Attack Trends by Rule

Web attacks detected over the course of the year are analyzed based on which of 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 2018.



At 32.71%, Extension Filtering accounted for the highest number of attack detections, with Error Handling (17.22%), Cross Site Scripting (6.99%), Request header Filtering (6.27%), and Stealth Commanding (5.77%) following behind.

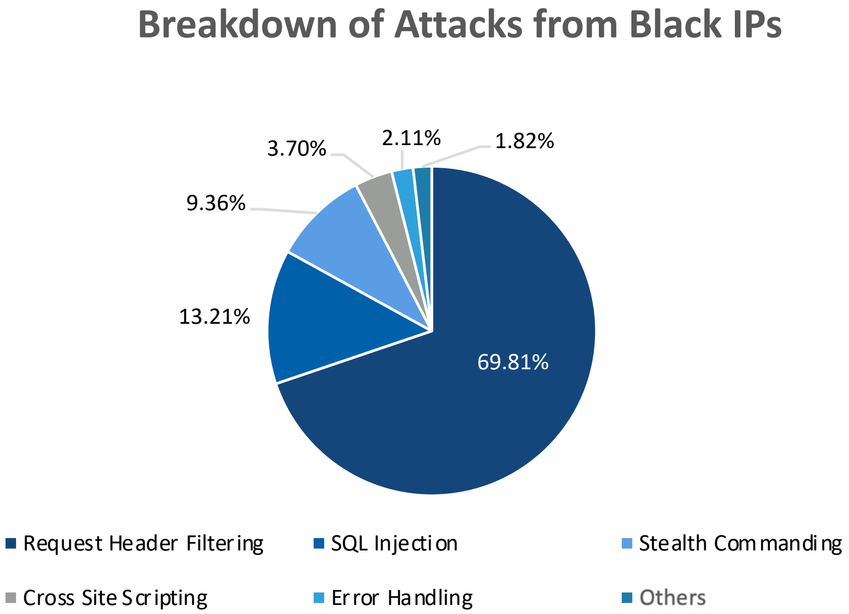
Extension Filtering accounted for the highest number of attacks back in 2015 and again in 2018. Extension Filtering refers to attempts to access configuration files (dll, conf, ini, etc.) rather than the ones in extension formats commonly used by websites. This is a very dangerous attack as it can directly have impact on web server behaviors and web services once exposed to other users.

Error Handling attacks ranked third (12.2%) in the 2012 roundup. The improper handling of errors when using web applications can occur various security issues such as providing hints about vulnerabilities to malicious users. In addition, it can also cause information leakage by not managing error messages for web server, WAS, DBMS server, etc.

Cross Site Scripting(XSS) attacks ranked fourth in the 2017 roundup. 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.

Other attacks such as Stealth Commanding are also well know that can cause great damages. It is critical to establish security measures in order to prevent these web attacks.

2. Trends in Primary Attacker Behavior



The above graph shows attacks by primary attackers (Black IPs) detected from January 1, 2018 to December 31, 2018. Primary attackers are categorized as such because of their threat score (80 or above), and their high likelihood of causing significant damage. The actions of such malicious attackers are likely to cause real damages, therefore, it is important to select primary attackers (Black IP) and look at their web attack trends.

The distribution of attacks in 2018 is as follows: Request Header Filtering(69.81%), SQL Injection(13.21%), Stealth Commanding(9.36%), Cross Site Scripting(3.70%), and Error Handling(2.11%).

