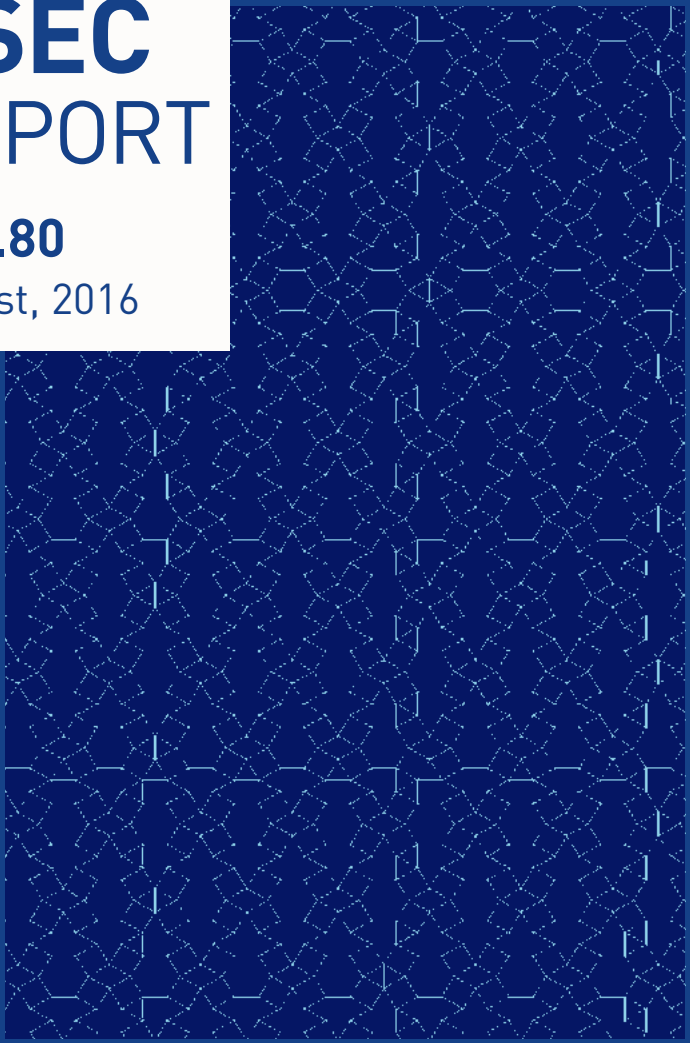
Security Trend

# ASEC REPORT

## VOL.80

August, 2016



AhnLab

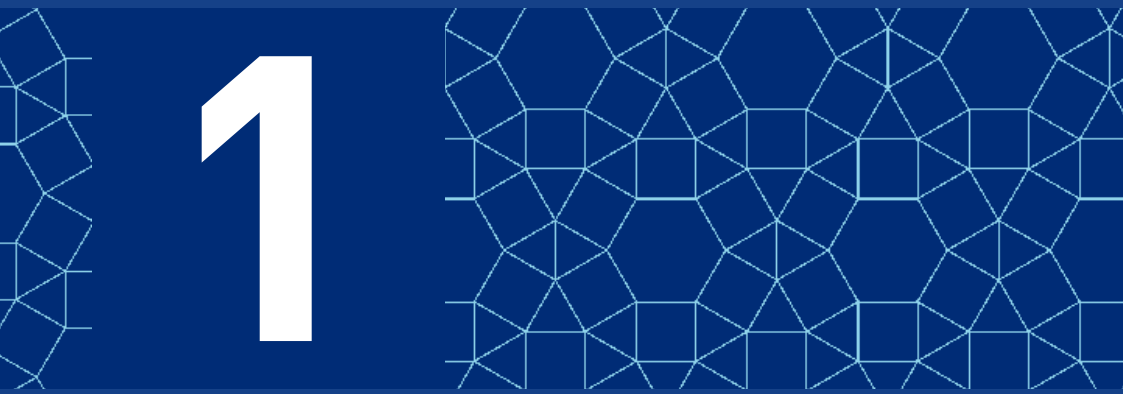
# ASEC REPORT

**VOL.80** August, 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 August 2016

Table of Contents



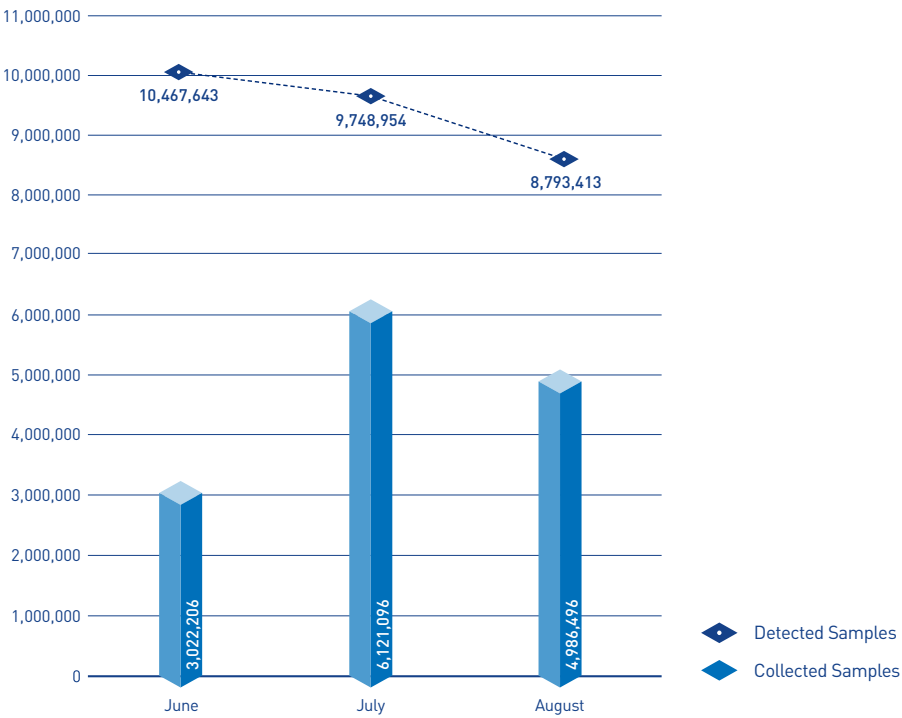
# 1

# SECURITY STATISTICS

## SECURITY STATISTICS

# 01
