Hardening Windows Clients Against Malware Infections

1.1 Introduction

This report is a summary of incidents that IIJ responded to, based on information obtained by IIJ for the purpose of operating a stable Internet, information obtained from observed incidents, information obtained through our services, and information obtained from companies and organizations that IIJ has cooperative relationships with. This volume covers the period of time from April 1 through June 30, 2016. In this period a number of hacktivism-based attacks were once again carried out by Anonymous and other groups. A large number of DDoS attacks occurred, along with information leaks and website defacements. Information leaks caused by targeted attacks also occurred both in Japan and overseas. It has been announced that approximately 6.97 million pieces of personal information may have leaked in an incident at a major travel agency in Japan. It also came to light that a large volume of password information had leaked in the past from sources such as major SNS services, and multiple attacks seeming to use this information have been observed. As shown here, many security-related incidents continue to occur across the Internet.

1.2 Incident Summary

Here, we discuss incidents handled and responded to by IIJ, between April 1 and June 30, 2016. Figure 1 shows the distribution of incidents handled during this period*1.

■ Activities of Anonymous and Other Hacktivist Groups

Attack activities by hacktivists such as Anonymous continued during this period. In correspondence with various events and assertions, DDoS attacks and information leaks targeted various companies and government-related sites.

As a protest against the drive hunting of dolphins and small whales in Japan, there have been intermittent DDoS attacks since last September which are believed to be performed by Anonymous. Various domestic sites have continued to be affected by similar damages during this time period as well (OpKillingBay/OpWhales/OpSeaWorld). Since April, however, the number of such attacks targeting Japan has dropped significantly. The reasons for this are not clear, but one possibility is that the attackers have lost interest and moved on to other attack campaigns. That said, this doesn't necessarily mean the attacks are over, since other attackers may continue the attack campaigns in the future. In any case, the attack activities of hacktivist groups like Anonymous are such that it is difficult to determine whether a series of attack campaigns has ended or will continue. Thus, instead of responding when an attack campaign begins, you should always be prepared and be able to respond whenever an attack occurs.

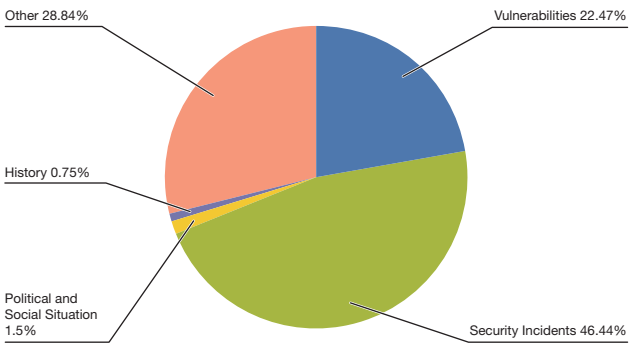


Figure 1: Incident Ratio by Category (April 1 to June 30, 2016)

Anonymous began an attack campaign named Oplcarus that targeted major financial institutions around the world in January 2016, and these attacks have continued intermittently. This came to prominence again in May, when the Bank of Greece and a large number of other financial institutions in countries such as Cyprus, France, and the Philippines fell victim to these attacks. Then through June the scope of these attacks expanded to include even more financial institutions, with some financial institutions in Japan also listed as attack targets, but no observable damages have occurred.

*1 Incidents in this report are split into five categories: vulnerabilities, political and social situations, history, security incidents or other.
Vulnerabilities: Responses to vulnerabilities in network equipment, server equipment or software commonly used across the Internet or in user environments.
Political and Social Situations: Responses to attacks stemming from international conferences attended by VIPs and international conflicts, and other related domestic and foreign circumstances and international events.
History: Warnings/alarms, detection and response to incidents for attacks that occur on the day of a historically significant date that have a close connection to a past event.
Security Incidents: Unexpected incidents and related responses such as wide spreading of network worms and other malware; DDoS attacks against certain websites.
Other: Security-related information, and incidents not directly associated with security problems, including high traffic volume associated with a notable event.

One big issue was internal data being disclosed on the internet related to the compromises at Gamma International in August 2014 and HackingTeam in July 2015. These companies develop the FinFisher and RCS surveillance software, respectively. In April 2016, the anonymous hacker Phineas Fisher*2, who was responsible for these attacks, disclosed the details of the techniques used to breach HackingTeam. Another disclosure was a video on YouTube in May showing the compromise of a Catalan police organization website. It was also revealed that Bitcoins worth 10,000 euros were stolen from a certain bank, and donated to a Kurdish group active in the Rojava region during the same time period. He (or she) is justifying this behavior by claiming that disclosing information stolen from companies and stealing money from banks is a form of "Ethical Hacking," and will result in improving the security of computers used by the general public. On the other hand, in interviews they stated that these actions are "for the lulz," so it could be said that there are elements similar to the activities of groups such as LulzSec, which created a storm of controversy in 2011. Currently it appears they are acting alone, but due to the impact of the incidents they have been responsible for in the past, we will continue to keep a close eye on future developments.

■ Vulnerabilities and Responses

During this period many fixes were released for Microsoft's Windows*3*4*5*6*7*8*9*10, Internet Explorer*11*12*13, Edge*14*15*16, and Office*17*18*19. Updates were also released for Adobe Systems' Flash Player, Acrobat, and Reader. A quarterly update was provided for Oracle's Java SE, fixing many vulnerabilities. Several of these vulnerabilities were exploited in the wild before patches were released.

In server applications, a quarterly update was released by Oracle, fixing many vulnerabilities in the Oracle database server and many other Oracle products.

A researcher showed that a practical attack against AES-GCM for TLS is possible when the Initialization Vector (IV) is reused. It was confirmed that some implementations, such as the IBM Domino Web server and Radware, were affected by this vulnerability and subsequently patched.

*2 "Hack Back! (@GammaGroupPR)" (https://twitter.com/GammaGroupPR).
*3 "Microsoft Security Bulletin MS16-039 - Critical: Security Update for Microsoft Graphics Component (3148522)" (https://technet.microsoft.com/en-us/library/security/MS16-039).
*4 "Microsoft Security Bulletin MS16-040 - Critical: Security Update for Microsoft XML Core Services (3148541)" (https://technet.microsoft.com/en-us/library/security/MS16-040).
*5 "Microsoft Security Bulletin MS16-053 - Critical: Cumulative Security Update for JScript and VBScript (3156764)" (https://technet.microsoft.com/en-us/library/security/MS16-053).
*6 "Microsoft Security Bulletin MS16-055 - Critical: Security Update for Microsoft Graphics Component (3156754)" (https://technet.microsoft.com/en-us/library/security/MS16-055).
*7 "Microsoft Security Bulletin MS16-056 - Critical: Security Update for Windows Journal (3156761)" (https://technet.microsoft.com/en-us/library/security/MS16-056).
*8 "Microsoft Security Bulletin MS16-057 - Critical: Security Update for Windows Shell (3156987)" (https://technet.microsoft.com/en-us/library/security/MS16-057).
*9 "Microsoft Security Bulletin MS16-069 - Critical: Cumulative Security Update for JScript and VBScript (3163640)" (https://technet.microsoft.com/en-us/library/security/MS16-069).
*10 "Microsoft Security Bulletin MS16-071 - Critical: Security Update for Microsoft Windows DNS Server (3164065)" (https://technet.microsoft.com/en-us/library/security/MS16-071).
*11 "Microsoft Security Bulletin MS16-037 - Critical: Cumulative Security Update for Internet Explorer (3148531)" (https://technet.microsoft.com/en-us/library/security/MS16-037).
*12 "Microsoft Security Bulletin MS16-051 - Critical: Cumulative Security Update for Internet Explorer (3155533)" (https://technet.microsoft.com/en-us/library/security/MS16-051).
*13 "Microsoft Security Bulletin MS16-063 - Critical: Cumulative Security Update for Internet Explorer (3163649)" (https://technet.microsoft.com/en-us/library/security/MS16-063).
*14 "Microsoft Security Bulletin MS16-038 - Critical: Cumulative Security Update for Microsoft Edge (3148532)" (https://technet.microsoft.com/en-us/library/security/MS16-038).
*15 "Microsoft Security Bulletin MS16-052 - Critical: Cumulative Security Update for Microsoft Edge (3155538)" (https://technet.microsoft.com/en-us/library/security/MS16-052).
*16 "Microsoft Security Bulletin MS16-068 - Critical: Cumulative Security Update for Microsoft Edge (3163656)" (https://technet.microsoft.com/en-us/library/security/MS16-068).
*17 "Microsoft Security Bulletin MS16-042 - Critical: Security Update for Microsoft Office (3148775)" (https://technet.microsoft.com/en-us/library/security/MS16-042).
*18 "Microsoft Security Bulletin MS16-054 - Critical: Security Update for Microsoft Office (3155544)" (https://technet.microsoft.com/en-us/library/security/MS16-054).
*19 "Microsoft Security Bulletin MS16-070 - Critical: Security Update for Microsoft Office (3163610)" (https://technet.microsoft.com/en-us/library/security/MS16-070).

April Incidents

1 **S** **1st: The website of NTT Corporation was targeted in a DDoS attack by Anonymous, causing it to be temporarily inaccessible (OpKillingBay).**

2 **S** **1st: It was discovered that incidents of unauthorized logins on the Mobage service provided by DeNA were due to identity fraud by third parties, and information on up to approximately 100,000 users may have been exposed.**

3 **S** **4th: A large number of internal documents exposing tax evasion at companies were leaked from Panamanian law firm Mossack Fonseca. The contents were disclosed to the public.**
Süddeutsche Zeitung, "Panama Papers: This is the leak" (http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/).

4

5 **S** **5th: The personal details of around 50 million Turkish citizens, amounting to two-thirds of the population, were leaked from a Turkish government agency and publicly disclosed.**

6 **V** **7th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb16-10.html).

7

8 **V** **12th: Multiple vulnerabilities were discovered in Windows and Samba, and patches were released for each.**
"Badlock Bug" (http://badlock.org/).

9 **V** **13th: Microsoft published their Security Bulletin Summary for April 2016, and released a total of thirteen updates, including six critical updates such as MS16-037, as well as seven important updates.**
"Microsoft Security Bulletin Summary for April 2016" (https://technet.microsoft.com/library/security/ms16-apr).

10

11 **V** **14th: Multiple heap buffer overflow vulnerabilities were found in Apple's QuickTime for Windows. However, Apple has ended support for the product, and no fixes were made.**
"Where to get answers about QuickTime 7 or QuickTime 7 Pro" (https://support.apple.com/en-us/HT201175).
"Apple Ends Support for QuickTime for Windows; New Vulnerabilities Announced" (https://www.us-cert.gov/ncas/alerts/TA16-105A).

12

13 **O** **15th: The "Bill on Partial Revisions to the Basic Act on Cyber Security and the Act on Facilitation of Information Processing" was approved by the Upper House. These revisions will establish a new qualification titled, "Information Processing Security Supporter".**

14 **V** **19th: Oracle released their quarterly scheduled update for multiple products including Java SE and Oracle Database Server, fixing a total of 136 vulnerabilities.**
"Oracle Critical Patch Update Advisory - April 2016" (http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html).

15

16 **S** **21st: It was discovered that unauthorized access had occurred at the website of Nippon Television Network Corporation, and personal information related to 430,000 individuals may have been leaked. The attacker exploited a zero-day vulnerability in Keitai Kit for Movable Type to perform an OS command injection attack.**
"Regarding the potential leak of personal information due to unauthorized access to our website" (http://www.ntv.co.jp/oshirase/index_20160421.html) (in Japanese).

17

18

19 **S** **22nd: A security researcher found that data on 93.4 million Mexican voters had been made publicly available online. This was caused by a MongoDB configuration error.**
"BREAKING: Massive Breach of Mexican Voter Data" (https://mackeeper.com/blog/post/217-breaking-massive-databreach-of-mexican-voter-data).