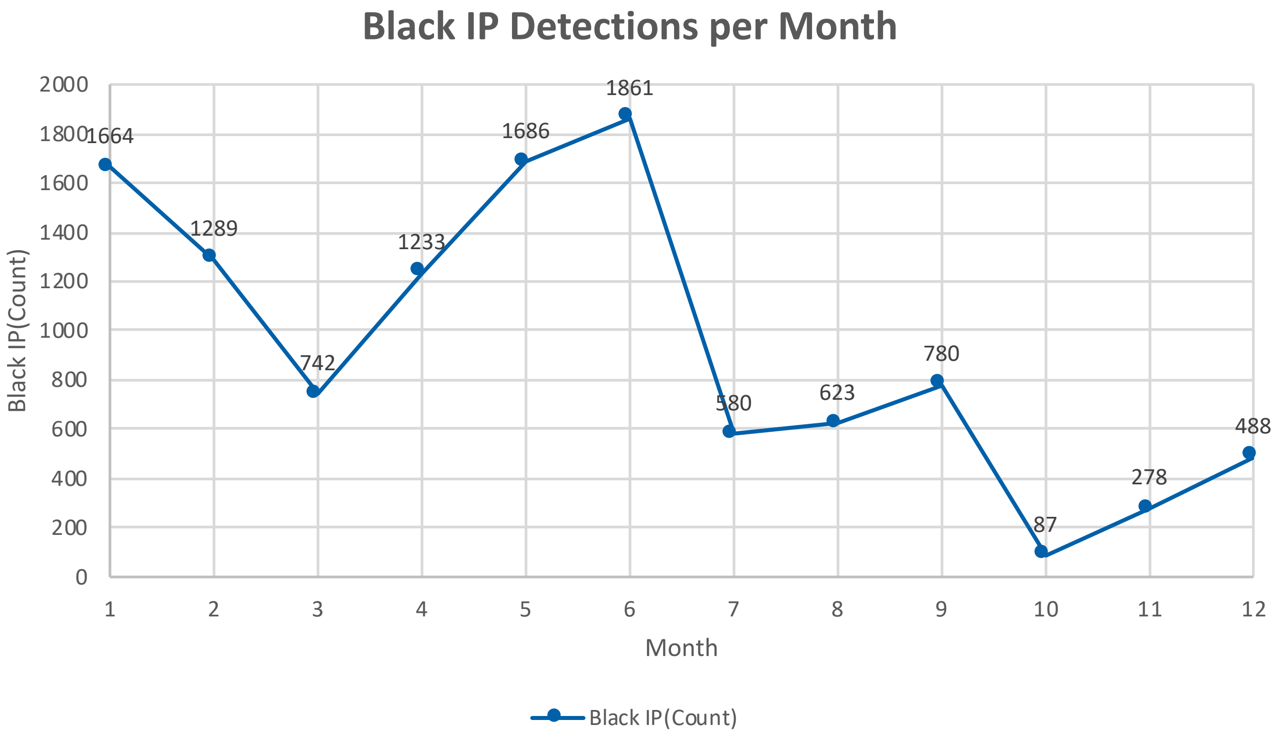
Request Header Filtering is an attack using HTTP Request from a web browser. Unlike normal HTTP request, the hackers can omit required elements or contain other and abnormal elements and send the request. Such attacks can tamper or damage web server's information and cause secondary damages.

The next was SQL Injection, which is a technique of Injection which executes unacceptable or irrelevant SQL statements and end up attacking the database. This is one of the most common attacks that can cause a large amount of information leakage. As various SQL Injection attack methods are detected, it is important to continuously pay attention to SQL Injections attacks.

Lastly, the third is Stealth Commanding attack method, which often occurs 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.

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.

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 atta ck (as a single hacker may utilize multiple IP addresses or launch repeated attacks in other months), the number of Black IP s detected each month can help gauge which part of the year saw the greatest volume of advanced attacks.

It may not be 100% objective due to the criteria of selecting Black IPs, however, it is possible to identify patterns by linking the fluctuation and connection to specific events in order to further secure strengthen the web when similar patterns and attacks are predicted in the future.

A yearly average of 942 Black IPs had been detected in 2018 (maximum 1861 and minimum 87 times), with notable increases in January, May, and June compared to in 2017, with over 1000 detections.

