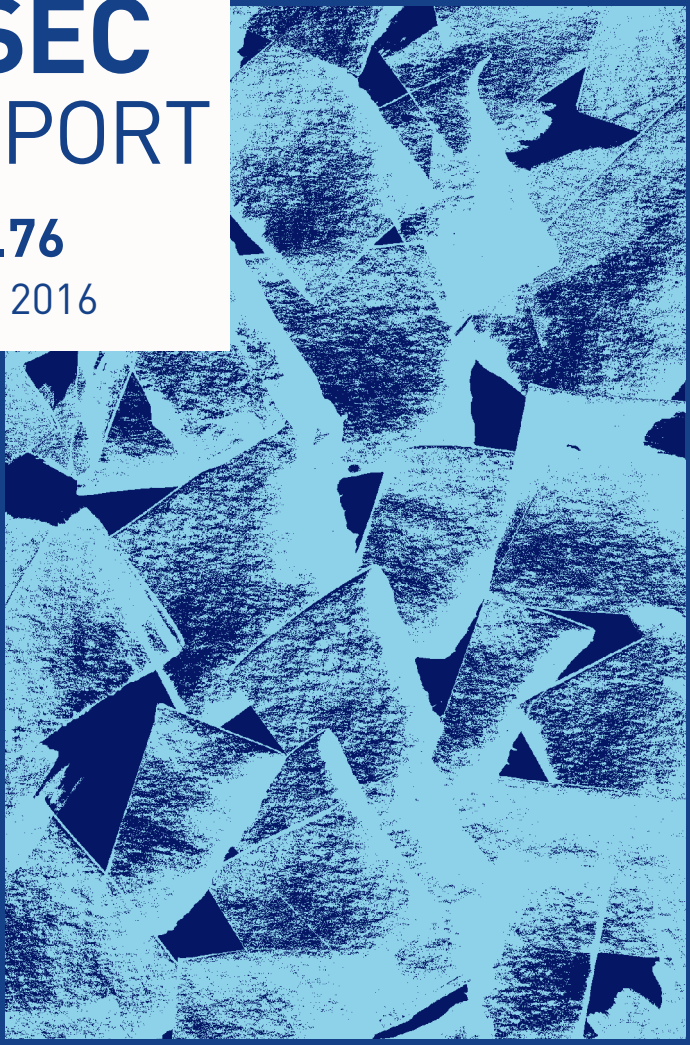
Security Trend

# ASEC REPORT

## VOL.76

April, 2016



AhnLab

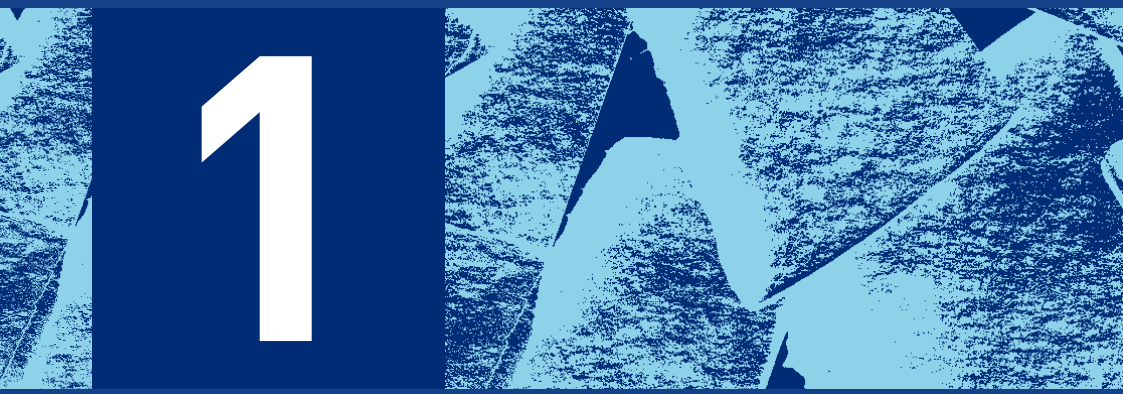
# ASEC REPORT

**VOL.76** April, 2016

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

## SECURITY TREND OF April 2016

Table of Contents



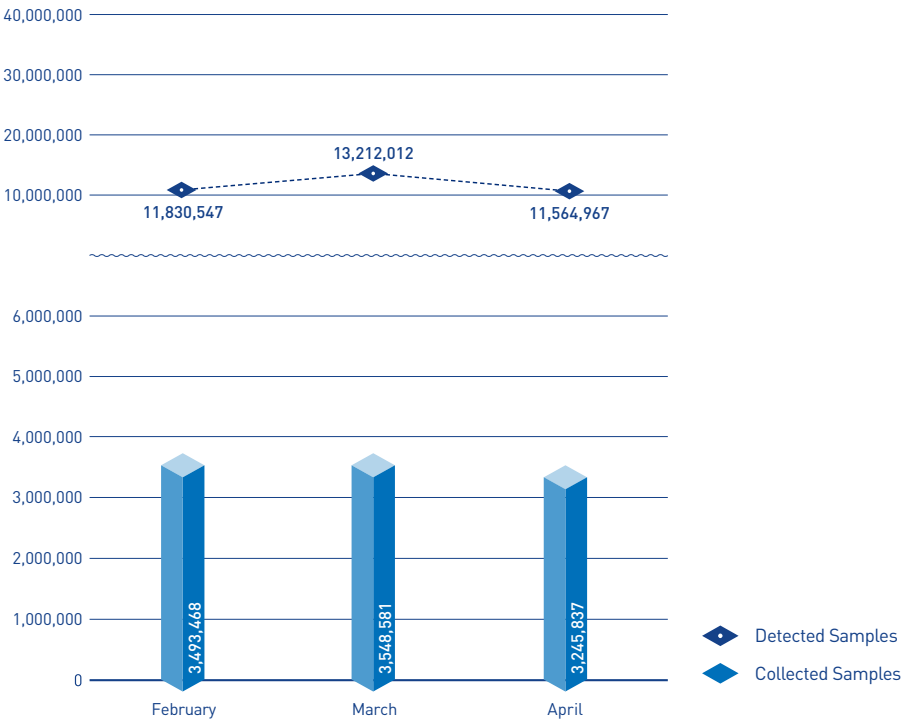
# 1

# SECURITY STATISTICS

## SECURITY STATISTICS

# 01
# Malware Statistics

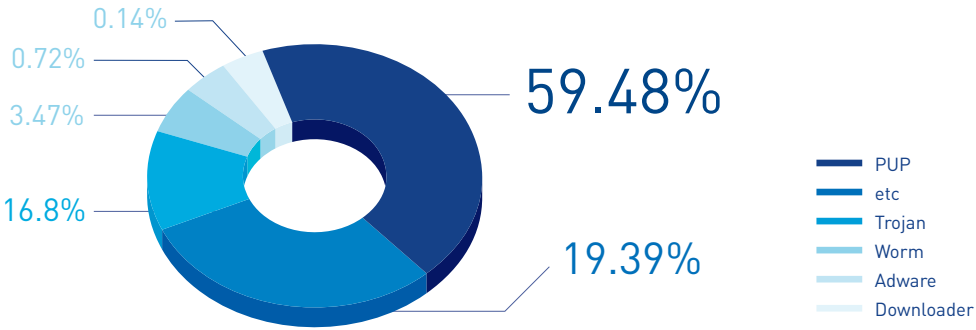
According to the ASEC (AhnLab Security Emergency Response Center), 11,564,967 malware were detected in April 2016. The number of detected malware decreased by 1,647,045 from 13,212,012 detected in the previous month as shown in Figure 1-1. A total of 3,245,837 malware samples were collected in April.




[Figure 1-1] Malware Trend

* "Detected Samples" refers to the number of malware detected by AhnLab products deployed by our customers.
* "Collected Samples" refers to the number of malware samples collected autonomously by AhnLab that were besides our products.

Figure 1-2 shows the prolific types of malware in April 2016. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 59.48% of the total. It was followed by Trojan (16.8%) and Worm (3.47%).




[Figure 1-2] Proportion of Malware Type in April 2016

Table 1-1 shows the Top 10 malware threats in April categorized by alias. Trojan/Win32.Starter was the most frequently detected malware (260,913), followed by Malware/Win32.Generic (129,941).

