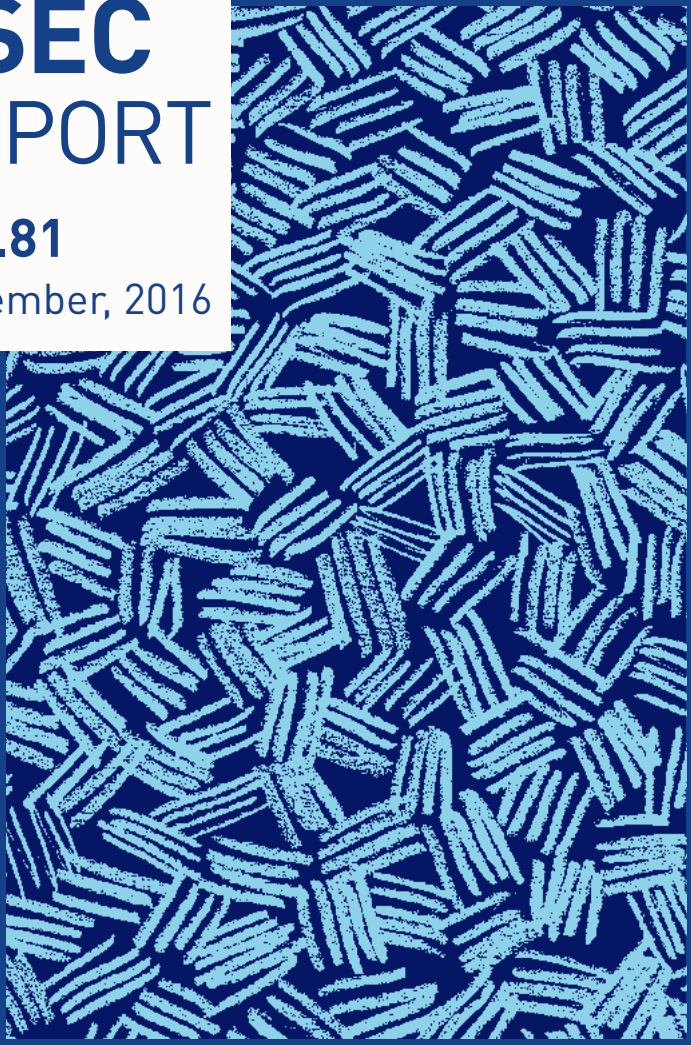
Security Trend

ASEC REPORT

VOL.81

September, 2016



AhnLab

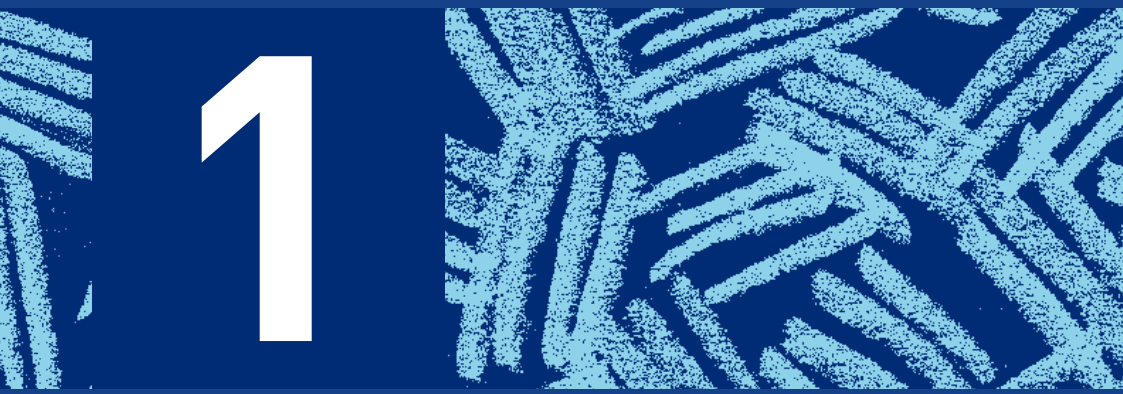
ASEC REPORT

VOL.81 September, 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 September 2016

