20 year Anniversary

Asian Cyber Security Vendor of the Year

Penta SECURITY
cloud · iot · enterprise

Web Application Threat Trend Report

Trends for 2016

Penta SECURITY

Contents

I. Overview

II. Executive Summary

III. 2016 Web Attack Trends Analysis

1. Web Attack Trends by Rule
2. Primary Attacker Trends
3. Black IP Fluctuation Trends
4. Web Attack Trends by Industry
5. Web Attack Trends by Continent
6. Web Attack Trends by Time of Day

IV. Appendix

1. Data Compilation Target and Time Period
2. Key Differences from Previous Reports
3. Definition of Technical Terms
4. Black IP List

I. Overview

1. Report Summary

The **Web Application Threat Trend (WATT) Report** is a comprehensive report of attack trends and patterns compiled by Penta Security System's Intelligent Customer Support (ICS) team. The report is compiled 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]

The report focuses on providing information to customers and security administrators of each corporation and organization that utilizes WAPPLES.

The purpose of this report is to not only identify and predict future web attack patterns through the analysis of the latest web attack trends, but also to apply the trends and patterns to WAPPLES patented logic-based detection engine.

Subscribers are encouraged to use this report to be informed on statistical information regarding major web attacks based on the detection rules of WAPPLES. Information available covers various trends including attacks based on type, Black IP address, continent, industry, time of day, etc.

[1] Industry Quotient, Frost & Sullivan, 2015.

II. Executive Summary

This report covers trends in attacks, primary attackers and Black IP trends, as well as trends that emerged from looking at attack patterns when segmented based on industry, region, and time of day. The overall analysis is centered upon the analysis of attack data in relation to the five rules that are considered top priority in WAPPLES.

Web Attack Trend Analysis Overview

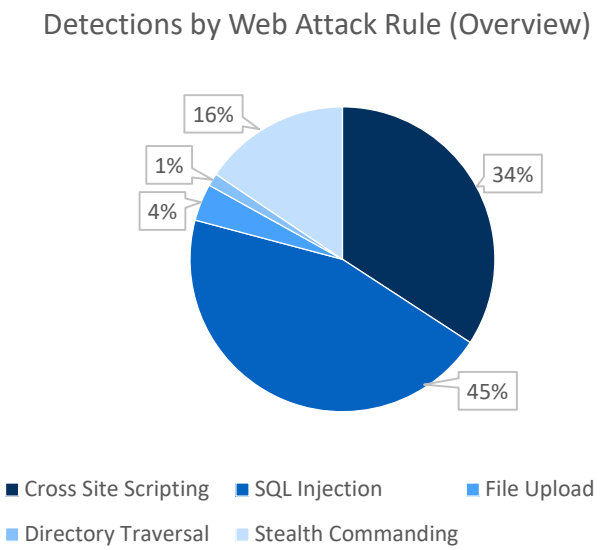
1. Of the five rule-based attacks, SQL injection (SQLi) accounted for the highest percentage of attacks at 45%. Aside from the month of March, SQLi held the highest percentage of attacks throughout 2016 (in March, Cross-Site Scripting or XSS exceeded SQLi with 48.4% of attacks).
2. The main attack types that account for 30% of the overall web attack numbers are SQL Injection (46%) and Cross-Site Scripting (30%). SQL Injection and Cross-Site Scripting attacks require serious attention due to the severity of the threats. These are threats that are capable of leaking internal information with just one successful attack.
3. Penta Security's security intelligence research team maintains a classification system based on specific threat factors that define particular IP addresses as especially malicious. These particularly dangerous IP addresses are labeled by Penta Security as "Black IPs." In 2016 the average number of Black IPs detected per month was 4551, which was higher than expected. January and September were notably high, at 8104 and 8834 respectively.
4. The main attack types for each industry were identified as below:
    - SQL injection: Transportation, Manufacturing & Construction, Food & Leisure
    - Cross-Site Scripting (XSS): Science & Technology, Social & Community
    -File Upload: Education and Financial Services
5. Data revealed that the XSS was found to be the most common attack for Asia, while SQLi was more common for Europe. North America showed a high percentage of Directory Traversal attacks.
6. Attacks took place at all hours of the day, but a particular spike of up to double the amount of attacks was noted between the hours of 18:00 and 19:00 – after typical business hours.