# Malware Statistics

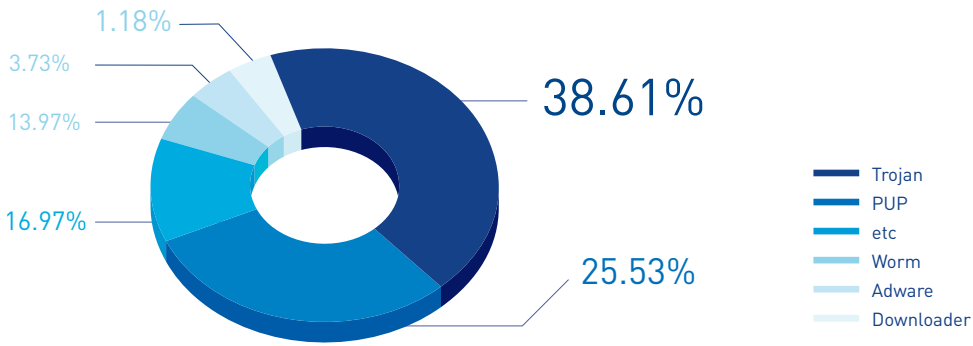
According to the ASEC (AhnLab Security Emergency Response Center), 8,793,413 malware were detected in August 2016. The number of detected malware decreased by 955,541 from 9,748,954 detected in the previous month as shown in Figure 1-1. A total of 4,986,496 malware samples were collected in August.