Table of Contents



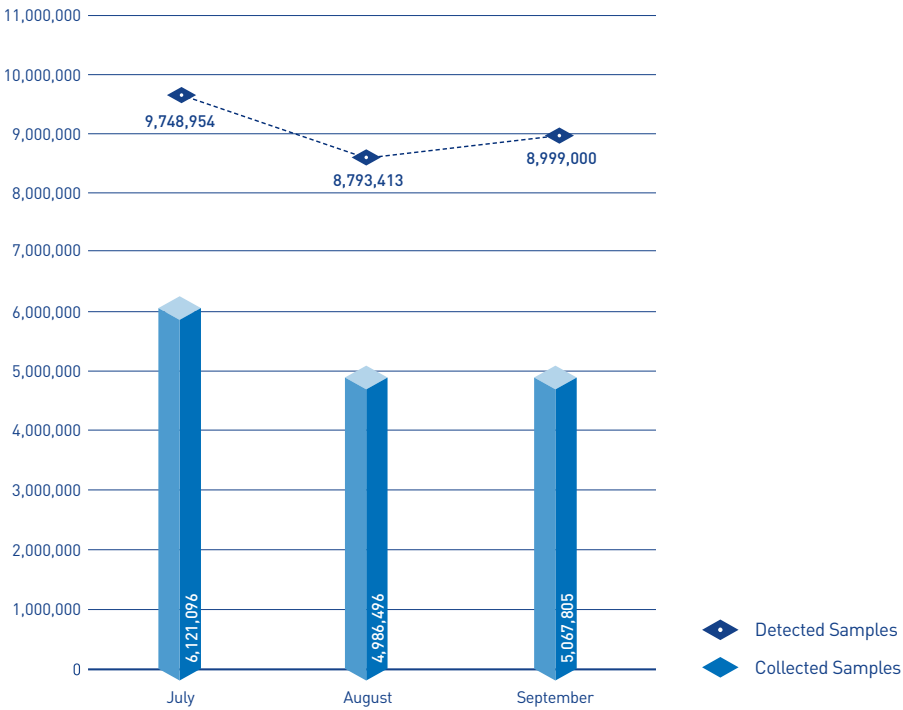
1

SECURITY STATISTICS

SECURITY STATISTICS

01 Malware Statistics

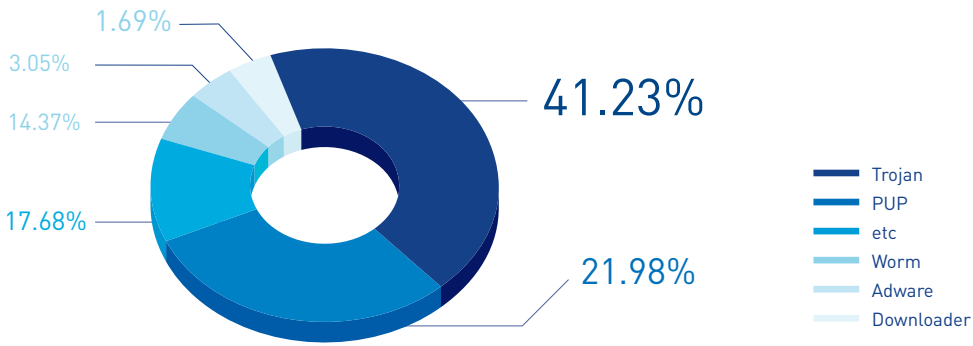
According to the ASEC (AhnLab Security Emergency Response Center), 8,999,000 malware were detected in September 2016. The number of detected malware increased by 205,587 from 8,793,413 detected in the previous month as shown in Figure 1-1. A total of 5,067,805 malware samples were collected in September.



[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 September 2016. It appears that Trojan was the most distributed malware with 41.23% of the total. It was followed by PUP(Potentially Unwanted Program, 21.98%) and Worm (14.37%).



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

Table 1-1 shows the Top 10 malware threats in September categorized by alias. Malware/Win32.Generic was the most frequently detected malware (364,620), followed by Trojan/Win32.Starter (237,449).

