SOC Report

1.1 Data Analytics Platform Innovation

Since fiscal 2016, IIJ has been working on bolstering its security business from the perspective of human resources, systems, and operations to provide better services to customers. One of the efforts to strengthen our systems is the innovation of our Data Analytics Platform for the comprehensive analysis of security-related information. The Data Analytics Platform aims to cope with increasingly sophisticated cyber attacks by detecting malicious malware activity and other threats through a multifaceted approach to analyzing data. such as IIJ service logs. This enables us to implement preventative measures and post-incident handling for security threats appropriately.

Use of the Data Analytics Platform will make it possible to identify sophisticated cyber attacks that until now have been difficult to detect at an early stage. Here, we will discuss three features of the Data Analytics Platform: (1) Data collection and analysis as an ISP, (2) Data obtained through corporate activities, and (3) Analysis using IIJ's unique big data infrastructure.

■ (1) Data Collection and Analysis as an ISP

In addition to compromising devices by exploiting vulnerabilities, attackers also attempt to launch successful attacks by tricking users into making mistakes. For this reason, it may not be possible to detect cyber attacks using a single security device. Defense in depth using different security devices is an effective way to cope with increasingly complex cyber attacks. Likewise, multi-layer detection equipment provides a robust method for detecting cyber attacks. The Data Analytics Platform performs multifaceted analysis of various logs to detect cyber attacks. The logs collected and analyzed naturally include those from security devices such as firewalls, IPS/IDS, and anti-virus solutions provided as IIJ services, along with those from Web access and incoming/outgoing email. Furthermore, as an ISP we are in the unique position of being able to include logs from backbone traffic and DNS queries in the analysis data. By collecting and analyzing a wide range of logs, we can detect the malicious activity of malware that was previously difficult to uncover.

■ (2) Data Obtained Through Actual Corporate Activities

The Data Analytics Platform detects cyber attacks by utilizing logs from IIJ services, in addition to data from sources such as honeypots and crawlers. IIJ services are used in business activities of companies, so we can utilize data on cyber attacks encountered during these activities. For example, we can gather and analyze logs from the IIJ Secure Web Gateway Service and IIJ Secure MX Service related to user activities for over a million corporate accounts in Japan, including Web access, email, and anti-virus scan result logs. Collecting and analyzing these data enables us to take a close look at the campaign trends of targeted attacks against Japan, or attacks against an unspecified number of users.

■ (3) Analysis Using IIJ's Unique Big Data Infrastructure

Sophisticated cyber attacks can lead to the concealment of malware that continues to exfiltrate confidential data without being discovered by the targeted organization. Even if you are initially unable to avoid being compromised by a 0-Day attack, the speed with which you discover it can determine whether you suffer damages. Figure 1 shows an overview of the Data Analytics Platform architecture. The Data Analytics Platform is constructed as IIJ's own big data infrastructure, based on the open source Hadoop framework. This unique infrastructure makes it possible to separate over hundreds of thousands of logs per second into logical field and value groups, so they can be analyzed in a database using a multifaceted approach. It also enables analysis results to be obtained with sufficient speed when analyzing logs in database form. Furthermore, the architecture is built to allow the expansion

© Internet Initiative Japan Inc.

of imported data types and improvements to performance, so it can cope with cyber attacks that continue to become more sophisticated and complex. The Data Analytics Platform makes it possible to identify from a vast amount of data, the malicious activity of threats such as malware at an early stage.

There are various options for output, including reputation information such as a blacklist of C&C servers, and attack observation data. We began posting the attack observation data output on our wizSafe Security Signal*1 security information site from October 2017.

The wizSafe Security Signal publishes periodic observation data each month, while also providing timely security information in blog form.

The following sections discuss the activities that were discovered using the Data Analytics Platform, based on the details reported in the wizSafe Security Signal over the past six months. Of note was a cryptocurrency mining service, DDoS attacks, and attacks targeting vulnerabilities in Apache Struts 2.