20

21 **S** **23rd: It was discovered that unauthorized access had occurred at the website of J-WAVE, Inc., and personal information related to 640,000 individuals may have been leaked. The attacker exploited a zero-day vulnerability in Keitai Kit for Movable Type to perform an OS command injection attack.**
"Notice regarding the potential leak of personal information due to unauthorized access to the J-WAVE website: J-WAVE 81.3 FM RADIO" (http://www.j-wave.co.jp/topics/1604_info.htm) (in Japanese). "Notice regarding the results of a special investigative committee investigation into the potential of personal information leaks due to unauthorized access: J-WAVE 81.3 FM RADIO" (http://www.j-wave.co.jp/topics/1606_info.htm) (in Japanese).

22

23

24 **S** **26th: A BAE Systems researcher reported there was a malware infection in the SWIFT payment system at the Bangladesh Bank that caused the illegal bank transaction incidents that occurred back in February. SWIFT also issued an alert to its customers.**

25

26 **V** **27th: A vulnerability (S2-032) in Apache Struts 2 that could allow arbitrary code execution when Dynamic Method Invocation (DMI) is enabled was discovered and fixed. The National Police Agency also issued an alert due to observations of this vulnerability being targeted in attacks.**
Apache Software Foundation, "S2-032" (https://struts.apache.org/docs/s2-032.html). National Police Agency, "Regarding observations of access targeting a vulnerability in Apache Struts 2" (https://www.npa.go.jp/cyberpolice/detect/pdf/20160427.pdf) (in Japanese).

27

28 **S** **27th: It was discovered that customer details, including credit card information may have leaked from NETSEA's "NETSEA" B2B wholesale platform site due to remote unauthorized access.**
"Apology regarding unauthorized access | NETSEA" (http://netsea.co.jp/press/20160427.php) (in Japanese).

29

30 **S** **29th: It was discovered that unauthorized access had occurred at the website of Eikoh Seminar, and personal information related to 2,761 individuals may have been leaked. The attacker exploited a zero-day vulnerability in Keitai Kit for Movable Type to perform an OS command injection attack.**
Eikoh Inc., "Apology and notice regarding the leak of customer information" (http://www.eikoh.co.jp/news/pdf/20160429.pdf) (in Japanese).

*Dates are in Japan Standard Time

Legend V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

Multiple vulnerabilities in the Apache Struts 2 Web application framework were discovered and fixed, including one (S2-032) that could allow arbitrary code execution when Dynamic Method Invocation (DMI) is enabled, and another (S2-037) that could allow arbitrary code execution when the REST plug-in is enabled. A vulnerability in the ImageMagick image processing software that could allow arbitrary OS commands to be executed when specially-crafted content is opened was discovered and fixed. Also, an OS command injection vulnerability in a plug-in for the Movable Type CMS was discovered and fixed. The affected plug-in is Keitai Kit for Movable Type, which is used to produce content for mobile phones. Attacks targeting these vulnerabilities were observed immediately after the release of fixed versions, and alerts were issued by JPCERT/CC and the National Police Agency. Notably, attacks targeting the vulnerability in Keitai Kit for Movable Type were ongoing prior to the developer releasing a fixed version, and leaks of personal information in large quantities occurred through multiple websites.

■ Information Leaks Due to Targeted Attacks

During this period there was once again a string of incidents both in Japan and overseas that involved malware infections on computers at organizations, as well as resulting information leaks. In June, it was announced that approximately 6.97 million pieces of personal information (including more than 4,000 valid passport numbers) may have leaked from a major travel agency in Japan. In this incident, an internal computer was infected with malware after a staff member received an email made to appear as if it was sent by a major client, in this case an airline company, and opened a file attached to this email. It is now known that the attacker then gradually expanded the scope of the intrusion to other internal computers and servers before creating data files that contained large quantities of personal information, and attempting to externally transmit these data files.

In addition to this, since mid-June there have been successive announcements by local authorities, such as city offices, where unauthorized communications with external parties had occurred after computers in their offices were infected with malware. It is not clear whether or not the series of incidents are connected, but the content of the attack emails sent to these local authorities seems to indicate that it is highly likely they were sent to a large number of unspecified organizations.

It was also found that unauthorized access by a third party in June targeting a system used by the Democratic National Committee (DNC) in the United States led to the leak of internal documents and other information related to the presidential primary elections. CrowdStrike, the security vendor that investigated this incident, determined that two different Russian attack groups called COZY BEAR (APT29) and FANCY BEAR (APT28) were responsible, and announced that they had compromised internal systems at the DNC as early as 2015. Prior to this, U.S. Director of National Intelligence (DNI) James Clapper had warned that cyber attacks were being conducted against multiple organizations in the United States connected to the presidential elections. It is also believed that the DNC compromise was part of Russian intelligence activity targeting systems related to political activities in the United States.

After this, a hacker calling themselves GUCCIFER 2.0 claimed to be responsible for the DNC compromise through their blog, and published documents they said were obtained from the DNC*20. GUCCIFER 2.0 has denied being connected to other Russian hacker groups, insisting that they acted alone on their blog and through the media. However, there are many puzzling details, so it is also possible that this could be a misdirection by Russia. Either way, these incidents underscore the extreme difficulty of attribution, or the identification of culprits behind cyber attacks. The importance of attribution has been pointed out in recent years.

■ Mass Password Information Leaks

During this period, a series of discoveries revealed that large quantities of password information had previously been leaked from services such as SNS. It is believed that these discoveries were related to data acquired through compromises perpetrated by Russian hacker groups between 2011 and 2013. The information leaks were discovered when the data began to be sold to the general public this year through Russian message boards and sites selling this information on the Dark Web. In each of these cases the scale of the leak was very extensive, including credentials for around 360 million MySpace accounts, around 167 million LinkedIn accounts, around 127 million Badoo accounts, around 100 million VK accounts, and around 65 million Tumblr accounts. Also, the MySpace and LinkedIn leaks included unsalted SHA-1 hashed password information. This makes it relatively easy to

*20 "GUCCIFER 2.0" (https://guccifer2.wordpress.com/).

May Incidents

1
- S **4th: The website of the Bank of Greece was targeted in a DDoS attack by Anonymous, causing it to be temporarily inaccessible (Oplcarus).**

2
3
- V **5th: A vulnerability in ImageMagick that could allow arbitrary OS commands to be executed when content is opened was discovered and fixed.**
"ImageMagick Security Issue - ImageMagick" (https://www.imagemagick.org/discourse-server/viewtopic.php?f=4&t=29588).
"ImageTragick" (https://imagetragick.com/).

4
- V **5th: Multiple vulnerabilities in Adobe Acrobat and Reader that could allow unauthorized termination and arbitrary code execution were discovered and fixed.**
"Security Updates Available for Adobe Acrobat and Reader" (https://helpx.adobe.com/security/products/acrobat/apsb16-14.html).

5
- V **11th: Microsoft published their Security Bulletin Summary for May 2016, and released a total of sixteen updates, including eight critical updates such as MS16-051, as well as eight important updates.**
"Microsoft Security Bulletin Summary for May 2016" (https://technet.microsoft.com/library/security/ms16-may).

6
7
- S **11th: It was discovered that unauthorized logins through identity fraud by third parties had taken place on the Ameba service run by CyberAgent, and information on 50,905 users may have been exposed.**
CyberAgent, Inc., "Notice regarding unauthorized logins to 'Ameba' and password reset request" (https://www.cyberagent.co.jp/newsinfo/press/detail/id=11977) (in Japanese).

8
9
- S **11th: A police report was forwarded to a prosecutor on potential charges for obstructing business by damaging a computer by a male student in the first year of high school, who has been suspected of launching a cyber attack against the website of the junior high school in Osaka he had attended.**

10
11
- V **12th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb16-15.html).

12
13
- S **13th: It was discovered that user email addresses and password information had leaked from Tumblr in early 2013. It was later confirmed that user information and credentials related to over 65 million users were being sold on Dark Web markets.**
"Tumblr Staff" (https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had).

14
15
16
- V **16th: Apple released iOS 9.3.2, OS X El Capitan 10.11.5, and Security Update 2016-003, fixing multiple vulnerabilities, including one that could allow an application to execute arbitrary code with kernel privileges. tvOS 9.2.1 and watchOS 2.2.1 were also released on the same day.**
"About the security content of iOS 9.3.2" (https://support.apple.com/en-us/HT206568). "About the security content of OS X El Capitan v10.11.5 and Security Update 2016-003" (https://support.apple.com/en-us/HT206567). "About the security content of tvOS 9.2.1" (https://support.apple.com/en-us/HT206564).
"About the security content of watchOS 2.2.1" (https://support.apple.com/en-us/HT206566).

17
18
- S **18th: The Tokyo Metropolitan Police Department arrested a male from Nagasaki on suspicion of violating the Unauthorized Computer Access Law. The charges are for unauthorized access to the SNS and cloud service accounts of entertainers and other individuals. Unauthorized logins were performed on services such as iCloud by guessing passwords based on names and birth dates, to view private images.**

19
- S **18th: DDoS attacks targeted DNS service provider NS1, affecting customer services such as Imgur.**
"A Note From NS1's CEO: How We Responded To Last Week's Major, Multi-Faceted DDoS Attacks" (https://ns1.com/blog/how-we-responded-to-last-weeks-major-multi-faceted-ddos-attacks).

20
21
- S **19th: It was discovered that the email addresses and passwords of around 167 million users had actually leaked from LinkedIn in 2012, rather than the approximately 6.5 million that was initially reported. It was also confirmed that account information was being sold on Dark Web markets.**
"Protecting Our Members | Official LinkedIn Blog" (https://blog.linkedin.com/2016/05/18/protecting-our-members).

22
23
- S **19th: The master key for the TeslaCrypt ransomware was suddenly released by the developers, and decryption tools were made available by security vendors.**
"ESET releases new decryptor for TeslaCrypt ransomware" (http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/).

24
25
- V **20th: A researcher revealed that a practical attack against AES-GCM for TLS is possible if the Initialization Vector (IV) is reused.**
"GitHub - nonce-disrespect / nonce-disrespect: Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS" (https://github.com/nonce-disrespect/nonce-disrespect).

26
27
- S **23rd: Approximately 1.44 billion yen in cash was illegally withdrawn from around 1,400 convenience store ATMs across 17 prefectures in Japan. Counterfeit cards that were created based on card information leaked from the Standard Bank in South Africa were used.**

28
29
- V **26th: A vulnerability in Cisco network products that could cause a DoS condition when specially-crafted IPv6 Neighbor Discovery (ND) packets are received was discovered. This vulnerability affected all versions of IOS, IOS XR, and IOS XE, among other products. Cisco is preparing to release fixed versions.**
"Cisco Products IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability" (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6).

30
31
- S **28th: It was discovered that email addresses and password information for about 360 million users who had created accounts prior to 2013 had leaked from MySpace. It was also confirmed that account information was being sold on Dark Web markets.**
"Myspace Blog" (https://myspace.com/pages/blog).

*Dates are in Japan Standard Time

Legend V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

crack the password, so there was a high risk that the data could be used for exploits right away. Because of this, a number of incidents thought to be related to these leaks have occurred.

In June, there were unauthorized logins by third parties at multiple services such as GitHub and GoToMyPC. These were list-based attacks that leveraged password information leaked from other websites, and targeted users that reuse the same password on multiple sites, and links have been identified with the aforementioned mass password information leaks.

There was also a series of hijackings starting in May that targeted the SNS accounts of notable public figures in the technology industry, such as Twitter co-founder Biz Stone, Facebook CEO Mark Zuckerberg, and Google CEO Sundar Pichai. A group calling themselves the OurMine Team have claimed responsibility for these hijackings. This series of account hijackings is thought to be one of the after effects of the aforementioned password information leaks.

Anticipating the damages that can be caused by such account hijackings that target users who reuse their passwords, some companies have started to preemptively address this issue. For example, Facebook, Amazon, and Netflix have analyzed user password information leaked from other services, and are forcing users to reset their password if they are found to have been using the same password on their service. Such measures began to be implemented after the leak of around 150 million password information records from Adobe in 2013. Although having users avoid reusing passwords across multiple services is a fundamental measure that prevents these kinds of hijackings, in reality, a large number of users reuse passwords, so in the current environment it will be difficult to eliminate such damages.

There are also websites that collect large quantities of leaked password information, and issue alerts to users. For example, security researcher Troy Hunt launched a free service, "Have I been pwned?," after the Adobe leaks in 2013*21. Users can search for their email address on this website to check whether or not their password information has been leaked. It also offers a service that sends you a notification when affected by information leaks in the future if you register your email address beforehand. However, one must exercise extreme caution when using such services, since some sites that claim to offer similar services are simply aimed at collecting information from users.