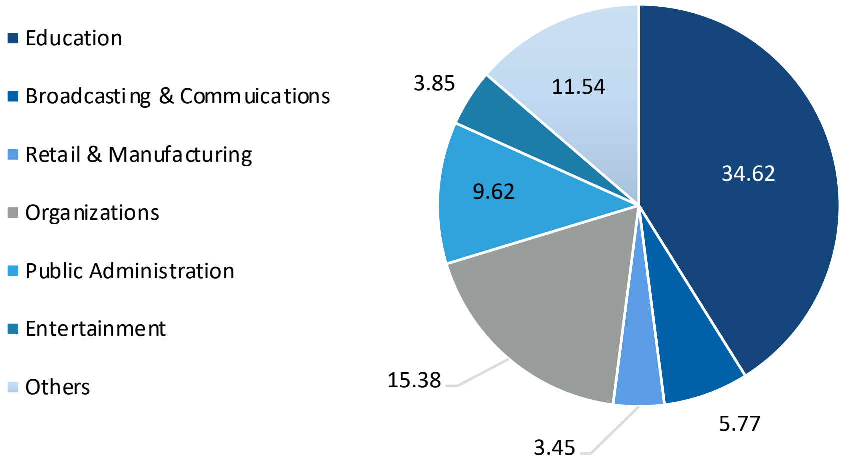
These months saw a number of incidents involving 1) Increased hacking and cyber attack attempts for Ministry of Unification in 2018, 2) Continuous hacking attempts for cryptocurrency exchanges, 3) IP camera hacking incidents that led to invasion of privacy, which are all interconnected with each other.

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. 2018 Web Application Threat Trends

4. Industry-specific Trends

Distribution of Attacks Across Industry Targets



Main Attacks

Cross Site Scripting
Include Injection
File Upload
SQL Injection
Stealth Commanding
Directory Traversal

The chart specifies which attacks were most commonly detected on all industry-associated WAPPLES devices. There were more than just attack trends by rule which allows each industry to analyze and be prepared for various attacks.

Attacks were distributed across industry targets as follows: Education (34.62%), Broadcasting and communications (5.77%) , Retail and manufacturing (3.45%), Organizations (15.38%), Public administration (9.62%), Entertainment (3.85%), and Others (11.54%).

The above chart shows that various attacks occurred in education, broadcasting and communications, retail and manufacturing, organizations, public administration, and entertainment industries. In the case of education industry, the attempt occurred in order to capture the students' and faculty's sensitive information. Therefore, security managers must be able to manage and protect various information and data including sensitive information.

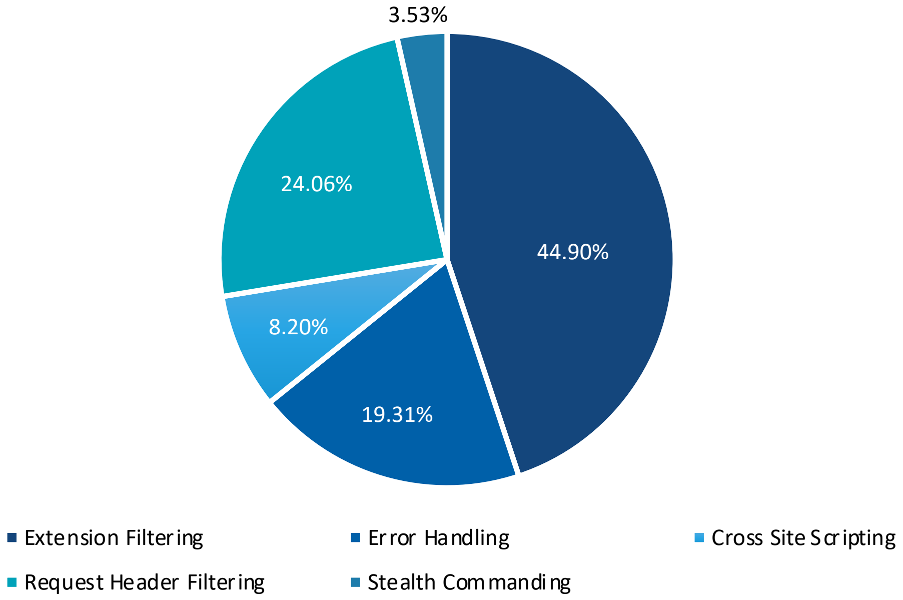
Retail and manufacturing, organizations, and other industries (text message services, etc.) could potentially lead to a secondary offensive utilizing social engineering to gain more privileged access or launch phishing scams.