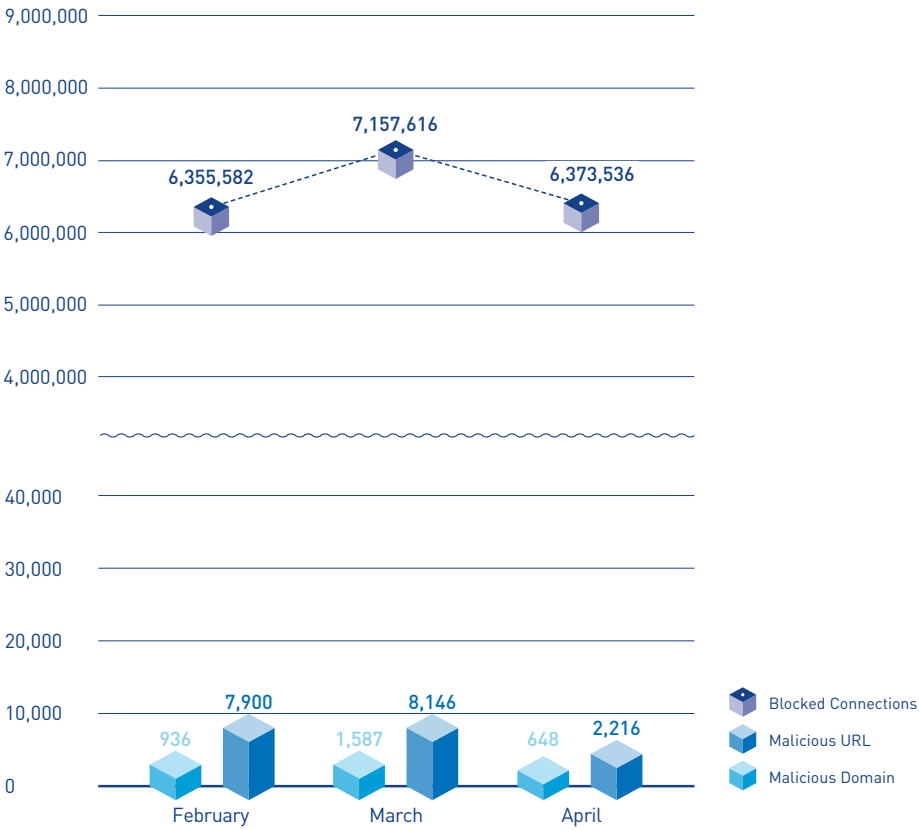
[Table 1-1] Top 10 Malware Threats in April 2016 (by Alias)

| Rank | Alias from AhnLab | No. of detections |
|---|---|---|
| 1 | Trojan/Win32.Starter | 260,913 |
| 2 | Malware/Win32.Generic | 129,941 |
| 3 | Trojan/Win32.Agent | 126,658 |
| 4 | ASD.Prevention | 105,841 |
| 5 | Unwanted/Win32.HackTool | 97,057 |
| 6 | Trojan/Win32.Neshta | 88,807 |
| 7 | Trojan/Win32.Banki | 82,504 |
| 8 | Unwanted/Win32.Keygen | 66,734 |
| 9 | HackTool/Win32.Crack | 66,495 |
| 10 | HackTool/Win32.AutoKMS | 59,478 |

## SECURITY STATISTICS

# 02
# Web Security Statistics

In April 2016, a total of 648 domains and 2,216 URLs were comprised and used to distribute malware. In addition, 6,373,536 malicious domains and URLs were blocked.