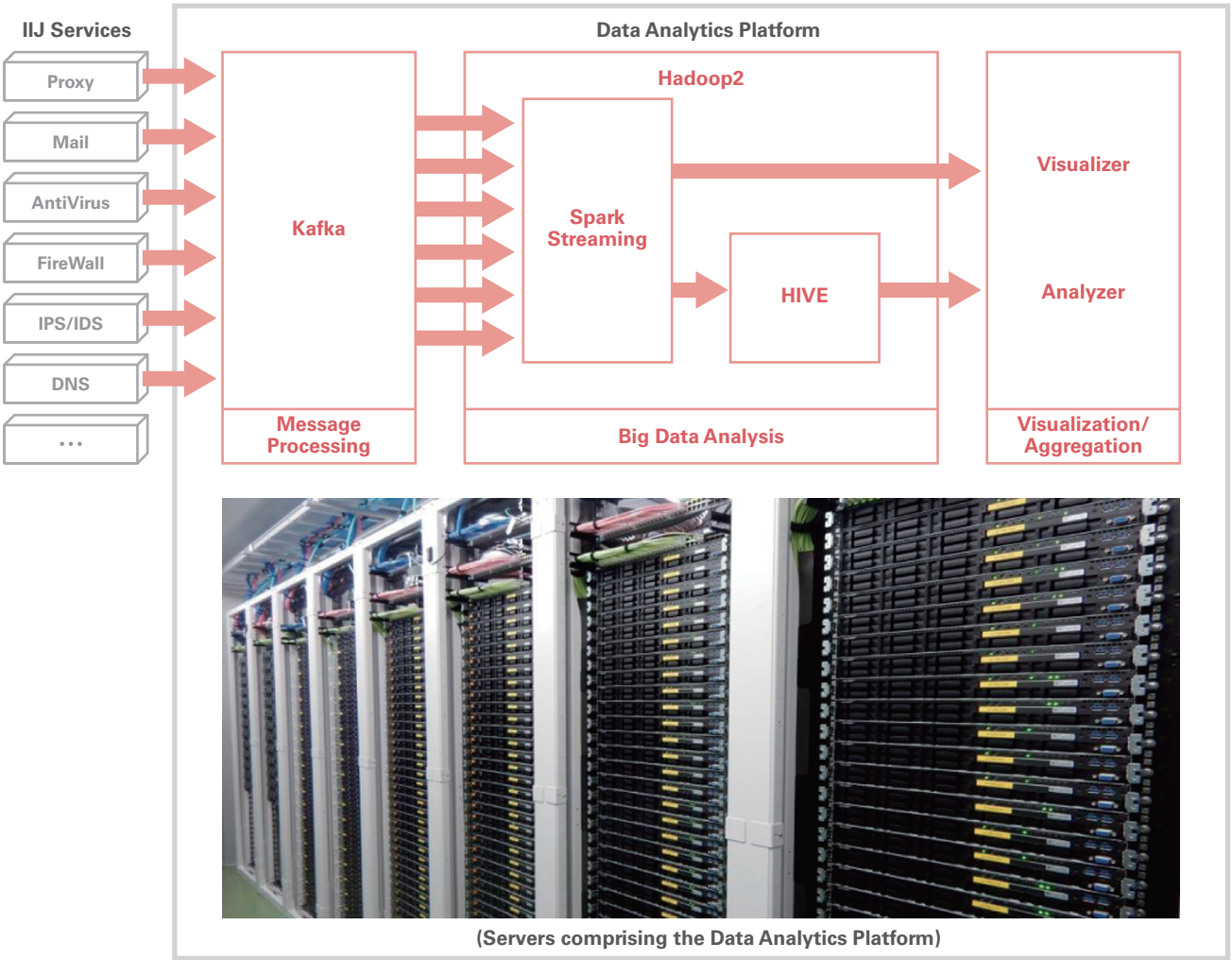

Figure 1: Overview of Data Analytics Platform Architecture

*1 wizSafe Security Signal - Milestones for Security and Safety (https://wizsafe.iij.ad.jp/) (in Japanese).