The industries that suffered from website attacks not only affected the universities, but moreover, affiliated organizations and leakage of students' and faculty's sensitive information. Attacks against these industries can also have impact on critical industrial information, therefore, special attention should be paid to handling the information.

III. 2018 Web Application Threat Trends

5. Regional Trends (1/3)

Breakdown of Attacks from Korea



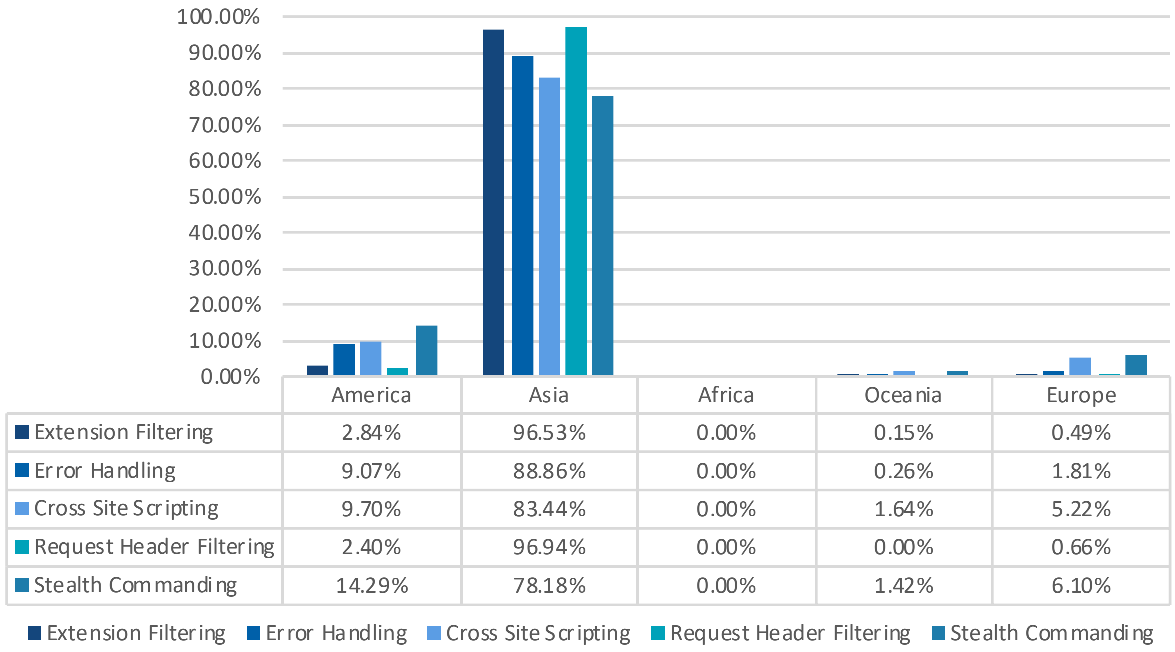
In the first part of this segment, attacks originating in Korea were analyzed separately. The chart above shows what kinds of attacks were most frequently launched from Korea in 2017. The choice of this particular segmentation was made in recognition that among the security administrators who use WAPPLES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

Attacks originating in Korea were segmented as follows: Extension Filtering (44.90%), Request Header Filtering (24.06%), Error Handling (19.31%), Cross Site Scripting (8.20%), and Stealth Commanding (3.53%).The ratios were similar to the overall attack ratios of web attack trends by rule and likewise, security managers based in Korea or in companies targeting Korean consumers should pay close attention to Extension Filtering, Request Header Filtering, and Error Handling especially since these attacks made up over 80% of all attacks. With one of the most active economies around the world that has extensive amount of sensitive and important information. In order to prevent information leaks and secondary attacks, it is necessary to be prepared for constant attacks such as performing abnormal functions through scripts or tampering with web server information to induce abnormal behavior and result.