■ Government Agency Initiatives

The 42nd G7 Summit (the G7 Ise-Shima Summit) was held in late May 2016. Mainly through cooperation between government ministries and the private sector, there was a promotion of security initiatives to counter cyber attacks that may occur in relation to the summit taking place. As a result, there were no incidents that interfered with these meetings while they were being held, or with the other various meetings that G7-related ministers held from April onward*22.

■ Other

Since the second half of last year, damages caused by ransomware infections have been escalating in Japan and overseas, and this trend has continued over the current survey period. The TeslaCrypt ransomware had one of the highest numbers of infections, but in May, the master key for decryption was released by the developers without prior notice, and security vendors made decryption tools available. Observations indicated that TeslaCrypt activity was already stagnating before this, so it appears that it was shut down for some reason.

For the past several years there have been concerns regarding the growing impact of scams committed through business emails, referred to as Business Email Compromise (BEC) schemes. A typical BEC technique involves attackers hijacking the email accounts of corporate CEOs, and obtaining funds illegally by sending emails to internal staff members ordering them to transfer money to specific accounts. According to an annual report*23 made public by the FBI's Internet Crime Complaint Center (IC3), there were 7,838 incidents reported in the United States in 2015, involving 263 million dollars in damages. Because damages from such

*21 "Have I been pwned? Check if your email has been compromised in a data breach" (https://haveibeenpwned.com/).
*22 National center of Incident readiness and Strategy for Cybersecurity, "Initiatives for the G7 Ise-Shima Summit" (http://www.nisc.go.jp/conference/cs/ciip/dai07/pdf/07shiryou0201.pdf) (in Japanese).
*23 FBI, "2015 Internet Crime Report" (https://pdf.ic3.gov/2015_IC3Report.pdf).

June Incidents

S 3rd: Members of a cybercrime group that was using the Lurk illegal money remittance malware were arrested in Russia. The Angler Exploit Kit was used for the Lurk infections, but due to this arrest, Angler Exploit Kit Activity has stagnated.
"Cisco Talos Blog: Connecting the Dots Reveals Crimeware Shake-up" (http://blog.talosintel.com/2016/07/lurk-crimeware-connections.html). "Locky, Dridex, and Angler among cybercrime groups to experience fall in activity | Symantec Connect" (http://www.symantec.com/connect/blogs/locky-dridex-and-angler-among-cybercrime-groups-experience-fall-activity).

S 3rd: It was discovered that the email addresses and password information of around 127 million users had leaked from the Badoo social network. It was also confirmed that account information was being sold on Dark Web markets.

S 6th: It was discovered that email addresses and password information for about 100 million users from around 2012 had leaked from a Russian SNS site, VK. It was also confirmed that account information was being sold on Dark Web markets.

S 13th: It was discovered that email addresses and password information for about 51 million users from 2013 had leaked from the iMesh file sharing service, which has already ceased operations. It was also confirmed that account information was being sold on Dark Web markets.

S 14th: It was discovered that there was unauthorized access by an external party against the servers of JTB Corp. subsidiary i.JTB, which may have caused the leak of around 6.79 million pieces of customer information. Customer information for JTB partners such as dTravel, Yahoo! Travel, and DeNA Travel were also affected by this attack.
JTB, "Regarding the potential leak of personal information due to unauthorized access" (http://www.jtbcorp.jp/jp/160614.html) (in Japanese). NTT DOCOMO, "Notice from DOCOMO: Regarding the potential leak of 'dtravel' personal information due to unauthorized access targeting the company servers of our partner JTB Group" (https://www.nttdocomo.co.jp/info/notice/page/160614_00_m.html) (in Japanese). Yahoo! Japan, "Regarding the JTB announcement about 'a potential leak of personal information'" (http://blogs.yahoo.co.jp/yjtravel_staff/20970682.html) (in Japanese).
DeNA Travel, "Notice regarding the potential leak of personal information due to unauthorized access at i.JTB Corp." (http://www.skygate.co.jp/information/2016/information0614.html) (in Japanese).

O 14th The FBI (IC3) issued an alert regarding the spread of damages through Business Email Compromise (BEC) schemes.
Internet Crime Complaint Center (IC3), "Business E-mail Compromise: The 3.1 Billion Dollar Scam" (https://www.ic3.gov/media/2016/160614.aspx).

V 15th: Microsoft published their Security Bulletin Summary for June 2016, and released a total of seventeen updates, including six critical updates such as MS16-063, as well as eleven important updates.
"Microsoft Security Bulletin Summary for June 2016" (https://technet.microsoft.com/library/security/ms16-jun).

S 15th: It was discovered that there was unauthorized access by an external party against the system of the U.S. Democratic National Committee (DNC). Security vendor CrowdStrike reported that two different Russian attack groups were responsible.
CrowdStrike, "Bears in the Midst: Intrusion into the Democratic National Committee" (https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/).

V 16th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.
"Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb16-18.html).

V 16th: A vulnerability (S2-037) in Apache Struts 2 that could allow arbitrary code execution when the REST plug-in is enabled was discovered and fixed.
Apache Software Foundation, "S2-037" (https://struts.apache.org/docs/s2-037.html).

S 17th: It was discovered that unauthorized logins by third parties through identity fraud had taken place at GitHub. The passwords of corresponding accounts were reset.
"GitHub Security Update: Reused password attack" (https://github.com/blog/2190-github-security-update-reusedpassword-attack).

S 18th: Funds totaling approximately 3.64 million ETH (Ethereum) were illegally transferred from a virtual currency investment fund, the DAO by an attacker who exploited a vulnerability in the code. The Ethereum development community later decided to restore the fund to its original state by performing a hard fork.
"CRITICAL UPDATE Re: DAO Vulnerability - Ethereum Blog" (https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/).
"Update3: The DAO is under attack - but Vitalik saved us - DAOhub" (https://blog.daohub.org/the-dao-is-under-attack-8d18ca45011b?gi=ddf32dc5304a#.2kgccwfka).

S 20th: It was discovered that unauthorized logins by third parties through identity fraud had occurred against the Citrix GoToMyPC service. The passwords for all accounts were reset.
"GoToMyPC® System Status - GoToMyPC Password Issues" (http://status.gotomypc.com/incidents/s2k8h1xhzn4k).

S 22nd: Leaks of personal information through unauthorized access by a third party occurred against sites built using the "SPIRAL EC" EC platform provided by PIPED BITS.
"Regarding leaks of personal information through unauthorized access to 'SPIRAL EC(R)'" (http://www.pi-pe.co.jp/pb/info/) (in Japanese).

S 24th: A security researcher found that data on 154 million U.S. voters had been made available to the public online.
"Another US Voter Database Leak" (https://mackeeper.com/blog/post/239-another-us-voter-database-leak).

S 27th: A 17-year-old youth was rearrested on suspicion of violating the Unauthorized Computer Access Law for allegedly compromising an educational information system (SEI-Net) and the internal LAN of a school in Saga Prefecture. This youth had previously been arrested on June 6 on suspicion of violating the Unfair Competition Prevention Law for allegedly distributing an unauthorized viewing program for B-CAS.
Saga Prefecture, "Incidents of unauthorized access targeting school education networks" (http://www.pref.saga.lg.jp/kiji00348348/index.html) (in Japanese).

*Dates are in Japan Standard Time

Legend V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

incidents have continued to spread further since the beginning of this year, another alert was issued in June. This alert indicated that damages caused by BEC are now 1,300% higher than at the beginning of 2015. There have not yet been many reports of such incidents occurring in Japan, but going forward it will be necessary to keep a close eye on the spread of damage.

1.3 Incident Survey

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence, and the methods involved vary widely. However, most of these attacks do not utilize advanced knowledge such as vulnerabilities, but aim to hinder or delay services by causing large volumes of unnecessary traffic to overwhelm network bandwidth or server processes.

■ Direct Observations

Figure 2 shows the state of DDoS attacks handled by the IIJ DDoS Protection Service between April 1 and June 30, 2016.

This shows the number of traffic anomalies judged to be attacks based on IIJ DDoS Protection Service criteria. IIJ also responds to other DDoS attacks, but these incidents have been excluded here due to the difficulty in accurately understanding and grasping the facts behind such attacks.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 splits DDoS attacks into three categories: attacks against bandwidth capacity*24, attacks against servers*25, and compound attacks (several types of attacks against a single target conducted at the same time).

During these three months, IIJ dealt with 267 DDoS attacks. This averages out to 2.93 attacks per day, which is a slight decrease in comparison to our prior report. Server attacks accounted for 62.55% of DDoS attacks, while compound attacks accounted for 34.08%, and bandwidth capacity attacks 3.37%.

The largest scale attack observed during this period was classified as a compound attack, and resulted in 2.84 Gbps of bandwidth using up to 635,000 pps packets.

Of all attacks, 81.27% ended within 30 minutes of the start of the attack, 17.23% lasted between 30 minutes and 24 hours, and 1.50% lasted over 24 hours. The longest sustained attack for this period was a compound attack that lasted for two days, 17 hours, and 15 minutes (65 hours and 15 minutes).

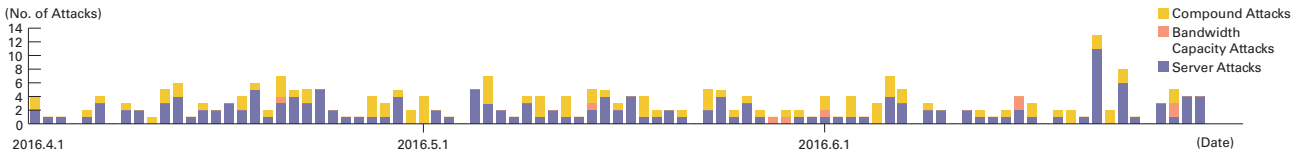


Figure 2: Trends in DDoS Attacks

*24 Attack that overwhelms the network bandwidth capacity of a target by sending massive volumes of larger-than-necessary IP packets and fragments. When UDP packets are used, it is referred to as a UDP flood, while ICMP flood is used to refer to the use of ICMP packets.

*25 TCP SYN flood, TCP connection flood, and HTTP GET flood attacks. In a TCP SYN flood attack, a large number of SYN packets that signal the start of TCP connections are sent, forcing the target to prepare for a large number of incoming connections, resulting in the waste of processing capacity and memory. TCP connection flood attacks establish a large number of actual TCP connections. In a HTTP GET flood a TCP connection with a Web server is established, and then a large number of GET requests in the HTTP protocol are sent, also resulting in a waste of processing capacity and memory.

We observed an extremely large number of IP addresses as the attack sources, whether domestic or foreign. We believe this is due to the use of IP spoofing*26 and botnets*27 to conduct the DDoS attacks.

Backscatter Observations

Next we present DDoS attack backscatter observations*28 through the honeypots*29 of the IIJ malware activity observation project, MITF. Through backscatter observations, portions of DDoS attacks against external networks may be detectable as a third-party without intervening.

For the backscatter observed between April 1 and June 30, 2016, Figure 3 shows the source IP addresses classified by country, and Figure 4 shows trends in the number of packets by port.

The port most commonly targeted by DDoS attacks observed was port 80/TCP used for Web services, and accounted for 40.3% of the total. This was followed by 53/UDP used for DNS at 27.5%, so the top two ports alone accounted for 67.8% of the total. Attacks were also observed on 443/TCP used for HTTPS, 22/TCP used for SSH, and both 27015/UDP and 25565/TCP that are sometimes used for gaming communications, as well as typically unused ports such as 42668/TCP, 50401/TCP, 44461/TCP, and 3306/UDP.

Communications at 53/UDP, which have been observed often since February 2014, remained high at an average of around 4,900 packets per day until May 25. From the next day it dropped to a daily average of about 20 packets, which represents a return to levels observed prior to February 2014. This same phenomenon was seen in the status of random communications under "1.3.2 Malware Activities." It is believed that the perpetrators of the DNS water torture attacks*30 we had observed up until this date either changed their attack method starting from this day, or ceased their attacks.