© Internet Initiative Japan Inc.

1.2 Cryptocurrency Mining Services

2017 was also a year where the sharp rise in the price of virtual currencies such as Bitcoin gained considerable attention. For example, the value of Bitcoin increased by about 20 times over the course of the year. Since a few years ago, virtual currencies such as Bitcoin have been used in ransomware demands due to their convenience and the anonymity they provide when sending and receiving them. For example, the Cryptlocker ransomware discovered in 2013 requested Bitcoin as one of the ransom payment methods. Many ransomware attacks demand ransom payments in cryptocurrency, but other than its use in financial transactions, some malware also performs fraudulent mining of said currency. There has also been an incident*2 where malware-infected devices form a botnet that mines for cryptocurrencies.

On September 14, 2017, a cryptocurrency mining service called Coinhive was launched. Coinhive is a service that enables the mining of a cryptocurrency called Monero using JavaScript. A website operator embeds the mining JavaScript in their site to induce mining of the Monero cryptocurrency using the CPU resources of website visitors' PCs. Under the Coinhive system, 70% of mining revenue is distributed to website operators. With cryptocurrency prices skyrocketing, more and more website operators are using the Coinhive service as a revenue source in place of Web advertisements. This kind of cryptocurrency mining service existed before, but since Coinhive's inception, a string of similar services using JavaScript such as Cloudcoins and Coinlab have appeared in quick succession.

Meanwhile, there have also been cases*3 where attackers have adopted cryptocurrency mining services that use JavaScript.

An attacker can obtain revenue from cryptocurrency mined on the PC of a website viewer by modifying the website and embedding JavaScript for mining. Some mining JavaScript consumes a lot of CPU resources, and there are concerns that this could affect the remaining battery life of notebook PCs or smartphones. This demonstrates that cases involving the fraudulent use of cryptocurrency mining services are on the rise, and some anti-virus software now treat JavaScript for mining as a risk and blocks it.

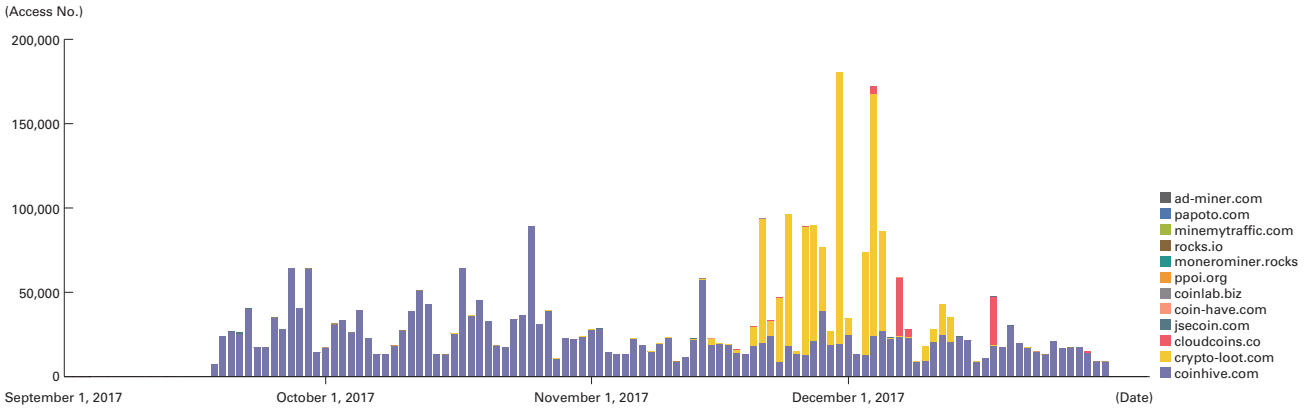

Figure 2: Access to Cryptocurrency Mining Services in 2nd Half of 2017

*2 Kaspersky Lab Daily, "Got any hidden miners? I wouldn't be so sure..." (https://www.kaspersky.com/blog/hidden-miners-botnet-threat/18488/).
*3 wizSafe Security Signal, "Cases of Cryptocurrency Mining Scripts Embedded Through Website Alteration" (https://wizsafe.iij.ad.jp/2017/10/94/) (in Japanese).

