Security Trend

ASEC REPORT

VOL.82

October, 2016

AhnLab

ASEC REPORT

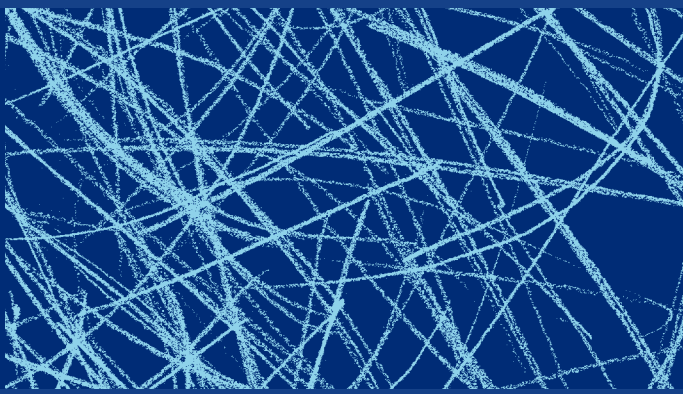
VOL.82 October, 2016

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 October 2016

Table of Contents

1

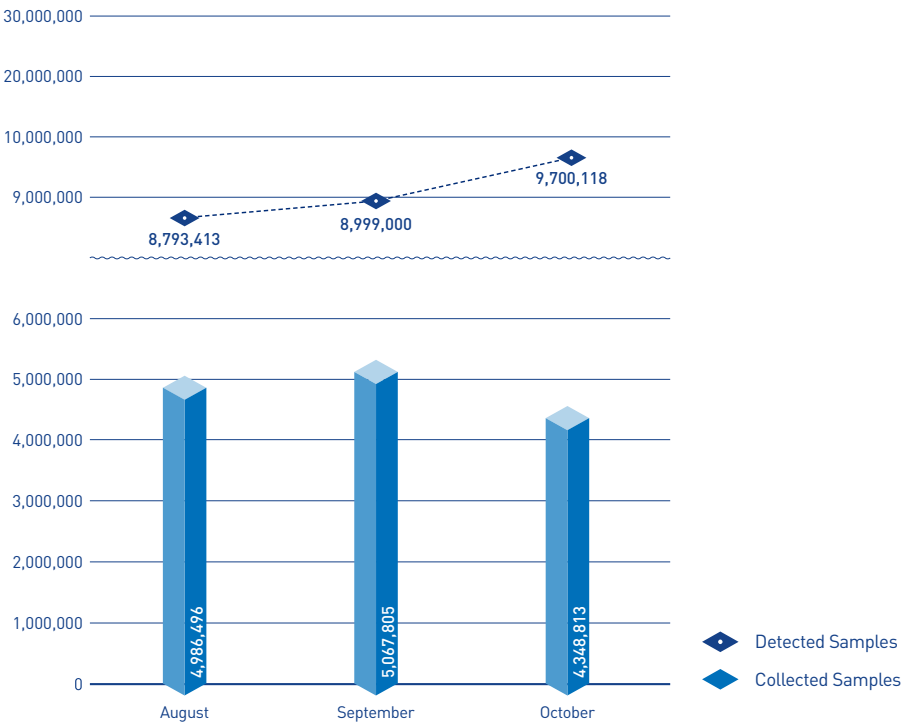


SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

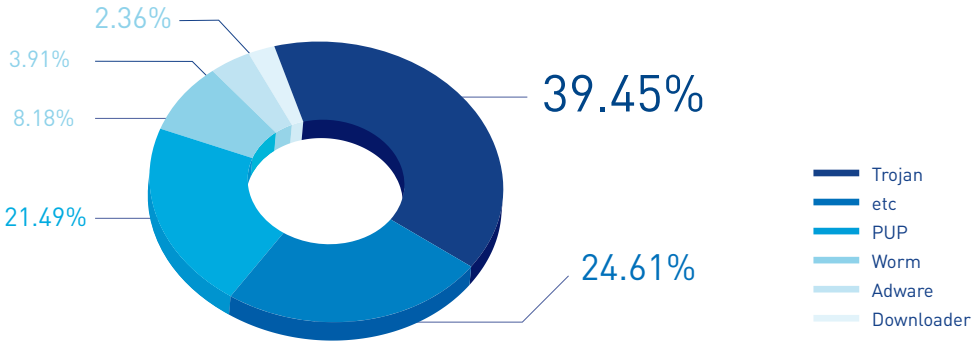
According to the ASEC (AhnLab Security Emergency Response Center), 9,700,118 malware were detected in October 2016. The number of detected malware increased by 701,118 from 8,999,000 detected in the previous month as shown in Figure 1-1. A total of 4,348,813 malware samples were collected in October.



[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 October 2016. It appears that Trojan was the most distributed malware with 39.45% of the total. It was followed by PUP(Potentially Unwanted Program, 21.49%) and Worm (8.18%).