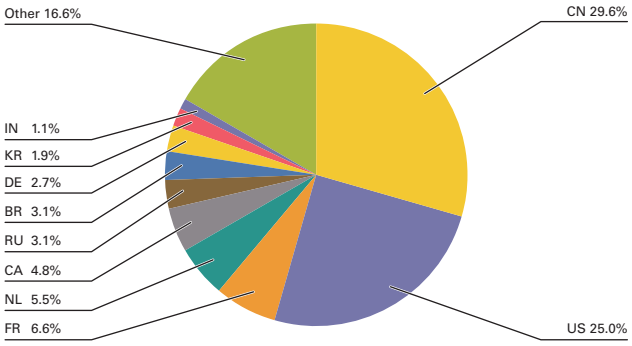


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

Looking at the source of backscatter packets by country thought to indicate IP addresses targeted by DDoS attacks in Figure 3, China accounted for the largest percentage at 29.6%. The United States and France followed at 25.0% and 6.6%, respectively.

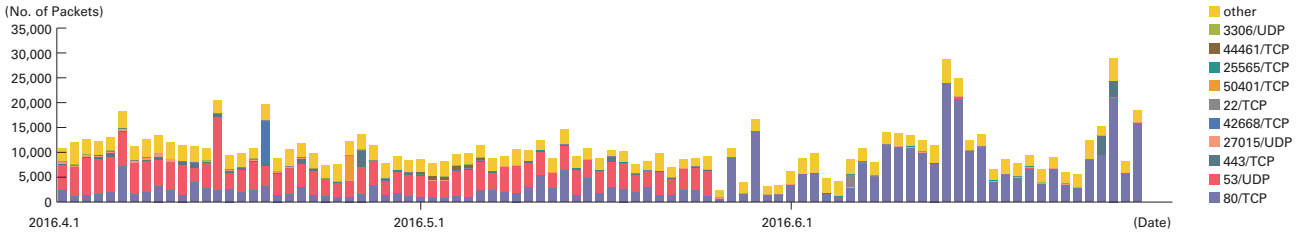


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*26 Impersonation of a source IP address. Creates and sends an attack packet that has been given an IP address other than the actual IP address used by the attacker to make it appear as if the attack is coming from a different person, or from a large number of individuals.

*27 A "bot" is a type of malware that after the infection, conducts an attack upon receiving a command from an external C&C server. A network made up from a large number of bots is called a botnet.

*28 The mechanism and limitations of this observation method, as well as some of the results of IIJ's observations, are presented in Vol.8 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.2 Observations on Backscatter Caused by DDoS Attacks."

*29 Honeypots placed by the MITF, a malware activity observation project operated by IIJ. See also "1.3.2 Malware Activities."

*30 Secure64 Software Corporation, "Water Torture: A Slow Drip DNS DDoS Attack" (https://blog.secure64.com/?p=377). For an explanation in Japanese, refer to the following document written by Mr. Yasuhiro Orange Morishita of Japan Registry Services. "DNS Water Torture Attacks" (http://2014.seccon.jp/dns/dns_water_torture.pdf) (in Japanese).

Now we will take a look at ports targeted in attacks where a large number of backscatter packets were observed. For attacks against Web servers (80/TCP and 443/TCP), there were attacks against the servers of a hosting provider in China on April 6 and April 12, and attacks against the servers for hosting blogs of a U.S. software development company on April 26. There were also attacks against a message board site related to automobiles on May 27, and attacks against multiple servers owned by a Canadian hosting provider on May 29. In addition to these, there were continued attacks against the servers of a U.S. hosting provider since June 8, and attacks on the reverse proxy servers of a U.S. security firm from June 27 through June 28.

Notable DDoS attacks during the current survey period that were detected by IIJ's backscatter observations included attacks by Anonymous against a government website for the state of North Carolina in the U.S. from May 15 through May 20.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*31, the malware activity observation project operated by IIJ. The MITF uses honeypots*32 connected to the Internet in a manner similar to general users in order to observe communications that arrive over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to search for a target to attack.

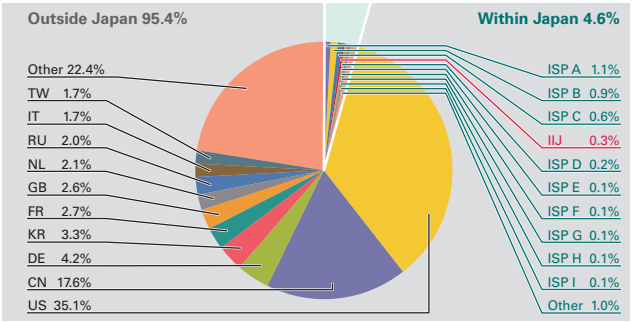


Figure 5: Sender Distribution (by Country, Entire Period under Study)

■ Status of Random Communications

Figure 5 shows the distribution of source IP addresses by country for incoming communications to the honeypots from April 1 through June 30, 2016. Regarding the total volume (incoming packets), because communications to 53/UDP were significantly higher than other ports during the survey period for this report, we have plotted trends for 53/UDP on Figure 6, while other ports are shown on Figure 7. The MITF has set up numerous honeypots for its observations. Here, we have taken the average number per honeypot, and shown the trends by

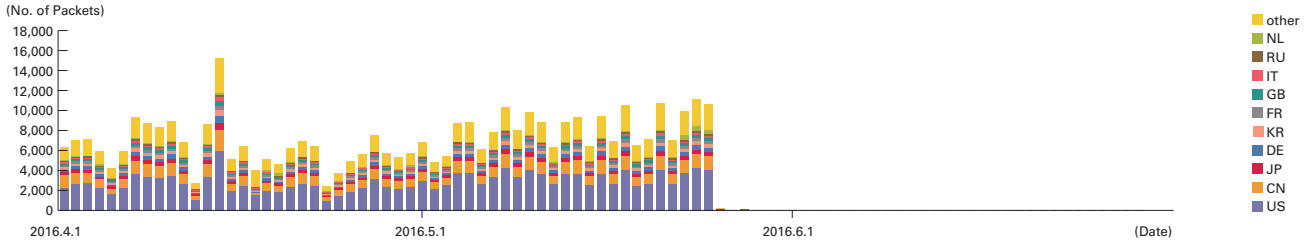


Figure 6: Incoming Communications at Honeypots (by Date, 53/UDP, per Honeypot)

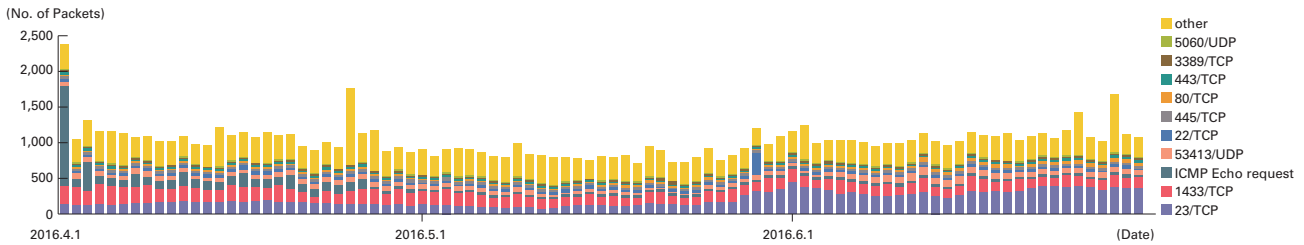


Figure 7: Incoming Communications at Honeypots (by Date, by Target Port, per Honeypot)

*31 An abbreviation of Malware Investigation Task Force. The Malware Investigation Task Force (MITF) began its activities in May 2007, observing malware activity in networks through the use of honeypots in an attempt to understand the state of malware activities, to collect technical information for countermeasures, and to link these findings to actual countermeasures.

*32 A system designed to record attacker and malware activities and their behavior by emulating vulnerabilities and simulating the damages caused by attacks.

country in Figure 6, and trends for incoming packet types (top ten) in Figure 7. Additionally, in these observations we made an adjustment so that multiple TCP connections to a specific port are counted as one attack, such as attacks against MSRPC.

Most of the communications that reached the honeypots during the survey period for this report were on 53/UDP used by DNS, 23/TCP used by telnet, ICMP echo requests, 445/TCP used by Microsoft OSes, and 1433/TCP used by Microsoft's SQL Server. Communications were also observed on 80/TCP and 443/TCP used by Web servers, 22/TCP used by SSH, 3389/TCP used by RDP, and 5060/UDP used by SIP.

As with the survey period for the previous report, there was a high number of 53/UDP communications. Upon investigating these communications, DNS name resolution requests from a range of source IP addresses allocated mainly to the United States and China were being repeatedly received on the IP address of a certain MITF honeypot. Multiple corresponding domain names were also confirmed, and many were sites covering a wide range of fields, such as online shopping, games, and science fiction novels in China. Because the majority of these communications involved repeated name resolution attempts for "(random).(existing domain)," we believe these to be DNS water torture attacks*33. These were no longer observed after May 26, 2016, so it is believed that either the attackers have changed their methods, or ceased the attacks altogether.

Continuing on from the previous survey period, there was also an increase in 1433/TCP. Upon investigation, we found that a large number of these communications were from IP addresses allocated to China, as well as many other IP addresses.

As with the survey period for the previous report, there were a high number of 53413/UDP communications. Upon investigation, we found that these communications were attacks targeting a vulnerability in Netis and Netcore brand routers. The vulnerability was reported by Trend Micro in August 2014*34, and JPCERT/CC reported there was a spike in attacks between April and June of 2015*35. 23/TCP communications rose overall, with a particularly notable increase in June. Upon investigation, we found that packets were arriving from IP addresses allocated to a wide range of countries, with the majority allocated to China and Brazil. Over 400,000 unique IP addresses appeared during this period. In early April there was also an increase in ICMP echo requests from multiple IP addresses allocated to Japan.

■ Malware Activity in Networks

Figure 8 shows the distribution of the source where malware artifacts were acquired from during the period under study, while Figure 9 shows trends in the total number of malware artifacts acquired. Figure 10 shows trends in the number of unique artifacts. In Figure 9 and Figure 10, the trends in the number of acquired artifacts show the actual number of artifacts acquired per day*36, while the number of unique artifacts is the number of artifact variants categorized in accordance with their hash digests*37. Artifacts are also identified using anti-virus software, and a color-coded breakdown of the top 10 variants is shown along with the malware names. As with our previous report, for Figure 9 and Figure 10 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling the data.

On average, 74 artifacts were acquired per day during the period under study, while there were 15 unique artifacts per day. After investigating the undetected artifacts more closely, included were multiple SDBOT families (a type of IRC bot) observed from IP addresses allocated to countries such as Taiwan, India, and Vietnam.

---

*33 Secure64 Software Corporation, "Water Torture: A Slow Drip DNS DDoS Attack" (https://blog.secure64.com/?p=377). For an explanation in Japanese, refer to the following document written by Mr. Yasuhiro Orange Morishita of Japan Registry Services. "DNS Water Torture Attacks" (http://2014.seccon.jp/dns/dns_water_torture.pdf) (in Japanese). The MITF honeypots do not query authoritative servers or cache servers when they receive DNS query packets, so they do not become a part of attacks.

*34 "Netis Routers Leave Wide Open Backdoor" (http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/)

*35 "JPCERT/CC Internet Threat Monitoring Report [April 1, 2015 - June 30, 2015]" (http://www.jpcert.or.jp/english/doc/TSUBAMEReport2015Q1_en.pdf).

*36 This indicates malware acquired by honeypots.

*37 This value is calculated by utilizing a one-way function (hash function) that outputs a fixed-length value for each input. Hash functions are designed to produce a different output for practically every different input. We cannot guarantee the uniqueness of artifacts through hash values alone, given that obfuscation and padding may result in artifacts of the same malware having different hash values. The MITF understands this limitation when using this method as a measurement index.

About 33% of undetected artifacts were in text format. Many of these text format artifacts were HTML 404 or 403 error responses from Web servers, and we believe these were due to infection activities of old malware such as worms continuing despite the closure of the download sites that newly-infected PCs access in an attempt to download malware. A MITF independent analysis revealed that during the current period under observation 85.1% of malware artifacts acquired were worms, 11.2% were bots, and 3.7% were downloaders. In addition, the MITF confirmed the presence of 7 botnet C&C servers*38 and 5 malware distribution sites.