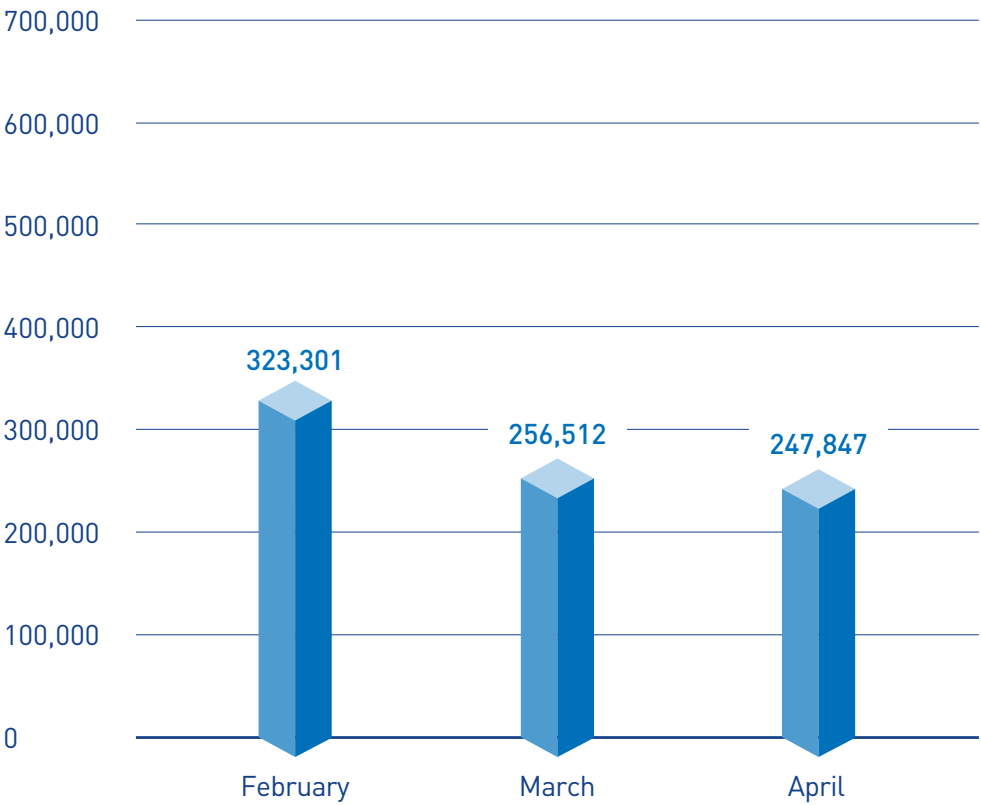

[Figure 1-3] Blocked Malicious Domains/URLs in April 2016

* "Blocked Connections" refers to the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers.

SECURITY STATISTICS

# 03 Mobile Malware Statistics

In April 2016, 247,847 mobile malware were detected as shown in Figure 1-4.




[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in April 2016. Android-PUP/SmsPay was the most distributed malware with 63,488 of the total.

[Table 1-2] Top 10 Mobile Malware Threats in April (by alias)

| Rank | Alias from AhnLab | No. of detections |
|---|---|---|
| 1 | Android-PUP/SmsPay | 63,488 |
| 2 | Android-PUP/SmsReg | 26,873 |
| 3 | Android-PUP/Noico | 20,396 |
| 4 | Android-Trojan/SmsSpy | 9,567 |
| 5 | Android-PUP/Dowgin | 9,315 |
| 6 | Android-PUP/Zdpay | 8,723 |
| 7 | Android-Trojan/SmsSend | 8,110 |
| 8 | Android-Trojan/Moavt | 6,637 |
| 9 | Android-Trojan/FakeInst | 5,783 |
| 10 | Android-Trojan/Agent | 5,035 |

# 2

# SECURITY ISSUE

BillGates Botnet Targets Linux Systems

SECURITY ISSUE

# BillGates Botnet Targets Linux Systems

The BillGates botnet has been recently discovered, which targets systems running Linux operating systems, collecting the infected system's data, overwriting systems files, and mounting DDoS attacks. The malware modifies its attribute itself after infiltrating a system, making it impossible to remove.

Linux operating systems make clear distinctions in user account controls for files, with permission to read, modify and execute files assigned to users (owners), groups and others. Without proper permission, as indicated in Figure 2-1, a file is not allowed to be executed unless a root user changes the file permission settings.

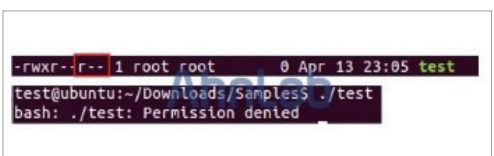



Figure 2-1 | Permission denied (--x) for executing a file created with root permission

The recently-discovered BillGates botnet is related to file types instead of file permission settings, with the attacker modifying the file attributes following the system's infection to prevent the malware from being deleted. This article explains how to delete a malicious file even after attributes have been altered in a system under attack.

First, after the file attribute has been changed by the malware, an attempt to remove the file as shown in Figure 2-2 outputs a message stating "Operation not permitted", and the file is not deleted.

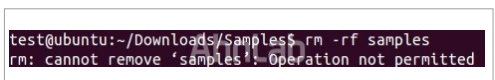



Figure 2-2 | Attempting a removal using the rm command

If the user surmises that permission setting is the reason for the inability to remove the file and makes a second attempt by using the file system information to remove the root account and

the inode, the same message is displayed. Also, the file is still unable to be deleted.

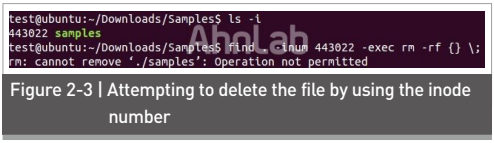



Figure 2-3 | Attempting to delete the file by using the inode number

If removal appears to be impossible as shown in Figure 2-2 and Figure 2-3, checking the file attribute using the "lsattr" command reveals that an "i" attribute has been added, as shown in Figure 2-4.