Theoretically, all organizations that possess valuable or sensitive information, regardless of industry, country, time period, or any other circumstances, as long as they are connected to the internet, have to be able to respond to and manage regular and continuous threats. The objective of this report is to provide various perspectives and insight into observations, especially those that are of particular importance.

* Refer to section "IV. Appendix" for definitions of technical terms.

III. 2016 Web Attack Trend Analysis

1. Web Attack Trends by Rule (1/2)



The graph above shows the frequency of detection of the five rules of web attacks in WAPPLES. These attacks are considered the most common and significant for 2016.

From January 1 to December 31, 2016, SQL Injection attacks were the most frequently detected, followed by Cross-Site Scripting, Stealth Commanding, File Upload and Directory Traversal.

SQL Injection is one of the most common techniques in web attacks and is a critical form of attack because of its potential to cause massive data leakage. Since stolen information can be leveraged for secondary criminal activities, SQL Injection attacks should not be thought of in terms of just the threat of information leakage. For example, in October 2015, UK telecom group "TalkTalk" was hit by an SQL Injection attack that exploited vulnerabilities in its customer database. This led to the exposure of nearly 157,000 customers' personal information, including names, addresses, birth dates and phone numbers. In its investigations, the Information Commissioner's Office (ICO) concluded that TalkTalk had failed to undertake basic security measures that could have prevented the attack and imposed a record fine of £400,000.[2]

Automated tools for SQL Injection attacks are readily accessible to hackers online. The danger lies in the fact that while an SQL Injection attack may be less costly to execute in comparison to other attacks, successful attacks could allow attackers to acquire large amounts of data.

Methods to defend against SQL injection attacks include:

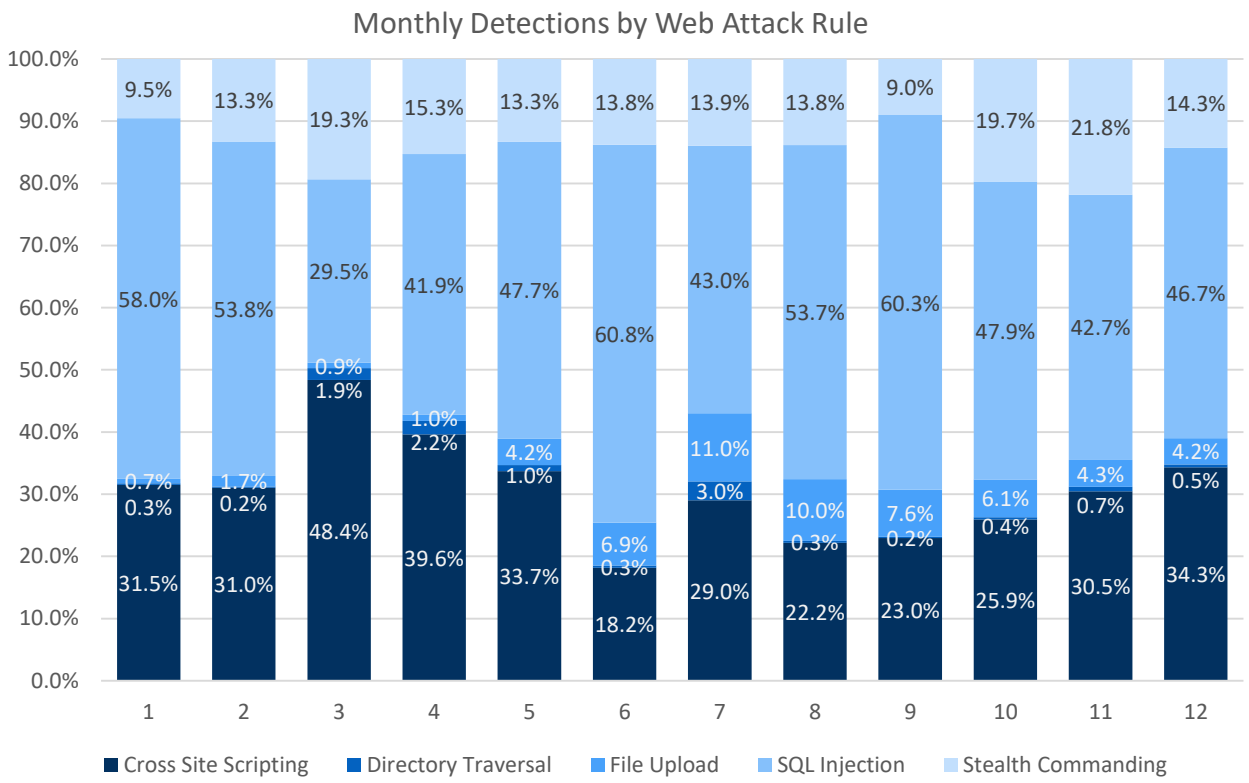
1. Avoid using Dynamic SQL which facilitates automatic generation of program statements
2. Build a good input validation process into the website design
3. Avoid exposure of database error messages