Conficker Activity

Including Conficker, an average of 8,543 artifacts were acquired per day during the period under study for this report, representing 372 unique artifacts. Conficker accounted for 99.1% of the total artifacts acquired, and 96.2% of the unique artifacts. Since Conficker remains the most prevalent malware by far, we have omitted it from the figures in this report. Compared to the previous survey period, the total number of artifacts acquired in this survey period decreased by approximately 28% and the number of unique artifacts decreased by about 13%, which is a gradual overall decline. According to the observations by the Conficker Working Group*39, as of July, 2016, a total of just over 550,000 unique IP addresses are infected. This indicates a drop to about 17% of the 3.2 million PCs observed in November 2011, but it shows that infections are still widespread.

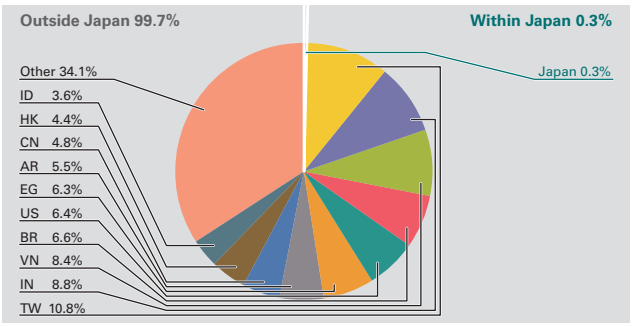


Figure 8: Distribution of Acquired Artifacts by Source (by Country, Entire Period under Study, Excluding Conficker)

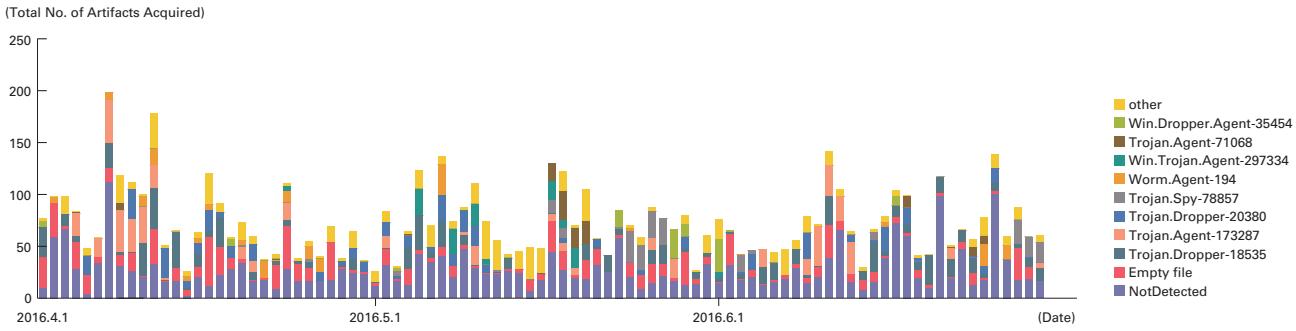


Figure 9: Trends in the Total Number of Malware Artifacts Acquired (Excluding Conficker)

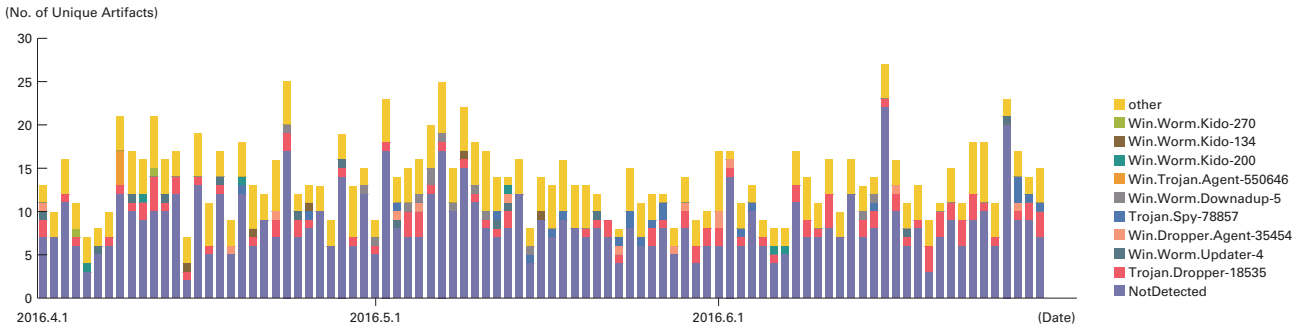


Figure 10: Trends in the Number of Unique Artifacts (Excluding Conficker)

*38 An abbreviation of Command & Control server. A server that provides commands to a botnet consisting of a large number of bots.

*39 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking). Because no numerical data beyond January 7 is available within the current survey period, we have visually observed the highest value in the graph from early July, and used it.

1.3.3 SQL Injection Attacks

Of the different types of Web server attacks, IIJ is conducting ongoing investigations on SQL injection attacks*40. SQL injection attacks have been noted a number of times in the past, and continue to remain a major topic in Internet security. SQL injection attacks are known to attempt one of three things: the theft of data, the overloading of database servers, or the rewriting of Web content.

Figure 11 shows the source distribution of SQL injection attacks against Web servers detected between April 1 and June 30, 2016. Figure 12 shows the trend in the number of attacks. These are a summary of attacks detected through signatures in the IIJ Managed IPS Service. The United States was the source for 32.3% of attacks observed, while China and Japan accounted for 19.6% and 17.5%, respectively, with other countries following. SQL injection attacks on Web servers have been declining from the levels seen in the previous report.

During this period, attacks from multiple sources in China directed at specific targets took place on April 5. On April 7, there were attacks from specific sources in China, Hong Kong, and South Korea directed at specific targets. These attacks are thought to have been attempts to scan for Web server vulnerabilities.

As previously shown, attacks of various types were properly detected and handled in the scope of the service. However, attack attempts continue, requiring ongoing caution.

1.3.4 Website Alterations

Here we indicate the status of website alterations investigated through the MITF Web crawler (client honeypot)*41.

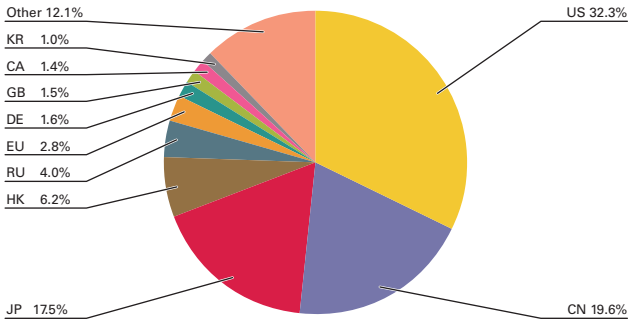


Figure 11: Distribution of SQL Injection Attacks by Source

This Web crawler accesses hundreds of thousands of websites on a daily basis, focusing on well-known and popular sites in Japan. The number of sites that it accesses are added accordingly. In addition to this, we temporarily monitor websites that have seen short-term increases in access numbers. By surveying websites thought to be viewed frequently by typical users in Japan, it becomes easier to speculate trends for fluctuations in the number of altered sites, as well as the vulnerabilities exploited and malware being distributed.

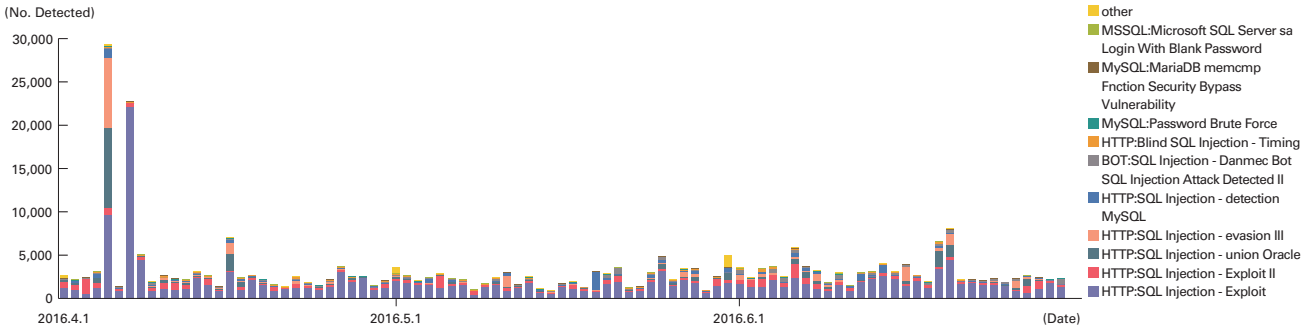


Figure 12: Trends in SQL Injection Attacks (by Day, by Attack Type)

*40 Attacks accessing a Web server to send SQL commands, and operating against an underlying database. Attackers access or alter the database content without proper authorization to steal sensitive information or rewrite Web content.

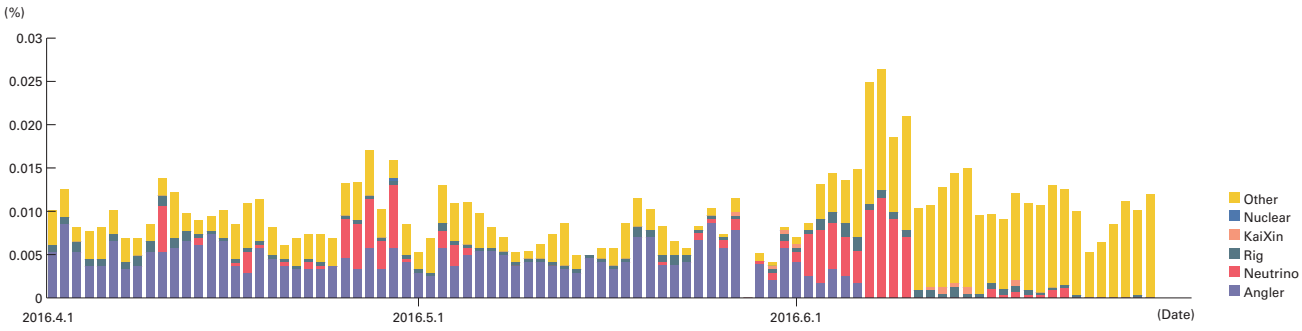
*41 Refer to "1.4.3 Website Defacement Surveys Using Web Crawlers" in Vol.22 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol22_EN.pdf) for a description of Web crawler observation methods.

For the period between April 1 and June 30, 2016, drive-by downloads using the Angler Exploit Kit accounted for the majority of passive attacks detected (Figure 13). A large number of Angler-based attacks had been observed on an ongoing basis since July 2015*42, but they were no longer detected at all after June 6, 2016. One reason for the disappearance of Angler is an incident*43 immediately prior to this in which a criminal organization thought to have utilized malware for exploits in Russia was busted, leading to the arrest of 50 people*44. For a period of time after this, Neutrino gained momentum as if to fill the hole left by Angler, but since late June its growth has stagnated along with Rig.

Many of the payloads observed in April were TeslaCrypt, but after the announcement that development of TeslaCrypt would be discontinued in May*45, it was replaced by CryptXXX. Other payloads such as Bedep and Ursnif were also observed.

Since mid-June, there was a sharp increase in the number of incidents where users were prompted to install a PUA*46 or redirected to fraudulent sites urging them to call a fictitious support center by displaying fake dialog boxes on the browser screen that suggested they had a malware infection, etc. It was also confirmed that many of these fraudulent sites displayed similar dialog boxes for Mac OS X clients as well, and prompted the installation of a PUA that could be executed in Mac OS X environments.

Due to the disappearance of Angler, attacks based on drive-by downloads have been returning to normal levels. Meanwhile, the number of fraudulent sites tricking users into PUA installations has been increasing. In browser environments, it is important to consider countermeasures for cases where PC users may intentionally install PUAs or malware due to social engineering techniques such as visiting fraudulent sites, in addition to the malware infections due to the exploitation of vulnerabilities*47. Website operators need to continue to take measures against the alteration of Web content, and properly manage mashup content provided by external sources, such as advertisements or aggregation services.