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

Table 1-1 shows the Top 10 malware threats in October categorized by alias. Malware/Win32.Generic was the most frequently detected malware (269,368), followed by Trojan/Win32.Starter (207,927).

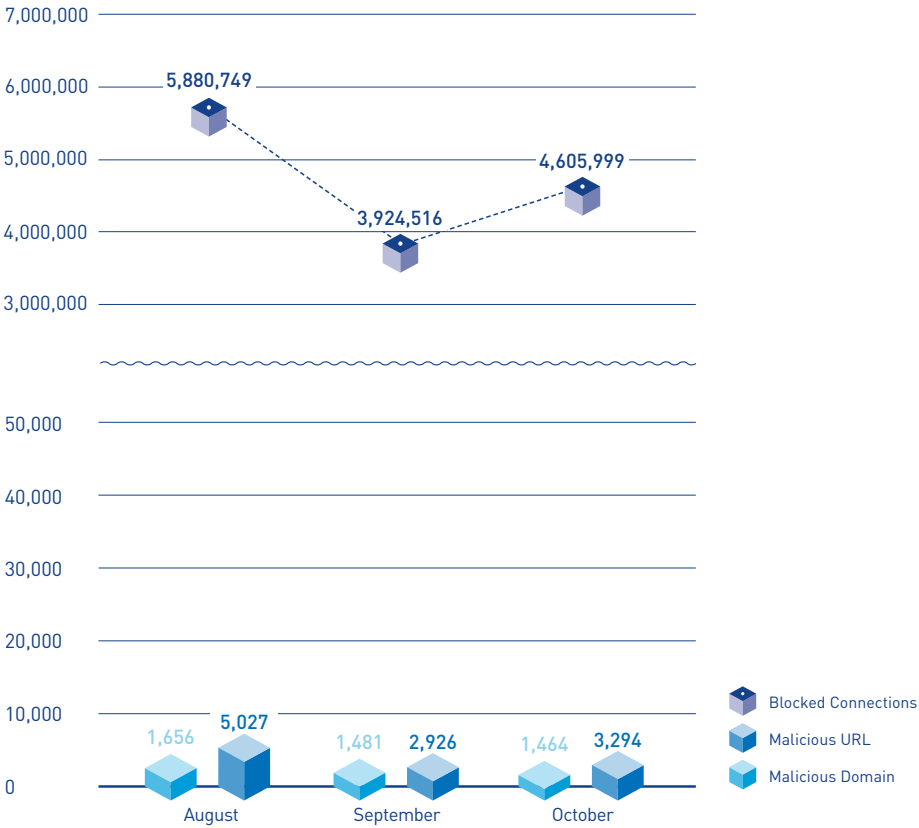
[Table 1-1] Top 10 Malware Threats in October 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Malware/Win32.Generic	269,368
2	Trojan/Win32.Starter	207,927
3	HackTool/Win32.KMSAuto	144,305
4	Trojan/Win32.Banki	141,351
5	Unwanted/Win32.HackTool	129,318
6	Unwanted/Win32.KMS	123,049
7	Worm/Win32.IRCBot	96,306
8	Trojan/Win32.Agent	90,254
9	Trojan/Win32.Neshta	86,531
10	HackTool/Win32.Crack	62,890