III. 2018 Web Application Threat Reports

5. Regional Trends (2/3)

Breakdown of Attacks by Continental Origin



	America	Asia	Africa	Oceania	Europe
■ Extension Filtering	2.84%	96.53%	0.00%	0.15%	0.49%
■ Error Handling	9.07%	88.86%	0.00%	0.26%	1.81%
■ Cross Site Scripting	9.70%	83.44%	0.00%	1.64%	5.22%
■ Request Header Filtering	2.40%	96.94%	0.00%	0.00%	0.66%
■ Stealth Commanding	14.29%	78.18%	0.00%	1.42%	6.10%

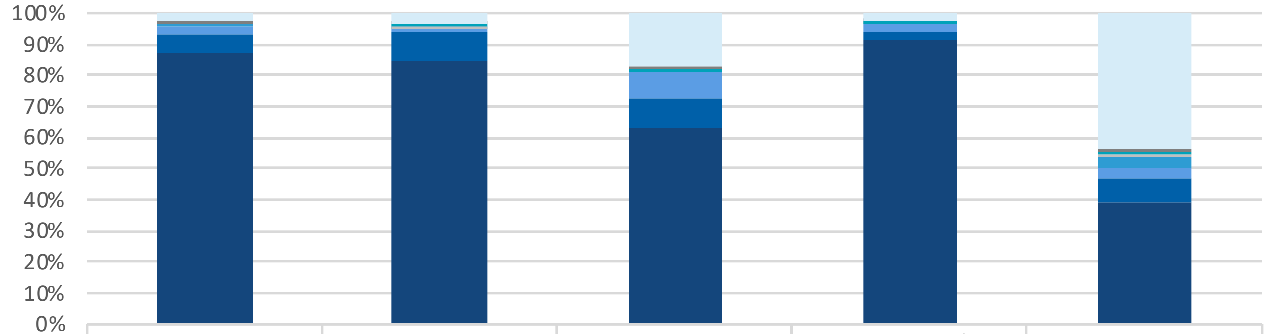
The chart above follows the attack trends in regions according to where attacks originated. Similar to patterns seen in 2017, the highest number of attacks originated from Asia, followed by North and South America combined, Europe, Africa, and Oceania. Known to be hubs for intercontinental exchanges and vibrant economic activity, Asia, Europe and the Americ as are highly targeted for web attacks, especially by attacks from within the respective regions. Although the type of web application attacks have changed, it can be assumed that the hackers aim to set countries with higher economic activity and intercontinental exchanges as web attack start points. Therefore security managers should be particularly prepared for web attacks originating from these three continents.

Extension Filtering accounted for the highest proportion of attacks, followed by Request Header Filtering, Error Handling, Cross Site Scripting, and Stealth Commanding. Asia was observed to be a major source of Extension Filtering, and Request Header Filtering and Stealth Commanding, and Cross Site Scripting for North and South America combined and Europe.

III. 2018 Web Application Threat Trends

5. Regional Trends (3/3)

Breakdown of Attacks by Country of Origin



	Extension Filtering	Error Handling	Cross Site Scripting	Request Header Filtering	Stealth Commanding
■ Others	2.95%	3.37%	17.37%	2.82%	43.50%
■ Germany	0.24%	0.29%	0.63%	0.14%	0.83%
■ Japan	0.33%	0.43%	0.85%	0.66%	0.84%
■ Russia	0.00%	0.95%	0.00%	0.15%	1.16%
■ Malaysia	1.15%	0.49%	0.00%	0.00%	3.49%
■ China	2.33%	0.83%	8.89%	2.26%	3.58%
■ USA	5.93%	8.86%	8.70%	2.35%	7.56%
■ Korea	87.06%	84.79%	63.57%	91.62%	39.04%