*Covers several hundreds of thousands of sites in Japan. In recent years, drive-by downloads using exploit kits have been configured to change attack details and even whether or not to attack based on the client system environment or session information, source address attributes, and an attack quota such as the number of attacks. This means that results can vary wildly depending on the test

Figure 13: Rate of Passive Attack Incidence When Viewing Websites (%) (by Exploit Kit)

*42 Refer to "1.4.2 Angler Exploit Kit on the Rampage" in Vol.28 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol28_EN.pdf) for more information about our observations of the status and functions of Angler in July 2015.

*43 Source - BBC News - © [2016] BBC, "Russian hacker gang arrested over $25m theft" (http://www.bbc.com/news/technology-36434104).

*44 For example, an article titled "Is the Angler exploit kit dead?" (https://nakedsecurity.sophos.com/2016/06/16/is-angler-exploit-kit-dead/) on the Sophos Naked Security technology blog touches upon the connection between this incident and the disappearance of Angler.

*45 We discuss the end of TeslaCrypt development in Vol.31 of this report (http://www.iij.ad.jp/en/company/development/iir/031.html) under "1.4.1 Various Ransomware and Their Countermeasures."

*46 An abbreviation of Potentially Unwanted Application. This is a generic term for applications deemed unnecessary for general work tasks, and thought to potentially lead to unwanted results for PC users and system administrators.

*47 Examples include limiting the assignment of administrator privileges and applying application white lists. See Vol.31 of this report (http://www.iij.ad.jp/en/company/development/iir/031.html) under "1.4.2 Hardening Windows Clients Against Malware Infections" for more information.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to conduct independent surveys and analyses of prevalent incidents. Here, we present information from the surveys we have conducted during this period, covering how to create profiles for the Volatility Framework, and hardening Windows clients against malware infections (part 2).

1.4.1 Creating Profiles for the Volatility Framework

About the Volatility Framework

The Volatility Framework (herein referred to as "Volatility") is open source software used to analyze memory images for computer forensics*48.

When you run Volatility you must specify a profile. Profiles are prepared for each OS, service pack, and architecture, and it is not possible to perform a proper analysis unless you specify the profile that matches the system that the memory image was obtained from. Figure 14 shows a list of profiles included in Volatility by default.

As this figure shows, only Windows profiles are bundled with the software by default. To analyze Linux or Mac OS X memory images, it is necessary to download profiles from the Volatility GitHub page*49. However, profiles are not available for all OS versions. Also, since many kernel updates are released for Linux, you may encounter cases where the Linux kernel version is different even for identical versions of an OS.

```
Profiles
--------
VistaSP0x64 - A Profile for Windows Vista SP0 x64
VistaSP0x86 - A Profile for Windows Vista SP0 x86
VistaSP1x64 - A Profile for Windows Vista SP1 x64
VistaSP1x86 - A Profile for Windows Vista SP1 x86
VistaSP2x64 - A Profile for Windows Vista SP2 x64
VistaSP2x86 - A Profile for Windows Vista SP2 x86
Win10x64 - A Profile for Windows 10 x64
Win10x86 - A Profile for Windows 10 x86
Win2003SP0x86 - A Profile for Windows 2003 SP0 x86
Win2003SP1x64 - A Profile for Windows 2003 SP1 x64
Win2003SP1x86 - A Profile for Windows 2003 SP1 x86
Win2003SP2x64 - A Profile for Windows 2003 SP2 x64
Win2003SP2x86 - A Profile for Windows 2003 SP2 x86
Win2008R2SP0x64 - A Profile for Windows 2008 R2 SP0 x64
Win2008R2SP1x64 - A Profile for Windows 2008 R2 SP1 x64
Win2003SP1x64 - A Profile for Windows 2008 SP1 x64
Win2008SP1x86 - A Profile for Windows 2008 SP1 x86
Win2008SP2x64 - A Profile for Windows 2008 SP2 x64
Win2008SP2x86 - A Profile for Windows 2008 SP2 x86
Win2012R2x64 - A Profile for Windows Server 2012 R2 x64
Win2012x64 - A Profile for Windows Server 2012 x64
Win7SP0x64 - A Profile for Windows 7 SP0 x64
Win7SP0x86 - A Profile for Windows 7 SP0 x86
Win7SP1x64 - A Profile for Windows 7 SP1 x64
Win7SP1x86 - A Profile for Windows 7 SP1 x86
Win81U1x64 - A Profile for Windows 8.1 Update 1 x64
Win81U1x86 - A Profile for Windows 8.1 Update 1 x86
Win8SP0x64 - A Profile for Windows 8 x64
Win8SP0x86 - A Profile for Windows 8 x86
Win8SP1x64 - A Profile for Windows 8.1 x64
Win8SP1x86 - A Profile for Windows 8.1 x86
WinXPSP1x64 - A Profile for Windows XP SP1 x64
WinXPSP2x64 - A Profile for Windows XP SP2 x64
WinXPSP2x86 - A Profile for Windows XP SP2 x86
WinXPSP3x86 - A Profile for Windows XP SP3 x86
```

Figure 14: Default Profiles for Volatility

In such cases, it is necessary to create a profile on your own to match the system being used. In this report we will explain the procedures for creating Volatility profiles for Linux kernels.

Preparation for Creating a Profile

Checking the Version of the System to be Analyzed

To create a Volatility profile, you must install Volatility on a system with the same version as the system that will be subject to the memory image analysis. See Figure 15 for instructions on how to check the OS version and Linux kernel version for most Linux distributions. Here, we will use CentOS Linux 7.2-1511 and Linux kernel 3.10.0-327.22.2.el7.x86_64 as an example.

*48 The Volatility GitHub page. "GitHub - volatilityfoundation/volatility: An advanced memory forensics framework" (https://github.com/volatilityfoundation/volatility).

*49 The profile download page. "GitHub - volatilityfoundation/profiles: Volatility profiles for Linux and Mac OS X" (https://github.com/volatilityfoundation/profiles).

Preparing a Machine for Creating a Profile

Prepare a machine for creating Volatility profiles (prepare a separate machine to minimize changes to the system subject to analysis). At this time it is best to ready a machine with the same OS version and Linux kernel version using the step explained above. A virtual machine can also be used to create the profile.

Downloading Volatility

Install the libraries required to run Volatility and create profiles (Figure 16). Git is used for part of the process, but some Linux distributions may have packages for these libraries. If this is the case, install them instead as necessary.

Next, download Volatility (Figure 17). Volatility can be run without installing it on a system, so here we will use it without installing. Run "$ python ./vol.py --info" in the directory you downloaded Volatility into, and make sure that no errors occur.

Installing a Linux Kernel Development Environment

Because it is necessary to compile a kernel module when creating profiles, you will need to install a Linux kernel development environment (Figure 18). Commands such as "make" and "gcc" are also required, so install each command as necessary. This completes the preparation.

Creating a Profile

Run the "make" command in the "volatility/tools/linux" directory. If there are no issues, a file called "module.dwarf" should have been created in this directory. Next, create a ZIP file containing the "module.dwarf" and "System.map" files in the "volatility/volatility/plugins/overlays/linux/" directory (Figure 19).

This ZIP file is the Volatility profile. There are no required naming conventions for profiles, but it is probably best to use a profile name that at least describes the OS version. If you wish to micromanage your profiles, include the Linux kernel version in the profile name as well.

```
RedHat
  $ cat /etc/redhat-release

CentOS
  $ cat /etc/centos-release

Debian
  $ cat /etc/lsb-release

Ubuntu
  $ cat /etc/debian_version

Linux Kernel
  $ uname -r
```

Figure 15: Checking the OS Version

```
Installing diStorm3
  $ git clone https://github.com/gdabah/distorm.git
  $ cd distorm
  $ sudo python setup.py install

Installing PyCrypto
  $ sudo yum install python-crypto

Installing DWARF
  $ sudo yum install libdwarf-tools

Installing elfutils
  $ sudo yum install elfutils-libs
```

Figure 16: Installing Related Libraries

```
Downloading Volatility
  $ git clone https://github.com/volatilityfoundation/volatility.git

Running Volatility
  $ cd volatility
  $ python ./vol.py
```

Figure 17: Downloading and Running Volatility

```
$ sudo yum install kernel-devel-3.10.0-327.22.2.el7.x86_64.rpm
$ sudo yum install kernel-headers-3.10.0-327.22.2.el7.x86_64.rpm
```

Figure 18: Installing a Linux Kernel Development Environment

```
$ cd volatility/tools/linux
$ make
$ sudo zip volatility/volatility/plugins/overlays/linux/CentOS72.zip ./module.dwarf /boot/System.map-3.10.0-327.22.2.el7.x86_64
```

Figure 19: Creating a Profile

You can check whether the created profile has been recognized in Volatility using commands such as those shown in Figure 20.

Creating Different Versions of a Profile

The procedures detailed up to this point have shown how to create Volatility profiles for the Linux kernel currently running. However, even if the OS version is the same, when creating profiles for different Linux kernel versions or a custom Linux kernel, it is necessary to change the process slightly.

When the Linux Kernel Version is Different

In place of the "Installing a Linux Kernel Development Environment" step, unpack the Linux kernel package you want to create a profile for into a directory of your choice as shown in Figure 21.

The other procedures remain basically the same, but when creating the profile, you must specify KDIR and KVER as parameters for the "make" command as shown in Figure 22.

One thing to note is that for CentOS 7, the "/lib/modules/<kernel_ver>/build" symbolic link will be broken, resulting in an error indicating that "/home/admin/ksrc/lib/modules/<kernel_ver>/build does not exist" when you run the "make" command. In this case, you can avoid the error by resetting the symbolic link for the build file, as shown in Figure 23.

When a Custom Linux Kernel is Used

When the Linux kernel is customized for a specific device or purpose, it is not possible to use the packages made available by the Linux distributors as-is. In this case, prepare the source code for the Linux kernel using one of the following methods.

1. If the source code and patches for the custom Linux kernel are available, use these.
2. If the source code and patches are not available, prepare source code for a version of the Linux kernel as close as possible to the one being used in the system subject to analysis. Also, using the kernel configuration on the system to be analyzed, keep the configuration as similar as possible*50.

As described above, while source code that corresponds as closely as possible to the Linux kernel running on the system to be analyzed is required, the other procedures remain the same.

```
$ python ./vol.py --info | grep Linux
Volatility Foundation Volatility Framework 2.5
LinuxCentOS72x64 - A Profile for Linux CentOS72 x64      <-The created profile
linux_banner        - Prints the Linux banner information
linux_yarascan      - A shell in the Linux memory image
```

Figure 20: Checking Profiles

```
$ wget http://ftp.iij.ad.jp/pub/linux/centos/7.2.1511/updates/x86_64/Packages/kernel-3.10.0-327.3.1.el7.x86_64.rpm
$ wget http://ftp.iij.ad.jp/pub/linux/centos/7.2.1511/updates/x86_64/Packages/kernel-devel-3.10.0-327.3.1.el7.x86_64.rpm
$ wget http://ftp.iij.ad.jp/pub/linux/centos/7.2.1511/updates/x86_64/Packages/kernel-headers-3.10.0-327.3.1.el7.x86_64.rpm
$ mkdir ksrc && cd ksrc
$ rpm2cpio ../kernel-devel-3.10.0-327.3.1.el7.x86_64.rpm | cpio -id
$ rpm2cpio ../kernel-headers-3.10.0-327.3.1.el7.x86_64.rpm | cpio -id
$ rpm2cpio ../kernel-3.10.0-327.3.1.el7.x86_64.rpm | cpio -id
```

Figure 21: Unpacking Different Linux Kernel Versions

```
$ make KDIR=/home/admin/ksrc/ KVER=3.10.0-327.3.1.el7.x86_64
```

Figure 22: Creating Profiles for Different Linux Kernel Versions

```
$ cd /home/admin/ksrc/lib/modules/3.10.0-327.3.1.el7.x86_64/
$ rm build
$ ln -s /home/admin/ksrc/usr/src/kernels/3.10.0-327.3.1.el7.x86_64/ build
```

Figure 23: Resetting a Symbolic Link

*50 However, if part of the internal data structure of the kernel differs between the created profile and the system to analyze, it may not be possible to analyze that part properly, so this must be taken into account when performing analysis.

Also, although Mac OS X profiles can be downloaded from the Volatility GitHub page as mentioned previously, you may not be able to download a profile for the latest version depending on the timing, such as immediately after a new version is released. The procedure for creating a profile is mostly the same as for Linux kernels*51, so it may be beneficial to consider creating a Mac OS X profile for yourself.