While a secure web design and implementation can be achieved through secure coding, in the field of security, human error always exists. Therefore one of the most fundamental ways of dealing with attacks is to maintain regular checks for web vulnerabilities and implement a WAF solution for greater assurance and trust.

[2] Source: http://www.computerweekly.com/news/450400451/TalkTalk-hit-by-record-400000-fine-over-data-breach

III. 2016 Web Attack Trend Analysis

1. Web Attack Trends by Rule (2/2)



The above graph shows the monthly detected frequency of the five rules of web attacks in WAPPLES.

As in previous years, the frequency of SQL Injection attacks was the highest, followed by Cross-Site Scripting attacks. However, in the month of March, Cross-Site Scripting attacks were found to be the highest. Since these two attacks are the most prevalent, responding to and preventing them is crucial.

Similar to SQL Injections attacks, Cross-Site Scripting attacks are also one of the most widely known attack techniques aimed at web applications. Cross-Site Scripting attacks are accomplished through malicious scripts embedded in forums or web mail. In case of a successful attack, the attacker may remotely execute commands, like downloading malicious code, which leads to secondary damages such as the leakage of user IDs and passwords.

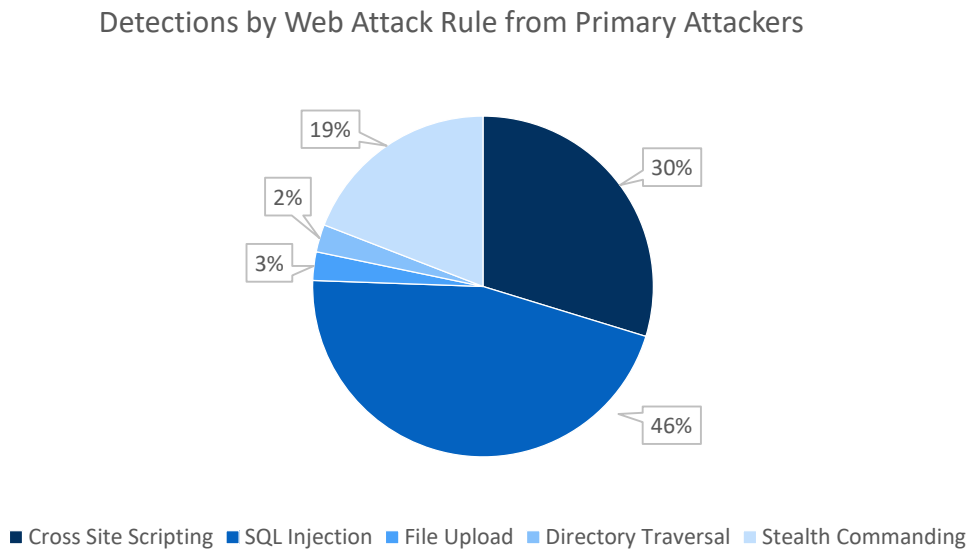
Internationally popular social media platform Twitter was attacked using Cross-Site Scripting, which directed users to pornographic sites when they moused over certain links on their accounts. Even notable figures were affected, including the White House spokesman and the wife of a former UK Prime Minister.[3]

Cross-Site Scripting attacks can be counteracted by validating externally accessed inputs and denying any unauthorized access through a Web Application Firewall.

[3] Source: http://edition.cnn.com/2010/TECH/social.media/09/21/twitter.security.flaw/

III. 2016 Web Attack Trend Analysis

2. Primary Attacker Trends



The graph above shows the distribution of web attacks, based on detection rules, of primary attacker IPs from all over the world which generated 30% of all attacks detected in 2016..