© Internet Initiative Japan Inc.

Figure 2 shows access numbers for the cryptocurrency mining service observed over the IIJ Secure Web Gateway Service since September 2017, when the Coinhive service launched. We can see that there are an increasing number of different cryptocurrency mining services, and access numbers for these services climbed until early December. Because this data is from the website access of enterprise users, access numbers are relatively low on Saturdays and Sundays, public holidays, and at the end of the year when corporate users were not active.

Whether the use of cryptocurrency mining services remains appealing in the future will depend on how the prices for cryptocurrencies change. The ease of using these services will also be affected by the risk assessment of JavaScript for cryptocurrency mining services by website viewers. For example, the operator of a legitimate website would not want to embed JavaScript that is blocked by anti-virus software on the PC of website visitors.

Cryptocurrency prices and security vendor trends also affect the ability of attackers to use cryptocurrency mining services. If the use of cryptocurrency mining services loses its appeal, attackers will likely look for other ways to obtain money.

1.3 DDoS Attacks

During the second half of 2017 (July to December), IIJ observed an average of 20.8 DDoS attacks per day and 638 DDoS attacks per month, totaling 3,828 attacks overall. Figure 3 shows the number of DDoS attacks that occurred in the second half of 2017. Because September contains dates such as September 18 when the Manchurian Incident started, we took precautions against the occurrence of many DDoS attacks, but we observed no related attacks to this in 2017. DDoS attacks have become a daily occurrence, and we believe fluctuations in the number that take place on a given day are affected less and less by specific time periods.

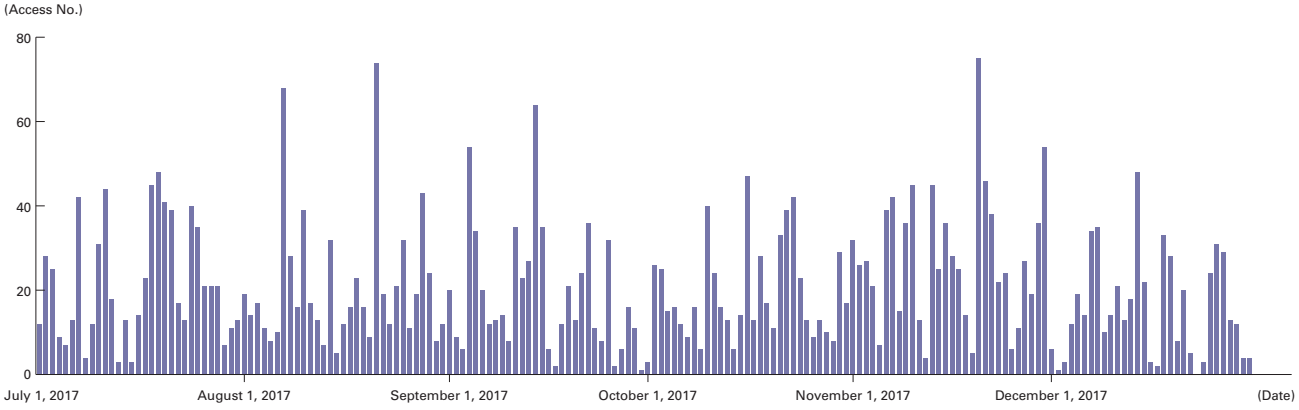

Figure 3: Trends in DDoS Attacks in 2nd Half of 2017

© Internet Initiative Japan Inc.