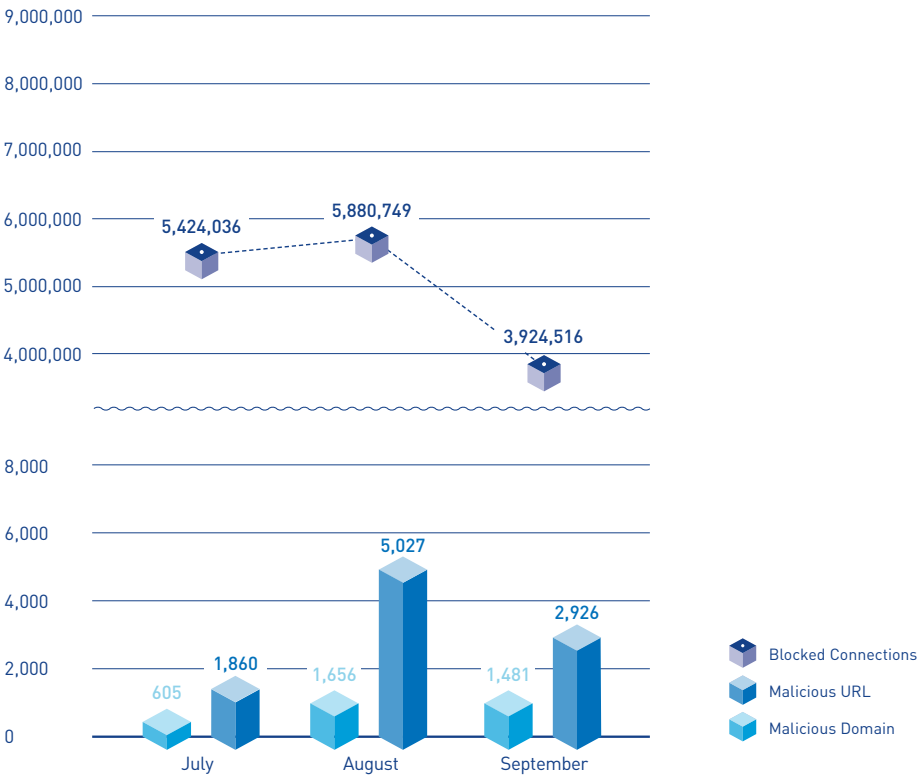
[Table 1-1] Top 10 Malware Threats in September 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Malware/Win32.Generic	364,620
2	Trojan/Win32.Starter	237,449
3	Unwanted/Win32.HackTool	136,623
4	Trojan/Win32.Agent	84,673
5	Trojan/Win32.Neshta	80,937
6	HackTool/Win32.Crack	72,632
7	Trojan/Win32.Banki	68,817
8	ASD.Prevention	60,727
9	Unwanted/Win32.Keygen	57,950
10	Trojan/Win32.OnlineGameHack	55,808

SECURITY STATISTICS

02
Web Security Statistics

In September 2016, a total of 1,481 domains and 2,926 URLs were comprised and used to distribute malware. In addition, 3,924,516 malicious domains and URLs were blocked.



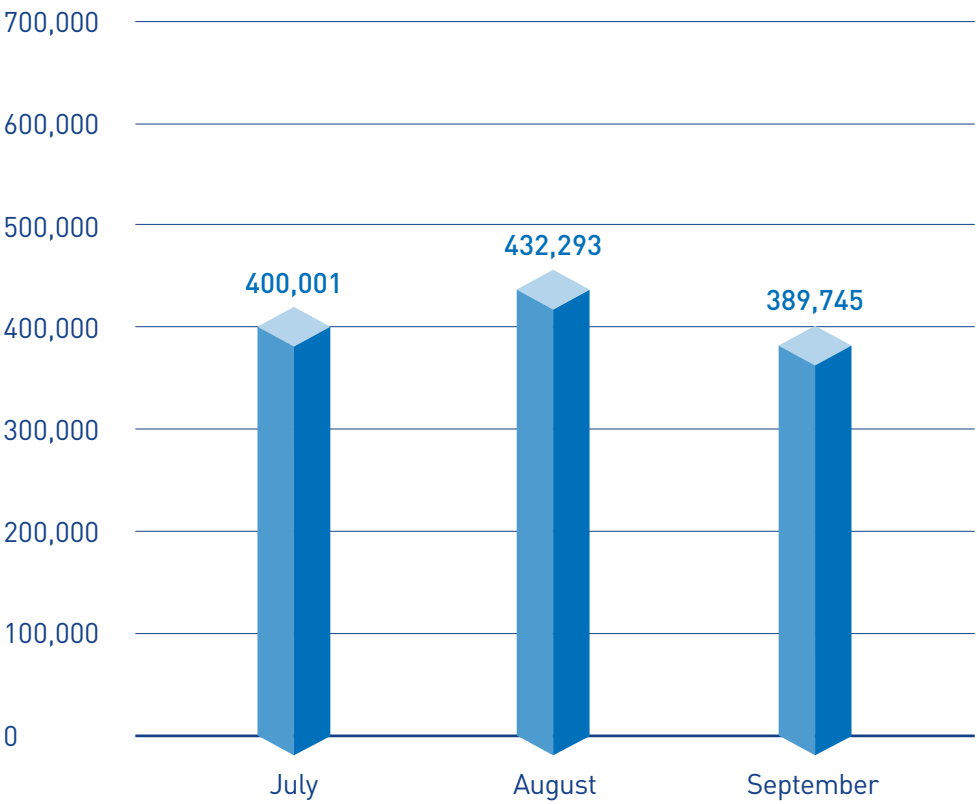
[Figure 1-3] Blocked Malicious Domains/URLs in September 2016