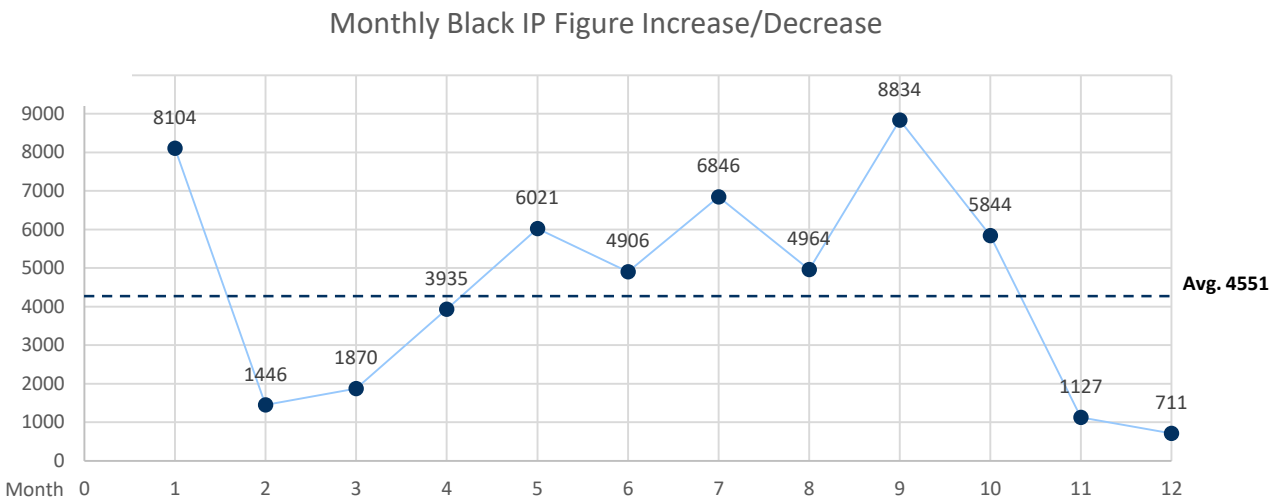
While the attacks from primary attackers in 2016 were conducted over the course of several days, the number of targets detected were in the single digits. In other words, there were many attacks of different types that honed in on specific targets. Primary attackers are likely professional hackers who, for monetary or political purposes, tend to carry out persistent attacks. Therefore it is important to analyze and respond to the attack trends of this particular group of attackers.

Primary attackers used SQL Injection (46%) attacks the most, followed by Cross-Site Scripting (30%), Stealth Commanding (19%), File upload (3%), and Directory Traversal (2%), in descending order of frequency.

Detection figures are not significantly different from those found in the previous section, "2016 Web Attack Trends by Rule." Following the overall attack trends, attacks corresponding to the SQL Injection and Cross-Site Scripting rules accounted for the highest percentage of attacks, which indicates that special attention should be paid to these rules.

III. 2016 Web Attack Trend Analysis

3. Black IP Fluctuation Trends



Penta Security Systems assigns a risk score to each attacker's IP according to the web attack threat level, taking into consideration the number of attacks per IP, the number of attacks per day, etc. IPs with a significantly high risk score are hereafter classified as Black IPs. The number of Black IPs detected each month throughout 2016 is shown in the graph above.