The largest DDoS attack observed during the survey period was observed in October 2017 and generated 16.55 Gbps of traffic using up to 1.79 million pps packets. The main attack technique used was a UDP flood, which causes line congestion. The longest sustained attack was a DDoS attack observed in September 2017 that continued for 46 hours 57 minutes. This attack mainly used the ICMP protocol. Table 1 shows the number of DDoS attacks that occurred each month in the second half of 2017, along with the largest and longest attacks and the methods used for each.

Threatening emails demanding the payment of money continued to be distributed during this observation period. In some cases, a small DDoS attack was carried out before threatening to launch a larger one. Since around December 2017, there were multiple incidents where notice of DDoS attacks was provided on Twitter with targets specified in Japanese. These were followed by multiple DDoS attacks being launched against the targeted websites, causing a denial of service. Targets included the websites of government and municipal offices.

There are various types of DDoS attacks, such as those aimed at monetary theft, and those carried out as hacktivist activity. However, in each case, attacks are usually intended to cause a big impact on business. Figure 4 shows the occurrence rates for DDoS attacks by day and time period. There were fewer attacks at night and on weekends than in the daytime and on weekdays. Business hours from 7:00 to 13:00 had more than triple the occurrence rate of the early morning hours of 1:00 to 7:00. There was also a difference of more than three times the number of incidents, when comparing Saturday and Monday.

Table 1: Max DDoS Attack Scale / Length in 2nd Half of 2017

Month / Year	Incidents	Max Attack Scale / Method		Max Attack Length / Method	
July 2017	673	17.86 Gbps	NTP Amplification	5 hrs 18 mins	IP Fragmentation/UDP
August 2017	655	10.16 Gbps	IP Fragmentation/UDP	16 hrs 43 mins	Flood
September 2017	575	12.06 Gbps	NTP Amplification	46 hrs 57 mins	ICMP
October 2017	593	16.55 Gbps	UDP Flood	24 hrs 9 mins	IP Fragmentation/UDP
November 2017	843	8.93 Gbps	IP Fragmentation/UDP	6 hrs 23 mins	UDP Flood
December 2017	489	13.39 Gbps	DNS Amplification	14 hrs 22 mins	ICMP/DNS Amplification

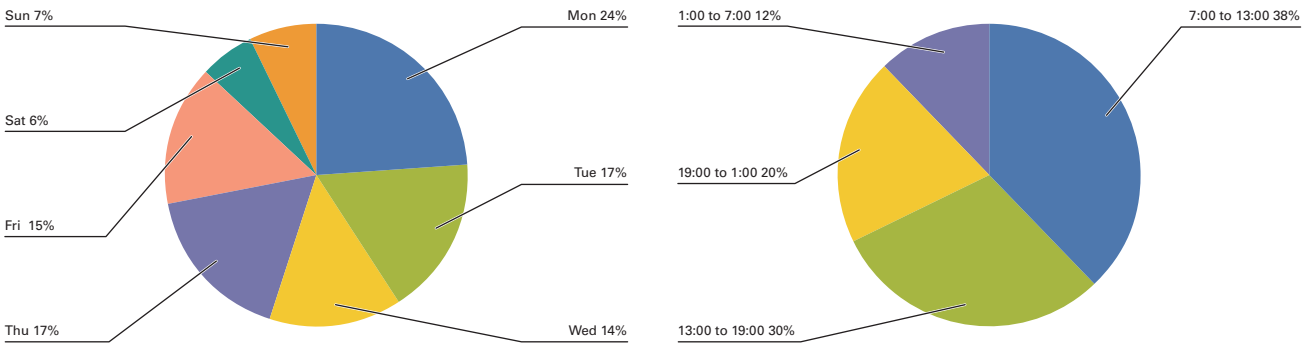

Figure 4: DDoS Attacks by Day / Time of Day

© Internet Initiative Japan Inc.