* "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 September 2016, 389,745 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 September 2016. Android-PUP/SmsPay was the most distributed malware with 109,366 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	109,366
2	Android-PUP/Shedun	60,317
3	Android-PUP/SmsReg	29,238
4	Android-PUP/Noico	23,426
5	Android-PUP/Zdpay	19,957
6	Android-PUP/Agent	15,889
7	Android-Trojan/AutoSMS	11,700
8	Android-Trojan/Agent	9,802
9	Android-PUP/Dowgin	8,352
10	Android-Trojan/Shedun	7,939

2

SECURITY ISSUE

Ransomware Downloader in HTA File Format Appears

SECURITY ISSUE

Ransomware Downloader in HTA File Format Appears

With the relentless ransomware threat showing no sign of easing off, a new type of ransomware downloader in the *.hta file format has recently been discovered. Short for "HTML Application" files, HTA files are unique in that they are launched and run like an application, unlike HTML files that run via a Web browser. The recently-discovered HTA ransomware downloader exploits this feature to distribute ransomware.

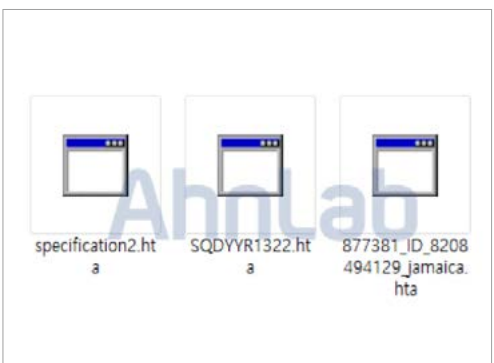


Figure 2-1 | HTA format ransomware downloader

HTA ransomware downloaders, shown in Figure 2-1, are usually distributed as attachments in spam emails, written in obfuscated script to make them difficult to analyze.

Figure 2-2 | HTA file run screen

Running the malicious HTA file produces a program window as shown in Figure 2-2 instead of the Web browser window, and the HTA file uses the normal Windows file mshta.exe to launch the malicious script.

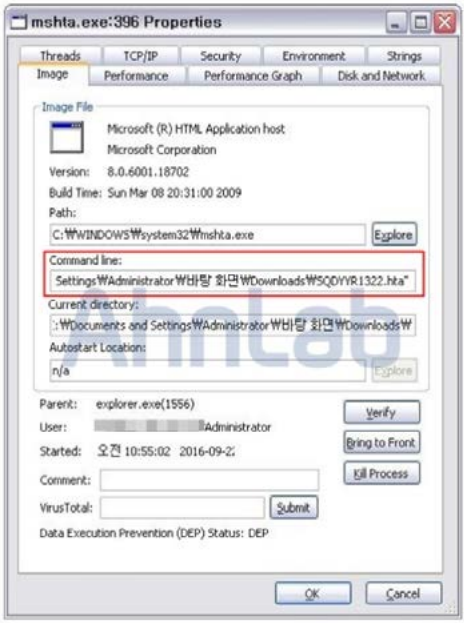


Figure 2-3 | mshta.exe properties

As shown in Figure 2-3, an examination of the command line value in the file properties of the mshta.exe file reveals the HTA file in the download path being run.

The malware then attempts network connections with the addresses shown in Table 2-1. The malware is designed to download the Cerber ransomware to the victim's PC via the network connection. However, no additional malicious activities took place after the connection was made when the malware was being analyzed.

Table 2-1 | Network connection information

207.179.106.94:80
198.46.82.242:80
70.39.235.94:80

This case illustrates the facts that directly running an PE file is not the only vector for a ransomware infection. An attack can also take place when a file downloaded by an HTA downloader is executed. A wide range of files with different extensions are being used as ransomware downloaders, the most common of which are *.js, *.wsf and *.hta.