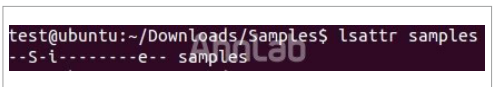



Figure 2-4 | Displaying the file attributes

When the additional "i" attribute has been added, changing the attribute as the root user using the "chattr" command, as shown in Figure 2-5, and then attempting to remove the file will successfully delete it.

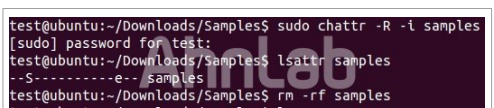



Figure 2-5 | Removing the file after changing the file attribute

File attributes can be modified with '+[attribute to add]' or '-[attribute to remove]', and adding the -R option will apply the changes to all subdirectories. This is similar to the "attrib" command of the Windows operating system.

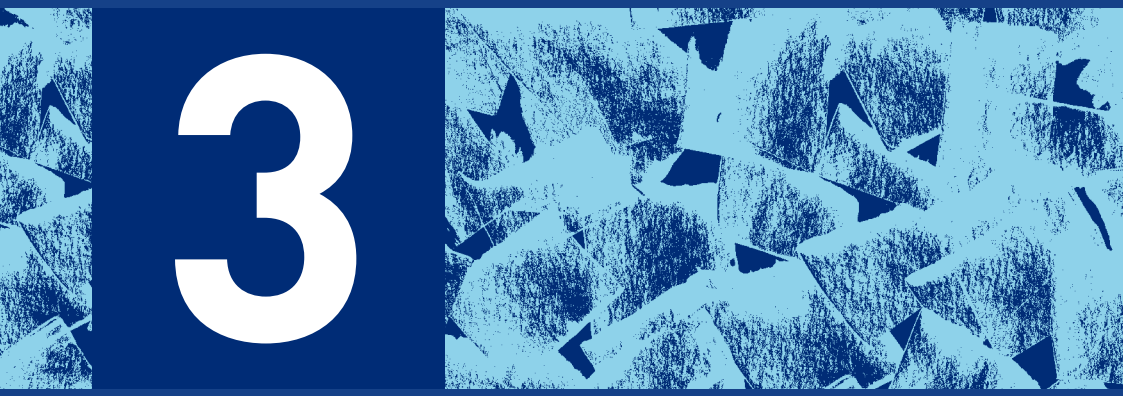
This Linux-targeting malware is the case that shows the necessity to check the file attributes as well as file permission settings as some files may be rendered impossible to remove due to attribute changes. However, key files or log files may be given "i" or "a" attributes under normal circumstances. Not all files with these attributes are malware or affected by malware, and only files verified as such should be removed.

Recently malware targeting Linux systems continue to increase, , with their modes of attack diversifying to include DDoS attacks or backdoor exploits, and are expected to continue to evolve and advance. Passwords must be set to ensure a safe Linux environment, and the latest security updates should be applied.

The relevant alias identified by V3 products, AhnLab's anti-virus program, are as below:

**<Alias identified by V3 products>**

Linux/Backdoor.1223123.B



# 3

# IN-DEPTH ANALYSIS

Ransomware "Jigsaw" Not Playing Games

IN-DEPTH ANALYSIS

# Ransomware "Jigsaw" Not Playing Games

A new ransomware has recently surfaced to strike fear into users. The ransomware, Jigsaw, is named after the eponymous villain of the "Saw" movie franchise.

Figure 3-1 | Jigsaw's puppet from the movie "Saw"

The character in the movies begins his killing spree by delivering his trademark greeting, "I want to play a game," via an unsettlingly-looking puppet. The ransomware also displays a message inspired by the movie as shown in Figure 3-2 to inform the user of the system's infection.


Figure 3-2 | Pay-up warning dialogue of Jigsaw ransomware

A message tells the user that documents, photographs, videos and other files have been encrypted, demanding a ransom in Bitcoins as shown in Figure 3-2. The message also warns that encrypted files will be deleted every hour, and shows a clock counting down from 60 minutes to give more pressure the victim in an attempt to make him or her pay.