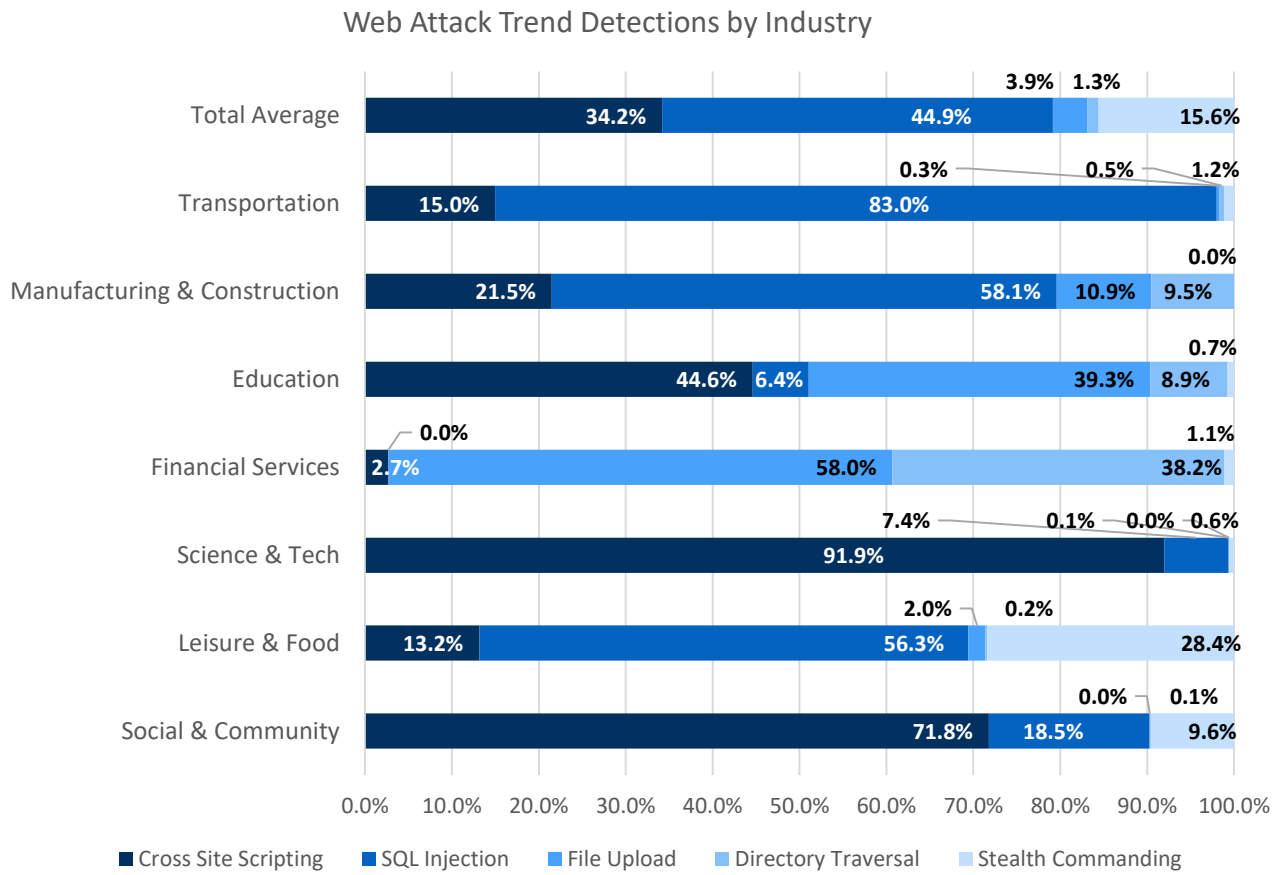
Since a single hacker can use multiple IPs, it is difficult to take the number of Black IPs as a direct indicator of the number of hackers attempting a web attack. However, by monitoring the increase or decrease in Black IPs, it is possible to gauge the attackers' scale of operation.

In 2016, the average number of Black IPs per month was 4551– a number higher than what the analyst team expected to see, and therefore highlighting the extent of threat posed by web attackers. Specifically, high numbers of Black IPs were detected in the months of January (8104) and September (8834), although fewer Black IPs were detected in November (1127) and December (711).

Although there is a limit to establishing a relationship between specific events and the fluctuation in Black IP numbers, web attacks are generally understood to increase whenever an international political situation or disaster arises. In addition, the high number of Black IPs also reveals the dangerous situation faced by organizations with valuable information, of not knowing when and how they will become targets of attacks.

III. 2016 Web Attack Trend Analysis

4. Web Attack Trends by Industry



The graph above illustrates the distribution of attacks detected per rule for each industry. Unlike the overall attack trends, there are large differences in attacks for each industry. Therefore, it is necessary to prepare countermeasures to tackle the web attack trends specific to the industry.