If a user, therefore, receives a spam email message containing a file with one of these extensions should not open or execute the file. Since malicious script files that download ransomware are often run via wscript.exe and mshta.exe, which are normal windows programs, users should perform a system check if these programs are found to be running without

the user's recognition or intent.

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

<Alias identified by V3 products>

JS/Downloader (2016.09.21.00)

3

IN-DEPTH ANALYSIS

Ransomware Disguised as Windows Updates Showed Up

IN-DEPTH ANALYSIS

Ransomware Disguised as Windows Updates Showed Up

New ransomware disguised as an update for the Windows operating system have recently been spotted, requiring users to exercise extra caution. Since security updates for operating systems including Windows and applications have long been touted one of the best ways of protecting systems, these new ransomware disguised as such updates have the potential to cause considerable havoc.

■ English-language Windows OS Ransomware

Figure 3-1 | Fake Windows update progress screen

One of Windows OS update disguised ransomware is so-called Fantom; it is disguised as a Windows 10 update. The malware creates a file named "WindowsUpdate.exe" in the user's PC. The malware then creates a screen disguised as an important Windows update as shown in Figure 3-1. While the fake progress screen is active, the ransomware encrypts the files stored in the system. Like most existing types of ransomware, almost every type of file is encrypted, and when the process is complete the files are given a ".fantom" extension.

Fantom then alters the system's desktop background and creates a file named "DECRYPT_YOUR_FILES.HTML" that informs the victim of the system's infection and instructions on freeing the affected files. In addition, "%APPDATA%\delback.bat" is created that deletes VCS

(volume shadow copy) files to prevent system restoration.

■ Russian-language Windows OS Ransomware

There has been an another ransomware, which is so-called RAA ransomware, discovered to target Russian-language Windows systems. RAA ransomware also disguises itself as a Windows update to lure users into running it.

RRA ransomware is distributed in the form of a document file, and clicking on the file will display a popup message informing the user, "This file has been created using the latest version of Microsoft Office Word. Download the official update package to view the document" in Russian as shown in Figure 3-2.

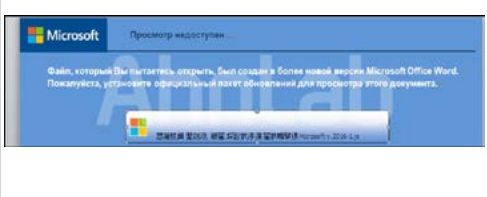


Figure 3-2 | DOC file containing the RAA ransomware (JS)

There is an installation button in the bottom of the message that shows the Microsoft logo, luring unsuspecting users to run the purported update. A script embedded internally that contains a set of malicious code, shown in Table 3-1, is run when the user executes the installation.

Table 3-1 | Code information for malicious activities

1. Duplicates the script t the My Documents folder - dfsdb.js
2. Encrypts files with specific extensions
3. Decrypts and creates data encoded in base64 (ransom note, executable file)
4. Accesses pre-designated URLs

An analysis of the malicious script revealed code for file encryption as shown in Figure 3-3. In addition, parts of the script are obfuscated as shown in Figure 3-4 to prevent the user from identifying them, and no other information on accessing URLs could be found other than the presence of an "href" tag (google.com).

Figure 3-3 | Part of the script for encoding and altering affected files

Figure 3-4 | Obfuscated script, and the lines for file encryption and executable generation

Once the file encryption is under way, the ransomware searches for target file extensions using JavaScript indexOff. The ransomware also searches files with extensions listed below in Table 3-2, which thus includes document files with .docm, .docx, and .xlsx extensions.

Table 3-2 | File extensions targeted for encryption

.doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar, csv

The executable file generated by the malicious script (ii.exe) attempts to make a network connection, but at the time of analyzing the malware failed to connect to the C&C server and no additional features could be identified. The infection message displayed by RAA ransomware is as shown in Figure 3-5.

Figure 3-5 | RAA ransomware infection message

■ Conclusion

New and variants of ransomware continues to be generated and distributed. To minimize the potential damages from ransomware attacks, users should apply the latest security updates for the

operating system and key programs, and keep important data backed up regularly. Like this case, however, some ransomware may be disguised as software updates and users should ensure that any OS or program updates are carried out via the software developer's official Web site.

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

<Aliases identified by V3 products>

Trojan/Win32.Tear (2016.08.26.03)

DOC/Downloader (2016.09.01.00)

JS/Downloader (2016.09.01.00)

Trojan/Win32.Upbot (2016.08.30.03)

AhnLab

ASEC REPORT

VOL.81
September, 2016

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