This ransomware is registered as a startup program and runs automatically

after booting the system. When the system is infected by Jigsaw ransomware, files with the extensions listed in Table 3-1 in the system are encrypted. After the files are encrypted, they are given a new extension, .fun.

Table 3-1 | File extensions targeted for encryption

.jpg, .jpeg, .raw, .tif, .gif, .png, .bmp , .3dm, .max, .accdb, .db, .dbf, .mdb, .pdb, .sql, .dwg, .dxf, .c, .cpp, .cs, .h, .php, .asp, .rb, .java, .jar, .class, .py, .js, .aaf, .aep, .aepx, .plb, .prel, .prproj, .aet, .ppj, .psd, .indd, .indl, .indt, .indb, .inx, .idml, .pmd, .xqx, .xqx, .ai, .eps, .ps, .svg, .swf, .fla, .as3, .as, .txt, .doc, .dot, .docx, .docm, .dotx, .dotm, .docb, .rtf, .wpd, .wps, .msg, .pdf, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .ppt, .pot, .pps, .pptx, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .sldx, .sldm, .wav, .mp3, .aif, .iff, .m3u, .m4u, .mid, .mpa, .wma, .ra, .avi, .mov, .mp4, .3gp, .mpeg, .3g2, .asf, .asx, .flv, .mpg, .wmv, .vob, .m3u8, .dat, .csv, .efx, .sdf, .vcf, .xml, .ses, .Qbw, .QBB, .QBM, .QBI, .QBR , .Cnt, .Des, .v30, .Qbo, .Ini, .Lgb, .Qwc, .Qbp, .Aif, .Qba, .Tlg, .Qbx, .Qby , .1pa, .Qpd, .Txt, .Set, .lif , .Nd, .Rtp, .Tlg, .Wav, .Qsm, .Qss, .Qst, .Fx0, .Fx1, .Mx0, .FPx, .Fxr, .Fim, .ptb, .Ai, .Pfb, .Cgn, .Vsd, .Cdr, .Cmx, .Cpt, .Csl, .Cur, .Des, .Dsf, .Ds4, , .Drw, .Dwg.Eps, .Ps, .Prn, .Gif, .Pcd, .Pct, .Pcx, .Plt, .Rif, .Svg, .Swf, .Tga, .Tiff, .Psp, .Ttf, .Wpd, .Wpg, .Wi, .Raw, .Wmf, .Txt, .Cal, .Cpx, .Shw, .Clk, .Cdx, .Cdt, .Fpx, .Fmv, .Img, .Gem, .Xcf, .Pic, .Mac, .Met, .PP4, .Pp5, .Ppf, .Xls, .Xlsx, .Xlsm, .Ppt, .Nap, .Pat, .Ps, .Prn, .Sct, .Vsd, .wk3, .wk4, .XPM, .zip, .rar

The list of infected files are saved as EncryptedFileList.txt in C:\Users\[User name]\AppData\Roaming\System32Work\, which contains a list of infected and deleted files.

Developed using the .net framework, new variants of Jigsaw are being constantly discovered. Analysis of Jigsaw variants collected by AhnLab reveals certain common factors, such as the encryption and decoding codes and a pattern of disguising file types as Firefox, the browser, indicating that the same threat factor appears to be continuously creating and releasing variants.


Figure 3-3 | Part of Jigsaw's source code

Latest types of ransomware tend to play on the user's fear and anxiety to extort payment. They are also becoming more technologically intricate and advanced. Restoring infected files is practically impossible since ransomware uses an encryption algorithm to scramble files. To minimize possible damages from ransomware, suspicious emails should be deleted immediately if possible and users should exercise extra vigilance such as backing up important data.

The relevant aliases of Jigsaw identified by V3 products, AhnLab's anti-virus program, are as below:

**<Aliases identified by V3 products>**

Trojan/Win32.Filecoder (2016.04.14.05)
Trojan/Win32.Filecoder (2016.04.14.05)
Trojan/Win32.Ransom (2016.04.13.09)
Trojan/Win32.Agent (2016.04.14.04)
Trojan/Win32.Agent (2016.04.14.04)
Trojan/Win32.Jigsaw (2016.04.12.03)

AhnLab

# ASEC REPORT

VOL.76
April, 2016

| | | | |
|---|---|---|---|
| Contributors | **ASEC Researchers** | Publisher | **AhnLab, Inc.** |
| Editor | **Content Creatives Team** | Website | **www.ahnlab.com** |
| Design | **Design Team** | Email | **global.info@ahnlab.com** |