SECURITY STATISTICS

02
Web Security Statistics

In October 2016, a total of 1,464 domains and 3,294 URLs were comprised and used to distribute malware. In addition, 4,605,999 malicious domains and URLs were blocked.



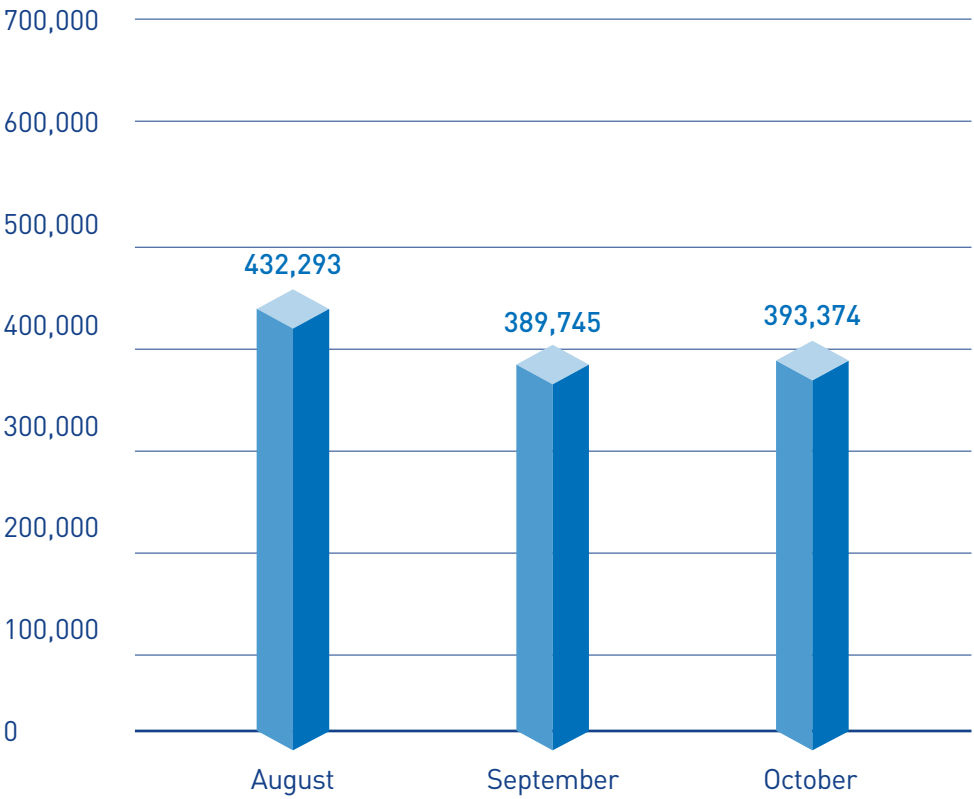
[Figure 1-3] Blocked Malicious Domains/URLs in October 2016

* "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 October 2016, 393,374 mobile malware were detected as shown in Figure 1-4.