1.4 Attacks Targeting Struts 2 Vulnerabilities

In 2017, attacks targeting critical vulnerabilities in Apache Struts 2 occurred frequently. As shown in Table 2, six vulnerabilities disclosed for Apache Struts 2 in 2017 possibly allowed remote command execution.

Of these vulnerabilities, CVE-2017-5638 (S2-045/S2-046) disclosed in March 2017 could be exploited in attacks relatively easy. Because the environmental requirements for attack targets were comparatively loose, unless a security patch was applied, the success rate for an attack was extremely high. As a result, there was a rash of cyber attacks that led to damages such as information leaks immediately after the vulnerability was disclosed. Table 3 provides examples of security incidents where Apache Struts 2

Table 2: Remote Command Execution Vulnerabilities in Apache Struts 2 (2017)

Bulletin#	Description	CVE#	CVSS v3 Base Score
S2-045	Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.	CVE-2017-5638	10 Critical
S2-046	Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)	CVE-2017-5638	10 Critical
S2-048	Possible RCE in the Struts Showcase app in the Struts 1 plugin example in Struts 2.3.x series	CVE-2017-9791	9.8 Critical
S2-052	Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads	CVE-2017-9805	8.1 High
S2-053	A possible Remote Code Execution attack when using an unintentional expression in Freemarker tag instead of string literals	CVE-2017-12611	9.8 Critical
S2-055	A RCE vulnerability in the Jackson JSON library	CVE-2017-7525	8.1 High

Table 3: Examples of Security Incidents Targeting Struts 2

Month/Year Disclosed	Incident Overview
March 2017	Leak of 676,290 pieces of information from a credit card payment site for metropolitan tax*4
April 2017	Leak of up to 23,000 pieces of information from a map data site*5
May 2017	Unauthorized access to a public server at the National Institute of Information and Communications Technology (NICT)*6
June 2017	Leak of up to 4,335 pieces of information from the Land General Information System*7
September 2017	Leak of information on up to 143 million individuals from Equifax*8

*4 Tokyo Metropolitan Government, "Unauthorized access to credit card payment site for metropolitan tax" (http://www.metro.tokyo.jp/tosei/hodohappyo/press/2017/03/13/02.html) (in Japanese).
*5 Ministry of Internal Affairs and Communications, "Unauthorized access to map-based small-area analysis (jSTAT MAP)" (http://www.soumu.go.jp/menu_news/s-news/01toukei09_01000023.html) (in Japanese).
*6 National Institute of Information and Communications Technology, "Unauthorized access exploiting Apache Struts 2 vulnerability" (https://www.nict.go.jp/info/topics/2017/05/170502-1.html) (in Japanese).
*7 Ministry of Land, Infrastructure, Transport and Tourism, "About the possibility of unauthorized access and information leaks in the Land General Information System" (http://www.mlit.go.jp/report/press/totikensangyo05_hh_000129.html) (in Japanese).
*8 Equifax, "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes" (https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832).

© Internet Initiative Japan Inc.

vulnerabilities were exploited. It has been revealed that the CVE-2017-5638 (S2-045/S2-046) vulnerability was exploited in some incidents. Equifax, a major credit information company in the United States, also announced a leak of personal information caused by CVE-2017-5638 (S2-045/S2-046) in September 2017. It is thought that this incident could have resulted in the leak of the personal information of 143 million customers in the United States, Canada, and the UK.

Figure 5 shows the number of attacks per site that exploited Apache Struts 2 vulnerabilities observed by IIJ in the second half of 2017 (July to December). We can see that attacks against CVE-2017-5638 (S2-045/S2-046) disclosed in March 2017 account for the majority. Some attacks targeting CVE-2017-5638 (S2-045/S2-046) are estimated to be large-scale explorative attacks made with the same tool using a botnet. The rapid increase in incidents*9 from October 20, 2017, is due to these attacks.