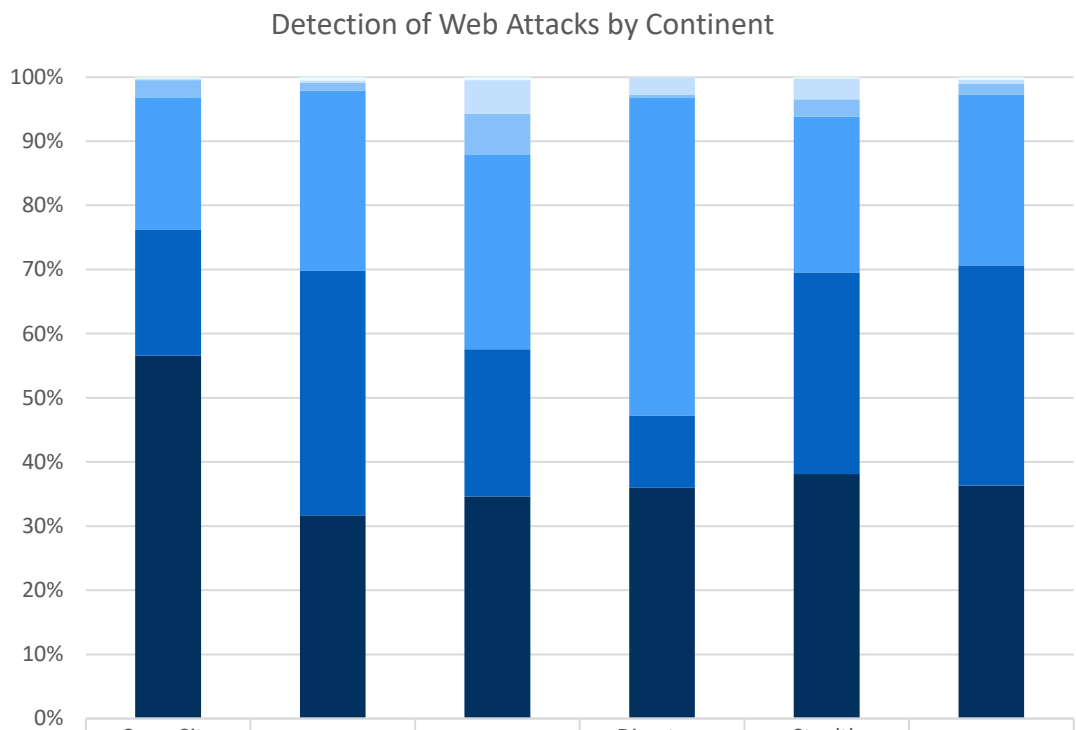
According to the chart, SQL Injection attacks account for the highest percentage in the Transportation, Manufacturing & Construction and Leisure & Food industries. The websites of these industries tend to handle large amounts of customer data. Therefore, it can be deduced that many attempts are made to seize customer data from the databases of these websites. These industries are advised to pay special attention to securing customer data.

Cross-Site Scripting attacks account for the highest percentage in the fields of Science & Tech and Social & Community. Administration of websites belonging to this field tend to be relatively lax, and therefore many attacks can be expected to target the individual PCs and terminals that access these websites. By exploiting vulnerabilities in the web browser, PCs and terminals can be targeted, and even maliciously manipulated to launch attacks on other websites from their servers. Users that access the websites of these industries should take special caution in securing their PCs and terminals.

File Upload attacks make up a significantly higher proportion of attacks detected within the Financial Services and Education industries than the average across all industries. Often with File Upload attacks, which involve the uploading of malicious files, attackers attempt to either gain server system privileges or distribute malicious files to users' PC and terminal via the website. The payload of these kinds of files can be critically damaging and as such, website owners and their security administrators need to take special care to guard against this and maintain the management system.

III. 2016 Web Attack Trend Analysis

5. Web Attack Trends by Continent



	Cross Site Scripting	SQL Injection	File Upload	Directory Traversal	Stealth Commanding	Total Percentage
Oceania	0.2%	0.5%	0.5%	0.0%	0.2%	0.4%
Africa	0.3%	0.4%	5.2%	2.7%	3.2%	0.6%
South America	2.7%	1.2%	6.5%	0.4%	2.7%	1.6%
North America	20.6%	28.1%	30.2%	49.6%	24.3%	26.6%
Europe	19.6%	38.1%	23.0%	11.3%	31.4%	34.4%
Asia	56.6%	31.7%	34.6%	36.0%	38.1%	36.3%

In the graph above illustrating the distribution of the source of detected attacks, data is classified by continent of origin.

As a whole, attacks that started in Asia and Europe accounted for the highest percentage of attacks, at 36.3% and 34.4% respectively of all attacks. North America, primarily the United States and Canada, accounted for 26.6% of attacks while South America, Africa and Oceania accounted for a relatively small percentage of attacks, at 1.6%, 0.6% and 0.4% respectively.