1.4.2 Hardening Windows Clients Against Malware Infections (Part 2)

In the previous IIR, we discussed fundamental measures, such as applying patches and only granting general user privileges, as well as a hardening method called application whitelisting. In this report we will introduce the other measures. Those who have not yet read the previous report should also see "Hardening Windows Clients Against Malware Infections (Part 1)" in IIR Vol.31*52.

■ EMET

EMET (Enhanced Mitigation Experience Toolkit) is a tool distributed by Microsoft for mitigating the exploitation of vulnerabilities*53. In addition to making maximum use of Windows security features, it also implements measures for mitigating known attack techniques. You can also install EMET and enforce policies on all clients in a domain*54. Version 5.5 is the most recent version at the time of writing, so we will explain how to use this version of EMET on a single host. Launching EMET GUI from the Start menu after installation will launch the EMET management tool.

1. Change **Quick Profile Name** to **Maximum security settings**. A pop-up window indicating you will need to reboot appears after making this change, so click **OK** (Figure 24).
2. Click **Import**, and then apply all the profiles in C:\Program Files (x86) \EMET 5.5\Deployment\Protection Profiles.
3. Reboot the host to enable the settings.

This concludes the basic configuration. After this, you can fine-tune settings by clicking **Apps** in the configuration window to add individual applications based on your environment, or remove any interfering functions individually when issues occur during testing or when using an application.

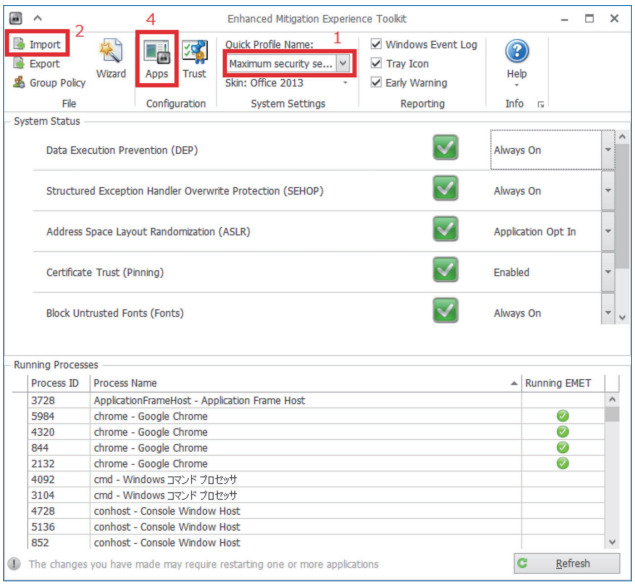


Figure 24: EMET Configuration Screen

■ Using a Stricter UAC Policy

UAC (User Account Control) is a feature implemented beginning with Windows Vista that disables privileged operations under normal circumstances, even for administrator accounts. This feature helps in detecting malicious changes by checking with the user whether the change was initiated by them prior to any program making important changes to the OS.

*51 Detailed procedures for creating Mac OS X profiles (https://github.com/volatilityfoundation/volatility/wiki/Mac).
*52 "Internet Infrastructure Review (IIR) Vol.31" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol31_EN.pdf).
*53 You can view information regarding EMET and download the toolkit from the following URL. "Enhanced Mitigation Experience Toolkit" (https://technet.microsoft.com/en-us/security/jj653751).
*54 Since version 3.0, EMET has supported the automatic installation of packages via Active Directory, as well as policy distribution. The following URLs provide detailed explanations using images and video. "Controlling EMET when using Active Directory" (http://n.pentest.ninja/?p=31157) (in Japanese). "ITSCFORUM Deploy and Manage EMET using a GPO" (https://www.youtube.com/watch?v=4MgODgeDr18&app=desktop).

Broadly speaking, there are four levels of UAC configuration, and in Vista, the highest level, "Always notify," was set by default. However, most users who had been using XP on its own were utilizing administrator privileges all the time, so switching to Vista resulted in frequent UAC pop-ups, causing many users to criticize this function. For this reason, from Windows 7 onward, the default was changed to the second highest level, "Notify me only when apps try to make changes to my computer." But this configuration has a number of flaws, and actual cases have been confirmed where UAC was bypassed to perform attacks that automatically elevate to administrative privileges without user consent*55. To avoid vulnerabilities like this, it is best to change the UAC configuration to the "Always notify" setting*56.

1. From the Control Panel, click **User Accounts** to view user accounts.
2. Click **Change User Account Control settings**, and the window shown in Figure 25 will appear.
3. On Windows 7 or later the second highest level will be set, so move the slider to the top, and then click **OK** (Figure 26).

This will prevent the automatic elevation of privileges, pop-ups will always appear, and make it easier for administrative users to notice any irregularities.

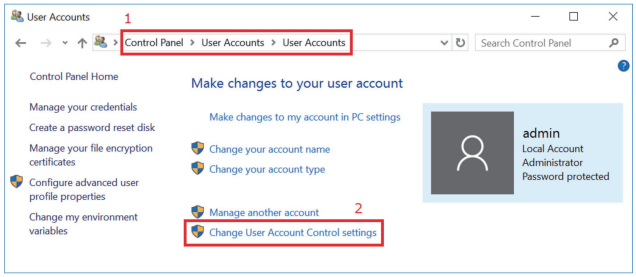


Figure 25: User Accounts Configuration Screen

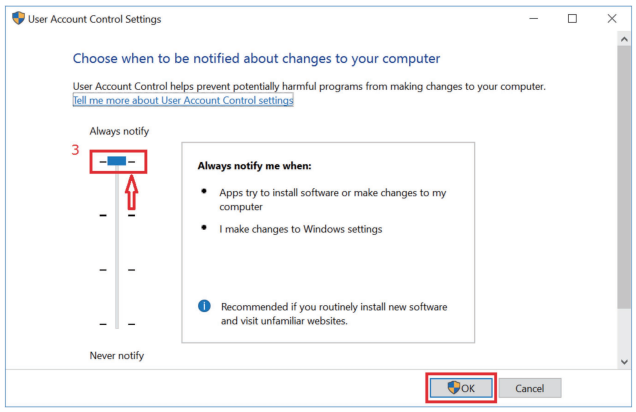


Figure 26: Change User Account Control Settings

■ Disabling WSH

WSH (Windows Script Host) is a function for running VBScript or JScript on a host. As mentioned in the previous report, IIR Vol.31, under "1.4.1 Various Ransomware and Their Countermeasures," cases where JScript (.js) files are attached to emails have been confirmed with TeslaCrypt and Locky. In the past, a technique where shortcut files (.lnk) with VBScript (.vbs) embedded were sent via email was seen. To prevent these kinds of attacks, disable WSH by adding the following value into the registry key using the Registry Editor.

- Key
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings
- Value name
  Enabled
- Value data (DWORD value)
  0

When disabled, a warning will appear when double-clicking .js or .vbs files, or when executing cscript.exe (Figure 27).

*55 In IIR Vol.21 under "1.4.1 The PlugX RAT Used in Targeted Attacks" (http://www.iij.ad.jp/en/company/development/iir/021.html), we touch upon automatic elevation to administrator privileges by bypassing UAC with PlugX. In the past, malware such as Dridex also bypassed UAC using a different sdb than PlugX. The following URL explains these techniques, "New UAC circumvention techniques using Dridex (2015-02-09)" (https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html) (in Japanese). A researcher created a list of UAC bypass techniques that can be utilized when using the default values in Windows 7 or later, and has published the list as a verification tool.
"UACMe" (https://github.com/hfiref0x/UACME).

*56 In domain environments, this is done through the Group Policy Management Editor. Navigating to **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Local Policies**, **Security Options** to adjust the User Account Control items will yield a similar result.

■ Blocking rundll32.exe and regsvr32.exe Communications

rundll32.exe and regsvr32.exe contain functions that can be used to obtain and execute VBScript (.vbs) and JScript (.js) files from a remote host via HTTP, etc. These functions could be exploited by attackers, so they should be blocked. However, because rundll32.exe and regsvr32.exe are also used by normal Windows processes, it is not possible to block execution of them entirely. Therefore, what needs to be blocked is when these executable files attempt to communicate externally. This can be done through the configuration of outbound rules for Windows Firewall with Advanced Security, or a personal firewall. In 64-bit environments, the executable files also exist on the SysWOW64 side, so these need to be blocked as well.

```
C:\Windows\System32\rundll32.exe
C:\Windows\System32\regsvr32.exe
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\SysWOW64\regsvr32.exe
```

These executable files could also be present in folders under C:\Windows\WinSxS, so these must be blocked as well.

■ Blocking PowerShell

PowerShell is an extremely powerful scripting language for Windows that can manage Windows and access Windows APIs. By default it cannot run file-based scripts, but this limitation can be bypassed easily. Shortcuts or external scripts via HTTP can be directly executed, and its use has been confirmed in actual attacks, so it is best to place a blanket restriction on the paths shown below, using AppLocker or Software Restriction Policies to prevent execution by general users.

```
C:\Windows\System32\WindowsPowerShell
C:\Windows\SysWOW64\WindowsPowerShell
```

Because folders under C:\Windows\WinSxS may also contain powershell.exe or powershell_ise.exe, these must be blocked as well.

■ Blocking HTAs

HTAs (.hta) are HTML application programs written using HTML, VBScript, and JScript. In a recent example, an attacker using Locky attempted to infect users by sending emails with .hta files attached, and prompting users to open them. Other than this, incidents where malware used malicious HTAs have been taking place since at least 2007*57. To deal with these, it is best to restrict mshta.exe using AppLocker or Software Restriction Policies. Because this may also be present in folders under C:\Windows\WinSxS, these must be blocked as well. A limited solution is to remove .hta file associations using the Group Policy Editor, but this can be bypassed when mshta.exe is called via a shortcut, so it is not a perfect solution.

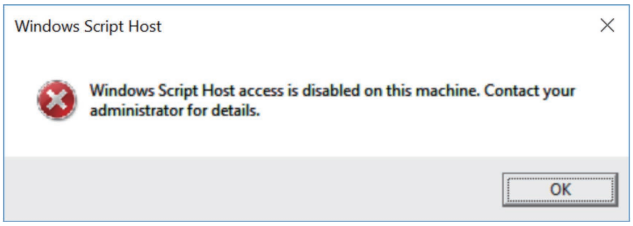


Figure 27 Confirming WSH is Disabled

*57 Malicious HTA incidents are discussed at the following URL. "The Power of (Misplaced) Trust: HTAs and Security" (https://nakedsecurity.sophos.com/2009/10/16/power-misplaced-trust-htas-insecurity/).

Preventing Web Browser Plug-ins from Running Automatically (Click to Play)

You can configure a setting in Google Chrome and Firefox called Click to Play that only allows Web browser plug-ins to run when a user has given explicit permission*58. This prevents Flash and other plug-ins from running automatically, and mitigates attacks (drive-by downloads) that infect users with malware through exploitation of vulnerabilities in plug-ins.

Google Chrome

1. On the Google Chrome menu, click **Settings** (Figure 28).
2. Click **Show advanced settings** at the bottom of the page.
3. Under **Privacy**, click **Content settings**.
4. Click **Let me choose when to run plugin content**.
5. Click **Done**, and Click to Play will be enabled (Figure 29).

Firefox

1. Type **about:config** in the address bar. A warning will appear after you do this, so click **I'll be careful, I promise!** (Figure 30).
2. Change the value for **plugins.click_to_play** to **true** to enable Click to Play (Figure 31).

Restricting Mashup Content

Firefox add-ons include plug-ins such as NoScript Security Suite*59 and RequestPolicy Continued*60 that limit the sites that can execute script or prevent access to domains other than those entered into the address bar. Using these add-ons can prevent redirection to an external site even when the website you normally browse is compromised, making it less likely you will be sent to a malicious website. This can help mitigate malware infections as a result.