■ Korea ■ USA ■ China ■ Malaysia ■ Russia ■ Japan ■ Germany ■ Others

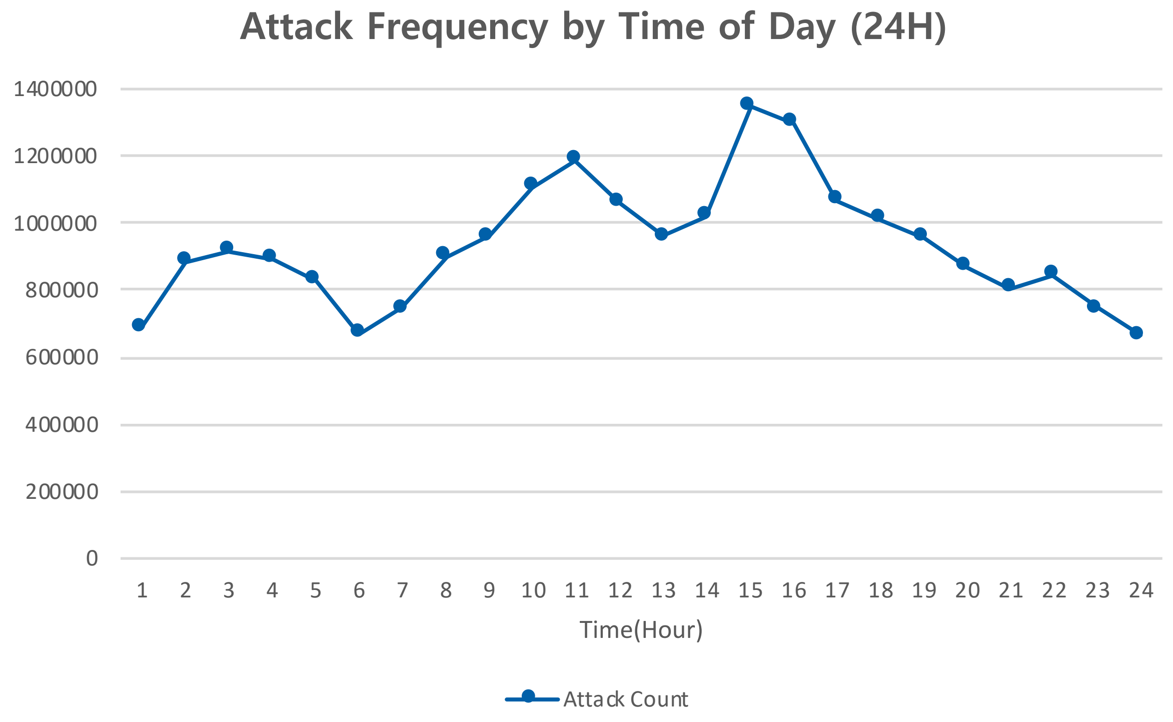
The chart above follows the seven countries have been identified to contribute the highest percentage of attacks and the distribution of attack types within these countries.

Compared to the previous report, Malaysia and Germany had entered the chart. While there might be some shifts in rankings, United States, China, Russia, Japan including Korea were among the Top 7 countries, continuously, and the countries that are in the top of the list of regional trends by rule are the major sources of attacks by country of origin.

A relatively high percentage of attacks in each country were made up of Extension Filtering and Stealth Commanding and United States, China, and Russia have again occupied top spots. There are countless countries in the Others section. In particular, since more than 40% of Stealth Commanding attacks occurred in other countries, therefore, defense against web attacks need to be stepped up regardless of the country of origin.

III. 2018 Web Application Threat Trends

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 inter vals, 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 600,000 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 10:30 to 12:30, and 15:00 to 17:00, as well as after usual work hours. At times before lunch and dinner, quickly undertaking web security countermeasures can be especially difficult.

Security might already be an imperative in certain organizations that are able to deploy resources for continuous monitor ing 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 respo nding 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 analysis from WAPPLES taken from January 1, 2018 through December 31, 2018.