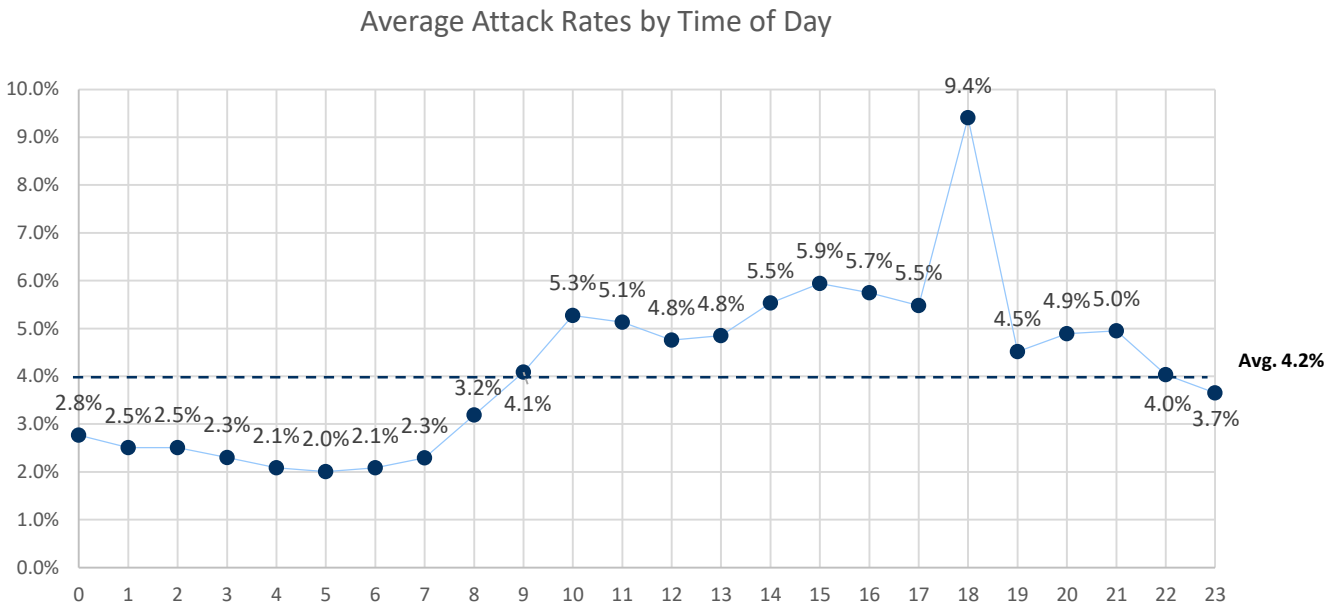
A high percentage of all Cross-Site Scripting attacks originated from Asia at 56.6%, and analysts reported that this may be because endpoint users in the region are more likely to utilize sites that have unsanitized input fields for scripts.

Additionally, within the overall attack trends, Directory Traversal attacks in particular stood out, as almost half of all these attacks originated from North America at 49.6%. However, because Directory Traversal attacks can be initiated by even amateur hackers through automated hacking tools, hacking attempts from this region may not always be attacking with criminal intent, but possibly for entertainment or even white-hacking/assessment purposes.

It is therefore necessary to address aspects of these continental attack trends when strengthening security policies.

III. 2016 Web Attack Trend Analysis

6. Web Attack Trends by Time of Day



The graph above shows what time of day attacks tend to occur. Data was collected from attacks within a period of one year based on local time.

According to internal analysis, attackers utilized automated tools to carry out hundreds of thousands of unsophisticated attacks on a massive scale. As can be seen, sizeable attacks are taking place at all times.

In particular, between the hours of 19:00 and 23:59, the average attack rate was 3.5% or more per hour, suggesting that it is necessary to pay attention to security beyond the typical working hours.

Specifically, the occurrence of attacks at certain times could be part of attackers' specific intentions. For example, 9.4% of attacks occurred between 18:00 and 19:00, which is more than twice the average. This phenomenon can be attributed to the fact that right at the end of the work day is a window of time in which security defense tends to be most neglected. During these times, it is crucial to consistently monitor and respond to attacks because ending the workday involves a flurry of activity, such as leaving the office or having dinner, thereby often coinciding with a lax in proper security defenses.

IV. APPENDIX

1. Data Compilation Target and Time Period

This data is based on log analyses from January 1, 2016 through December 31, 2016 for WAPPLES, the leading WAF in the Asia-Pacific region.