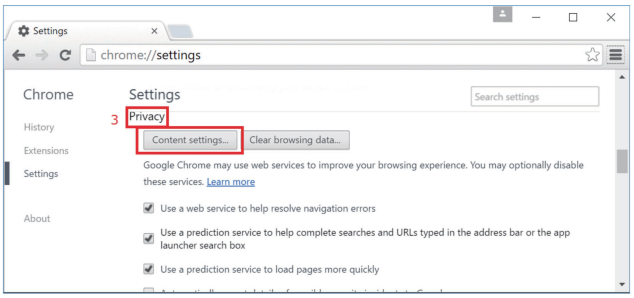


Figure 28: Chrome Settings

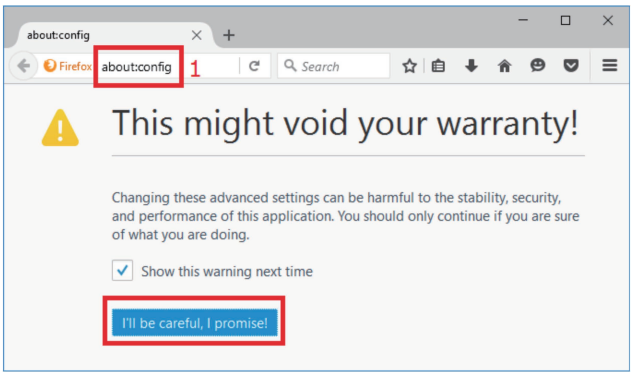


Figure 30: Firefox Advanced Settings Screen

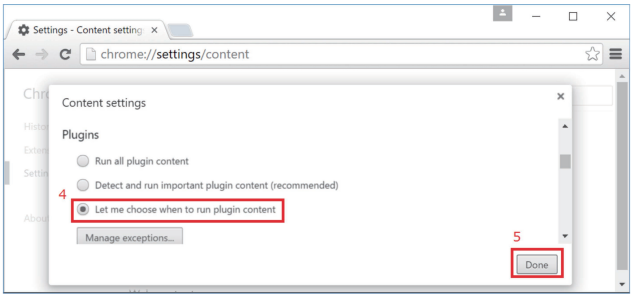


Figure 29: Chrome - Content Settings

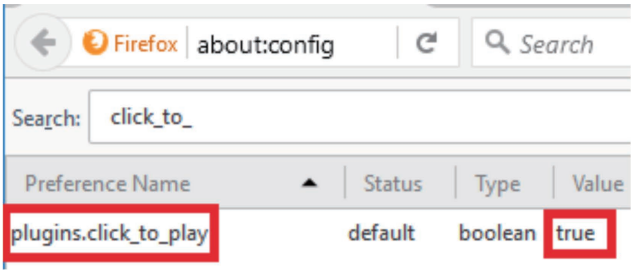


Figure 31: Firefox - Click to Play Settings

*58 Internet Explorer also has a feature called ActiveX filters that function like Click to Play. "Use ActiveX controls for Internet Explorer 11 and Internet Explorer 10" (https://support.microsoft.com/en-us/help/17469/windows-internet-explorer-use-activex-controls).

*59 "NoScript Security Suite" (https://addons.mozilla.org/en/firefox/addon/noscript/).

*60 "RequestPolicy Continued" (https://addons.mozilla.org/en/firefox/addon/requestpolicy-continued/).

■ Blocking Store Apps

Store apps can be used in Windows 8 and later, but because users are able to install apps freely, they may inadvertently install apps from the store that contain malware. Apps such as games are also included by default, which are not appropriate in a business environment. Thus, you should block the use of all store apps.

1. Run the Local Group Policy Editor as an administrator. This can be done by executing gpedit.msc.
2. From the console tree in the left pane, navigate to **Computer Configuration**, **Administrative Templates**, **Windows Components**, **Store** (Figure 32).
3. Switch the following items to **Enabled** (Figure 32).
   - **Turn off the Store application**
   - **Disable all apps from Windows Store** (this item is only found in Windows 10 or later)
4. To enable Software Restriction Policies, reboot the host you want to enforce policies for, or start a command prompt as an administrator and execute the "gpupdate /force" command.

If you access the store after disabling it, you will see that apps can no longer be accessed (Figure 33). You can also restrict apps through AppLocker.

■ Various Measures and Their Effect Against Intrusion Routes

Table 1 below is a summary of the effectiveness of individual measures for each route of intrusion.

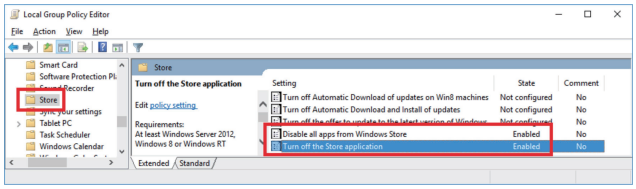


Figure 32: Store App Configuration Screen

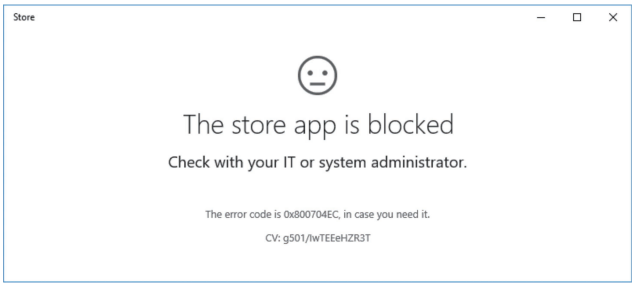


Figure 33: Screen Displayed When Store Apps are Blocked

Table 1: Various Measures and Their Effect on Intrusion Routes

Measure	Web	Email	Notes
Application whitelisting	○	○	Because malware is downloaded and installed under the user directory in many cases, it is possible to prevent infection. It is also possible to protect against executables with fake icons or .js and .vbs files received by email, even if they are accidentally double-clicked.
Do not grant administrator privileges to users	△	△	Can limit the scope of the malware activity to a single account. Prevents unintended program from being included.
EMET	△	△	Can mitigate exploits using malicious Web content or malicious document files.
Using stricter UAC policies	△	△	You can minimize the scope of damages, even when executed as an administrator user.
Disabling WSH		○	Can prevent infection when .js or .vbs files are received by email, or when JScript or VBScript are included in shortcuts.
Block rundll32.exe and regsvr32.exe communications	○	○	When used during a drive-by download, it mitigates infection. Can prevent when malicious shortcuts are sent via email.
Blocking PowerShell	○	○	When used during a drive-by download, it mitigates infection. Can prevent when malicious shortcuts are sent via email.
Blocking HTA	○	○	When .hta files are received by email or used during a drive-by download, it mitigates infection
Prevents Web browser plug-ins from running automatically (Click to Play)	○		Mitigates the occurrence of drive-by downloads.
Restricting mashup content	○		Mitigates the occurrence of drive-by downloads.
Blocking store apps			Protects against unintended programs being included, as well as the installation of malware or PUA (potentially unwanted applications) from the store.

*We assume drive-by downloads for Web, and attachments for Email. URL is included in drive-by-downloads.

○: Effective △: Effective under some conditions

■ The Potential of an Attack Succeeding

Implementing the abovementioned measures can prevent many malware infections, but under the following circumstances they will not help protect against an attack.

- When an attack successfully exploits an arbitrary code execution vulnerability
- When malware is executed with increased privileges, such as SYSTEM privileges exploiting a privilege escalation vulnerability, or when malware is unpacked and executed entirely in memory

However, bypassing EMET and successfully executing an unknown vulnerability (0-day) is extremely difficult, and we believe that most attacks will not be successful*61.

■ Side Effects

When AppLocker or Software Restriction Policies are used, a standard version of Google Chrome will no longer function. This is because Chrome is installed to the general user directory. As an alternative, you can use the standalone installer to install it under Program Files. However, even if you do this, the Google Chrome updater will still attempt to unpack and run executable files in the user's temp directory, so updates cannot be applied. To avoid this, you should allow the certificate of this updater as a permission rule*62.

When WSH is disabled, logon scripts that use VBScript will no longer function. When PowerShell is being used for PC management, blocking PowerShell execution will have an adverse effect.

*61 During the period covered by this report, there was a report of the Angler Exploit Kit completely evading the latest version of EMET, enabling attacks to succeed. "Angler Exploit Kit Evading EMET" (http://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html). In the past a number of vulnerabilities had been reported by researchers, but to my knowledge this was the first time an actual attack had been confirmed. That said, when this attack appeared, the Angler Exploit Kit did not exploit any 0-day vulnerabilities, so as long as patches were being applied properly there would be no damages. EMET may implement countermeasures for this technique in the next update, but at the time of writing it was considered difficult to prevent it through EMET. To mitigate the reported technique, you can disable Flash and Silverlight, or use the Click to Play function to prevent the automatic loading of DLLs related to programs like Flash. This demonstrates that it is necessary to apply what is known as defense in depth, implementing other techniques to protect against attacks for when a single countermeasure is compromised. It is also necessary to gather information on attacks and examine ways to mitigate them on an ongoing basis. EMET is merely a tool for mitigating vulnerabilities. You should not misunderstand what EMET is and think that implementing EMET means that you no longer need to apply patches.

*62 Chrome distributes Chrome for Work, which supports batch installation on Windows domain clients, centralized management using group policies, and policy enforcement for users (https://www.google.com/intl/en/chrome/business/browser/admin/). This mechanism allows administrators to deploy the newest versions to all clients. In addition, it can prevent users from installing extensions or add-ons on their own. Firefox and Thunderbird also use mechanisms called Mission Control Desktop (MCD) and AutoConfig to prevent users from changing the environment on their own, and force the use of administrator settings (https://developer.mozilla.org/en-US/Firefox/Enterprise_deployment).

Japan still has a deep-rooted culture regarding the use of self-extracting archives to send encrypted files as attachments when exchanging messages by email. When application whitelisting is enabled, all areas where a user can save executable files are blocked without exception, so recipients of such files will no longer be able to check the content of these attachments. The EMDIVI malware that was used frequently in targeted attacks two years ago used self-extracting archives. If the attacker obtained archivers and encryption tools identical to those used within the sender organization, and created the self-extracting archives and sent them by email, there would be no way to determine whether the attachment is harmless or not. When you want to encrypt attachments, you should use a password-protected ZIP file, or if stronger encryption is required, encrypt with GPG before sending. Another option is to use a trusted online storage service and share files over an HTTPS-encrypted communication channel, or encrypt the entire email using PGP/MIME or S/MIME. Either way, we need to eradicate this bad cultural habit as quickly as possible.

You may run into a number of other issues when implementing the configurations we have introduced here. When this happens, you will need to consider whether the issue can be avoided by devising new rules or changing a process. Our discussion here has been focused on preventing malware infections, but to conduct operations more securely you should also consider other measures, such as configuring audit policies for process creation, file creation, and write events, or even using third-party auditing software for monitoring. Windows 10 features freshly-implemented functions for maintaining security in the face of new threats, such as Device Guard*63 and Credential Guard*64. It may be beneficial to look into these. Because new threats are discovered every day, you will need to gather information, evaluate ways to deal with these threats, and review your policies on a regular basis.

1.5 Conclusion

This report has provided a summary of security incidents that IIJ has responded to. This time we discussed the creation of profiles for the Volatility Framework, and hardening Windows clients against malware infections (part 2). IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and disclosing information on incidents and associated responses through reports such as this.

Authors:
Mamoru Saito
Director of the Advanced Security Division, and Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ. After working in security services development for enterprise customers, in 2001 Mr. Saito became the representative of the IIJ Group emergency response team IIJ-SECT, which is a member team of FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member for several industry groups, including ICT-ISAC Japan, Nippon CSIRT Association, Information Security Operation providers Group Japan, and others.

Masafumi Negishi (1.2 Incident Summary)
Tadashi Kobayashi, Tadaaki Nagao, Hiroshi Suzuki, Minoru Kobayashi, Hisao Nashiwa (1.3 Incident Survey)
Minoru Kobayashi (1.4.1 Profile Creation for the Volatility Framework)
Hiroshi Suzuki (1.4.2 Hardening Windows Clients Against Malware Infections (Part 2))
Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ

Contributors:
Yuji Suga, Yasunari Momoi, Hiroyuki Hiramatsu, Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ

*63 "Device Guard overview" (https://technet.microsoft.com/library/dn986865(v=vs.85).aspx).
*64 "Protect derived domain credentials with Credential Guard" (https://technet.microsoft.com/library/dn986865(v=vs.85).aspx).