2) Key Differences from Previous Reports

Like the ICS Reports published up to 2015 and the 2016 and 2017 WATT Report, this report is based on true-positive log s 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 organizati ons, national and private research institutions, as well as university laboratories interested in web security trends. Penta Secu rity Systems publishes the WATT Report annually, detailing observed trends so they may be used as a comparative referenc e 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.

- **Extension Filtering**

Overview : Extension refers to the extension that records the file type in the name. By exploiting this, hackers use malicious/abnormal extensions for malicious purposes to induce file downloads, file execution, etc. to perform the desired behavior.

Expected consequence: Performance of abnormal function through script

- **Error Handling**

Overview : By using the Code included in the packet that the server responds, the processing result is informed to the client. In the case of a specific error message, Web Server, Web Application, and the type and version of DBMS are also informed. The lack of detection and blocking policies may lead to information leakage which can cause significant damages.

Expected Consequence: Information leakage, Preparation for secondary attacks

- **Cross Site Scripting**

Overview : An attack technique involving the insertion of malicious scripts into forum posts or emails to cause other user s 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

IV. APPENDIX

▪ Request Header Filtering

Overview : Unlike the normal HTTP Request that is sent from the web browser, hackers with malicious intent removes required element from the Header or writes another element and send it in the wrong form. It is often 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.

Expected Consequence : Web server information tampering, abnormal behavior of the server

▪ 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 pr otocols.

Expected consequence : Abnormal behavior of the server, data leakage

The terms introduced above are all vulnerabilities and attacks that can cause damages and service disruptions through information and data leakage. Based on the report published by Penta Security, it is critical to prepare your own security protection and countermeasures to protect valuable business and personal information.

IV. APPENDIX

4) Black IP List

Ranking	IP Address	Country	Threat Score
1	211.253.x.x	Korea	98.11
2	211.233.x.x	Korea	97.66
3	61.97.x.x	Korea	97.31
4	1.223.x.x	Korea	96.75
5	116.120.x.x	Korea	96.23
6	115.95.x.x	Korea	96.01
7	100.210.x.x	United States	95.54
8	222.231.x.x	Korea	95.22
9	36.234.x.x	Taiwan	93.89
10	10.206.x.x	United States	93.41
11	104.155.x.x	United States	92.88
12	210.94.x.x	Korea	91.09
13	211.218.x.x	Korea	91.01
14	211.253.x.x	Korea	89.71
15	211.253.x.x	Korea	89.44
16	35.197.x.x	United States	89.04
17	175.192.x.x	Korea	88.91
18	103.29.x.x	Japan	88.89
19	51.15.x.x	United Kingdom	88.51
20	118.129.x.x	Korea	87.78
21	222.239.x.x	Korea	87.64
22	122.54.x.x	Philippines	87.55
23	211.253.x.x	Korea	87.13
24	106.248.x.x	Korea	87.07
25	1.244.x.x	Korea	86.98
26	91.247.x.x	Ukraine	86.93
27	222.106.x.x	Korea	86.68
28	14.47.x.x	Korea	86.49
29	100.210.x.x	United States	86.21
30	54.249.x.x	United States	86
31	115.60.x.x	China	85.88
32	1.215.x.x	Korea	85.71
33	183.111.x.x	Korea	85.27
34	58.246.x.x	China	84.95
35	211.176.x.x	Korea	84.76
36	59.3.x.x	Korea	84.11
37	210.179.x.x	Korea	84.03
38	115.22.x.x	Korea	83.95
39	185.222.x.x	United States	82.64
40	125.133.x.x	Korea	81.23

Penta SECURITY
enterprise · iot · blockchain

KOREA	www.pentasecurity.co.kr
GLOBAL	www.pentasecurity.com
JAPAN	www.pentasecurity.co.jp

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

Asian Cyber
Security Vendor
of the Year

Recognized on the
Gartner WAF
Magic Quadrant

No.1 WAF
Vendor in the
APAC Region

ICSA Labs
Certified WAF

The First and Only
CCEAL4 Certified
WAF

PCI-DSS
Compliance