2. Key Differences from Previous Reports

This report is based on the ICS Report published up till 2015, which utilized only the true positive logs of WAPPLES' detection rules collected on the ICS server. In order to extend the report to not only the customers who use WAPPLES, but also security administrators of various companies and organizations, the region and time trends for occurrence were included in the report. In the future, Penta Security Systems plans to publish trend reports annually based on these contents so that they may be utilized as a comparative tool for annual data trends .

3. Definition of Technical Terms

▪ Cross-Site Scripting (XSS)

An attack technique that allows users to perform undesirable actions by inserting malicious scripts into forums, web mail, etc. In WAPPLES, it is classified as a "High" level risk and is also classified as "Cross-Site Request Forgery" in the OWASP Top 10.

▪ SQL Injection

An attack technique that can attack a database by manipulating the input value of the client with a technique of code injection and execution of an unintended SQL statement. WAPPLES classifies it as a "Serious" level risk because it is an attack technique that can cause a large amount of information leakage. It is classified under the "Injection" category in the OWASP Top 10.

▪ File Upload

An attack technique that allows a hacker to access the homepage after uploading a malicious program, allowing remote execution of system operating commands on the server computer. In WAPPLES it is classified as a "High" level risk. It is classified under the "Security Misconfiguration" category in the OWASP Top 10.

▪ Directory Traversal

An attack technique aimed at accessing files or directories outside of administrator control. In WAPPLES, it is classified as a "Normal" level risk and is classified as "Missing Function Level Access Control"' in the OWASP Top 10.

▪ Stealth Commanding

An attack technique that obtains information by attaching a server side script to an input to execute malicious commands. In WAPPLES, it is classified as a "Serious" level risk and is classified under the "Injection" category of the OWASP Top 10.

IV. APPENDIX

4. Black IP List

순위	공격지 IP	국가	위험도
1	221.229.x.x	China	98.0275
2	107.167.x.x	United States	97.9384
3	62.210.x.x	France	97.0522
4	195.154.x.x	France	96.5139
5	195.22.x.x	Poland	94.7279
6	124.243.x.x	Korea	94.1236
7	115.159.x.x	China	94.0112
8	146.185.x.x	Russian Federation	93.1569
9	180.97.x.x	China	92.6763
10	103.231.x.x	Hong Kong	92.4970
11	195.154.x.x	France	92.3385
12	211.235.x.x	Korea	92.2461
13	178.217.x.x	Poland	92.2412
14	103.36.x.x	Hong Kong	92.0852
15	213.179.x.x	United Kingdom	92.0187
16	62.210.x.x	France	92.0073
17	83.168.x.x	Sweden	91.9342
18	211.189.x.x	Korea	91.5459
19	211.149.x.x	China	91.1361
20	105.178.x.x	Rwanda	90.9338
21	74.208.x.x	United States	90.8974
22	37.59.x.x	France	90.5794
23	61.160.x.x	China	90.3571
24	223.62.x.x	Korea	90.2672
25	27.101.x.x	Korea	90.2309
26	73.179.x.x	United States	90.2192
27	58.87.x.x	Korea	90.1969
28	223.62.x.x	Korea	90.1898
29	223.62.x.x	Korea	90.1835
30	166.125.x.x	Korea	90.1424
31	62.210.x.x	France	90.0243
32	223.62.x.x	Korea	89.9989
33	223.62.x.x	Korea	89.9536
34	195.154.x.x	France	89.9515
35	58.227.x.x	Korea	89.8985
36	223.62.x.x	Korea	89.8978
37	40.77.x.x	United States	89.6961
38	223.62.x.x	Korea	89.6267
39	223.62.x.x	Korea	89.5339
40	223.62.x.x	Korea	89.4588
41	223.62.x.x	Korea	89.4504
42	136.243.x.x	Germany	89.3752
43	223.62.x.x	Korea	89.2625
44	89.163.x.x	Germany	89.2458
45	185.14.x.x	Ukraine	89.2198
46	178.202.x.x	Germany	89.2156
47	223.62.x.x	Korea	89.1977
48	223.62.x.x	Korea	89.1935
49	223.62.x.x	Korea	89.1893
50	210.125.x.x	Korea	89.1883

t h a n k y o u

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

Contact E-mail WATT@pentasecurity.com