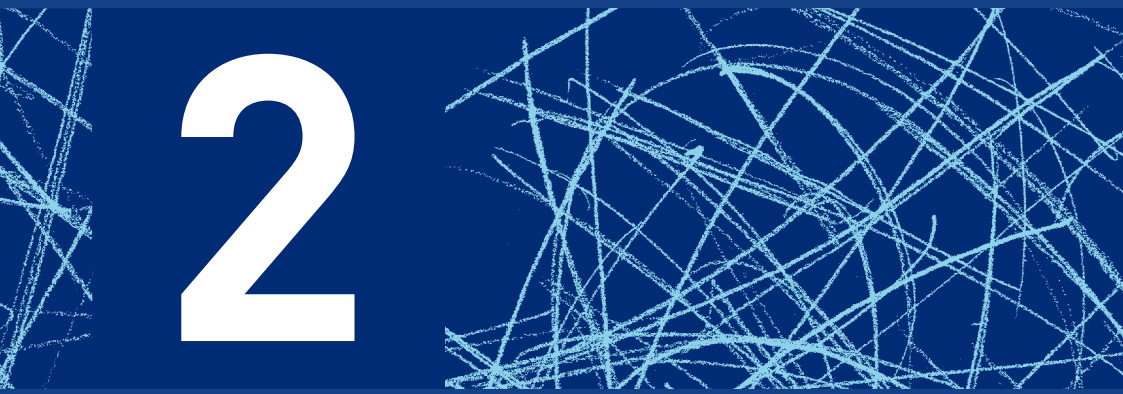


[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in October 2016. Android-PUP/SmsPay was the most distributed malware with 55,675 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	55,675
2	Android-PUP/Shedun	37,948
3	Android-PUP/Baogifter	31,087
4	Android-PUP/SmsReg	28,336
5	Android-PUP/Agent	27,592
6	Android-Trojan/FakeInst	26,767
7	Android-Trojan/SmsSend	12,471
8	Android-Trojan/Shedun	10,045
9	Android-PUP/Noico	9,590
10	Android-Trojan/AutoSMS	9,012



2

SECURITY ISSUE

Ransomware Targets Users During U.S. Elections

SECURITY ISSUE

Ransomware Targets Users During U.S. Elections

The eyes of the world were on the American presidential elections as the polling stations opened after months of fierce campaigning on November 8. Social issues that attract the attention of the public invariably draw in hackers as well, and a strain of ransomware found earlier in October is one such indication. Discovered during the height of the presidential campaign in October, this particular ransomware uses the imagery of then-candidate, Donald J. Trump.

Spotted in October, the ransomware uses an image of Trump in the infection message. According to the analysis result of AhnLab's security researchers, it is assumed that the malware was created around August 19. A silver lining seems to be the fact that the ransomware's key functions such as encryption did not appear to be functioning properly at the time of discovery, meaning that the ransomware may not have caused any real damage during the month of October. Another possibility is that a version still under development had been leaked.

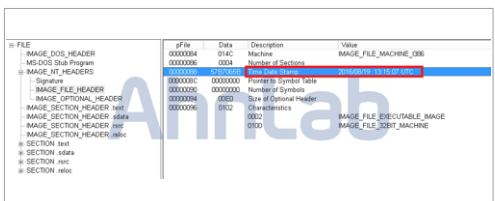


Figure 2-1 | Donald Trump ransomware properties information

An examination of the ransomware's resource properties shows the label CRPT-TRX, which seems to be a shortened form of CRyPTor-Trump, an amalgamation of the words Encrypt, Tor network, and Trump.

An unexpected error message appeared while the ransomware was being run for analysis. The error, related to the .NET Framework, showed that the ransomware is only able to run in .NET Framework

4.0.30319 or higher. However, running the ransomware after installing the appropriate .NET Framework version still failed to create specific files or initiate encryption of system files, revealing the rans ransomware to be still incomplete.

When the ransomware is executed, an "encrypt" folder is created and the files are stored in the folder renamed to random strings, and extensions changed to .ENCRYTED. However, the encrypted files are still readily opened and accessed, showing that only the names was changed and the ransomware is not fully functional.