It has already been more than six months since CVE-2017-5638 (S2-045/S2-046) was disclosed, but there are still many attack targets on the Internet that can be exploited, and attackers still have their sights set on these Web servers.

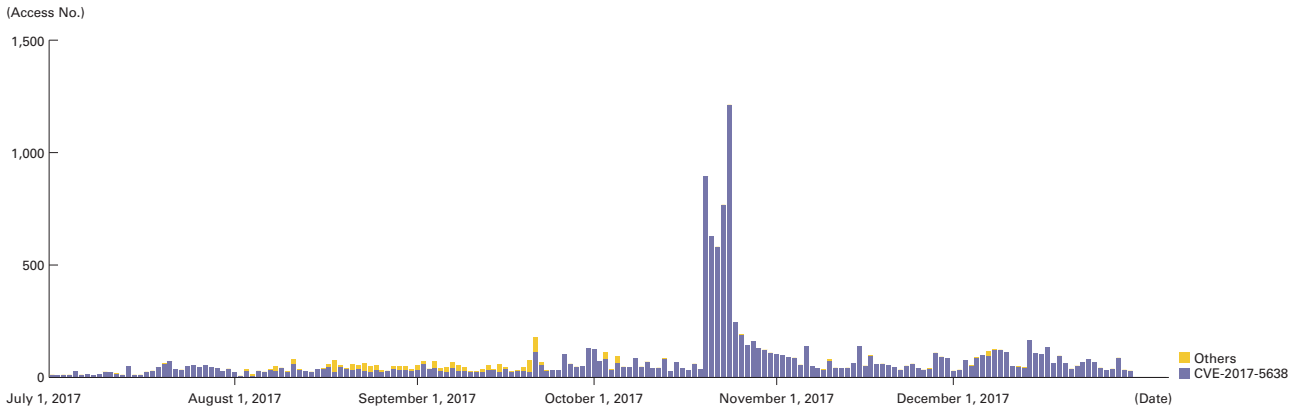

Figure 5: Attacks Per Site Targeting Apache Struts 2 in 2nd Half of 2017

*9 wizSafe Security Signal, "Observations of Attacks Targeting Apache Struts 2 Vulnerabilities" (https://wizsafe.iij.ad.jp/2017/11/106/) (in Japanese).

© Internet Initiative Japan Inc.

Apache Struts 2 is used as a Web application framework in various websites. Websites that did not apply Apache Struts 2 security patches properly were affected by attacks. Apache Struts 2 was the target of many attacks in 2017, but all servers and software that can be accessed via the Internet are considered potential targets by attackers. If even a single server or software vulnerability is not properly managed, it could lead to damages such as information leaks. It is essential to regularly review whether proper vulnerability management is being performed, regardless of whether Apache Struts 2 is used.

1.5 Conclusion

In this report, we looked at some of the results of long-term ongoing analysis of trends in cyber attacks utilizing the Data Analytics Platform. We have only scratched the surface of what the new Data Analytics Platform is capable of. Going forward, IIJ will continue to increase the type and amount of data incorporated and introduce new analytical techniques such as machine learning and AI, so we can take immediate action against sophisticated cyber attacks.

Author:
Kiyoshi Saito
General Manager, Security Business Department, Advanced Security Division, IIJ
As Director of the Security Business Department, Mr. Saito is engaged in the operation, implementation, and support of managed security services, as well as security consulting, SI, SOC integration, and business development.

Author:
Tsutomu Nakajima
Deputy Manager, Security Operations Center, Security Business Department, Advanced Security Division, IIJ
Mr. Nakajima leads a team of security analysts as Deputy Director of the SOC. He is also engaged in big data analysis work as an analyst himself, including incident analysis and the creation of security intelligence.

© Internet Initiative Japan Inc.