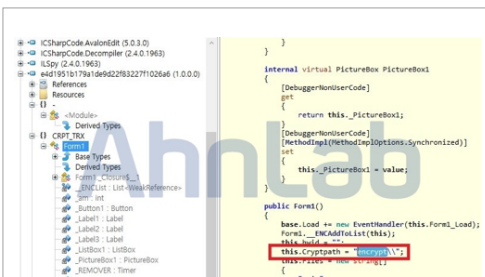


Figure 2-2 | Subfolder named "encrypt" created

Once a subfolder named "encrypt" is created and the ransomware runs again, it finally appeared to function as designed. A unique hardware ID is displayed at the top of the infection message, along with a picture of Donald Trump and a status indicator showing that files are being encrypted. A list of files in the subfolder is displayed below. The file names appear in their original forms on the list.

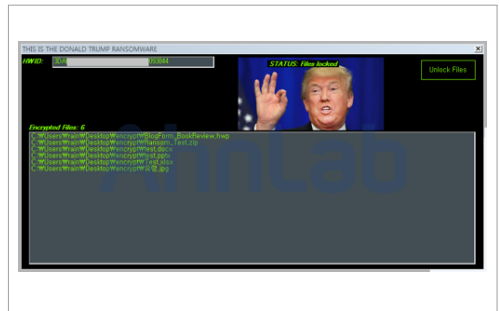


Figure 2-3 | Ransomware execution message

Once the ransomware runs, the files in the "encrypt" subfolder are indicated to be encrypted. The files are renamed with random characters, and extensions changed to .ENCRYPTED.

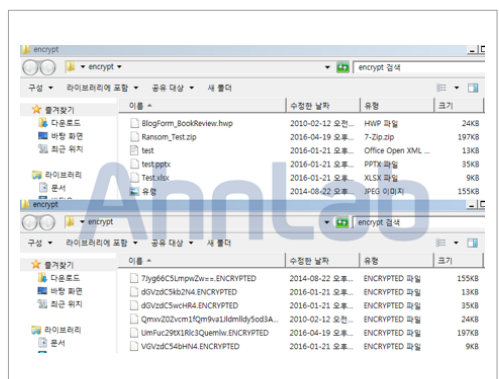


Figure 2-4 | File extensions changed to .ENCRYPTED

A check of the listed of file extensions targeted for encryption included within the code shows a list of files that are not dissimilar to other types of ransomware as shown in Figure 2-5.

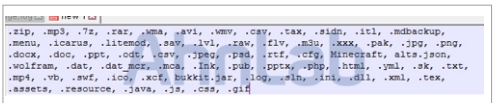


Figure 2-5 | File extensions targeted for encryption

As shown in Figure 2-6, an "Unlock Files" button appears on the top right corner of the message screen. Clicking on the button restores the files names to their original. However, another error message appears. The ransomware runs in a loop using the list of files, but does not shut down properly when the list value becomes "0" and creates n error. In fact, the "Encrypted Files" indicator in the middle of the message shown in Figure 2-6 continued to show a negative number.

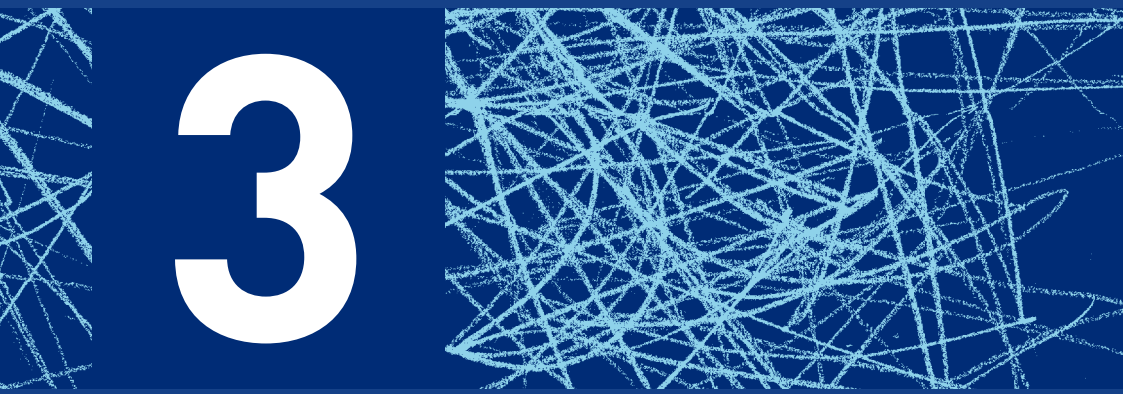
Figure 2-6 | Error message when "Unlock Files" is clicked

However, as noted earlier, opening the files supposedly encrypted by the ransomware showed that they were still untouched, with only the file names altered.

Examining the innards of the ransomware indeed showed that an encryption module exists but the module is not called during the encryption process. However, should this ransomware ever be completed or modified and distributed, it has the capability to encrypt files and cause damages. Users should stay vigilant, especially since similarly election-themed ransomware may continue to be distributed even after the elections in the United States are over.

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

<Alias identified by V3 products>
Trojan/Win32.CryptTRX(2016.09.30.06)



3

IN-DEPTH ANALYSIS

"Spear Phishing" Tries to Skewer User's Trust

IN-DEPTH ANALYSIS

"Spear Phishing" Tries to Skewer User's Trust

Whereas phishing emails in the past tended to attempt netting a large number of random targets, a recent spate of attacks has been targeting certain members of companies and organizations. The name of these attacks, "spear phishing", is a portmanteau of the words spear fishing, for its pinpoint nature, and phishing, the endemic practice of sending out fraudulent emails and other methods designed to trick users.

Spear phishing is commonly used as the attack trigger of Advanced Persistent Threats (APTs) due to their higher success rate made possible by targeting select individuals or groups of individuals. A series of such attacks have recently been uncovered.

These spear phishing attacks used an email inviting users to increase the size of their email storage as shown in Figure 3-1. Clicking on the link in the message, labeled "increase your storage capacity", takes the user to a Web site created by the attacker.

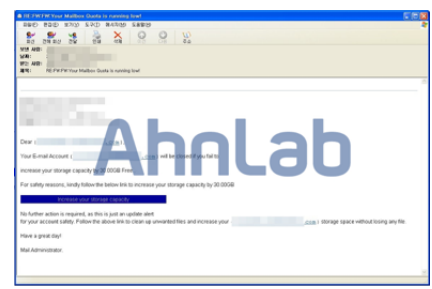


Figure 3-1 | Recently-discovered spear phishing email

Clicking on the link in the email message directs the user to a Web page designed to resemble a well-known email prgram as shown in Figure 3-2. Since the user had already received the email to his or her own email account, it is likely that the user will unsuspectingly begin filling out the email address and password.

Figure 3-2 | Fake phishing site

Once the user enters his or her password, the information is transmitted to the perpetrator's domain address as shown in Figure 3-3.

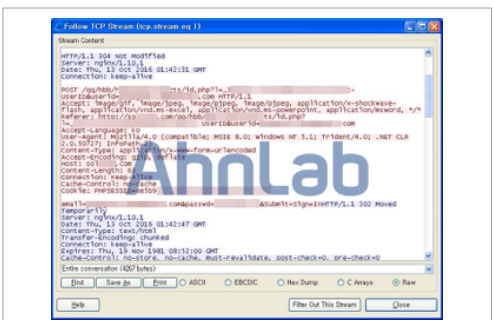


Figure 3-3 | Pilfered password being sent

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

<Alias identified by V3 products>
HTML/Phishing (2016.10.13.00)

While this attack simply tricks users into giving up their email password, more advanced spear phishing attacks often transition into an APT attack to extract sensitive information from government agencies or destroy a vital system.

Users should avoid opening emails hose origins are uncertain, and should especially take caution not to click on suspicious attachments or links.

AhnLab

ASEC REPORT

VOL.82
October, 2016

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