[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 August 2016. It appears that Trojan was the most distributed malware with 38.61% of the total. It was followed by PUP(Potentially Unwanted Program, 25.53%) and Worm (13.97%).




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

Table 1-1 shows the Top 10 malware threats in August categorized by alias. Malware/Win32.Generic was the most frequently detected malware (218,089), followed by Trojan/Win32.Starter (183,507).

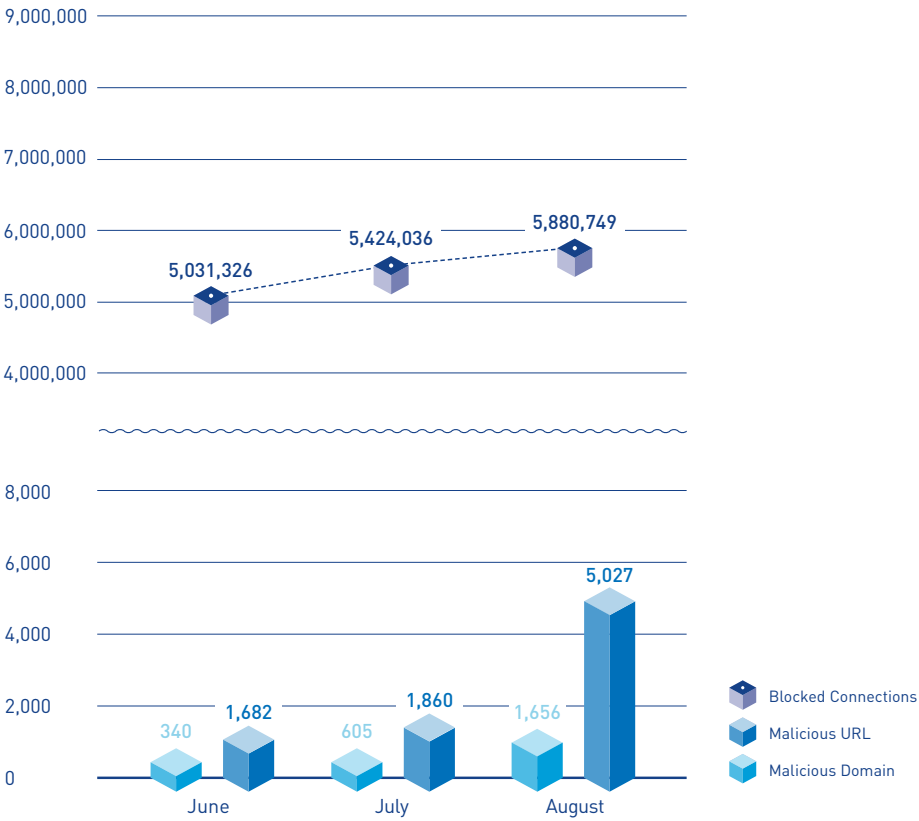
[Table 1-1] Top 10 Malware Threats in August 2016 (by Alias)

| Rank | Alias from AhnLab | No. of detections |
|---|---|---|
| 1 | Malware/Win32.Generic | 218,089 |
| 2 | Trojan/Win32.Starter | 183,507 |
| 3 | Unwanted/Win32.HackTool | 102,854 |
| 4 | Trojan/Win32.Neshta | 87,818 |
| 5 | Trojan/Win32.CryptXXX | 81,227 |
| 6 | Trojan/Win32.Banki | 80,766 |
| 7 | Trojan/Win32.Agent | 74,148 |
| 8 | HackTool/Win32.Crack | 58,715 |
| 9 | Adware/Win32.BrowseFox | 54,485 |
| 10 | ASD.Prevention | 52,818 |

## SECURITY STATISTICS

# 02
# Web Security Statistics

In August 2016, a total of 1,656 domains and 5,027 URLs were comprised and used to distribute malware. In addition, 588,749 malicious domains and URLs were blocked.



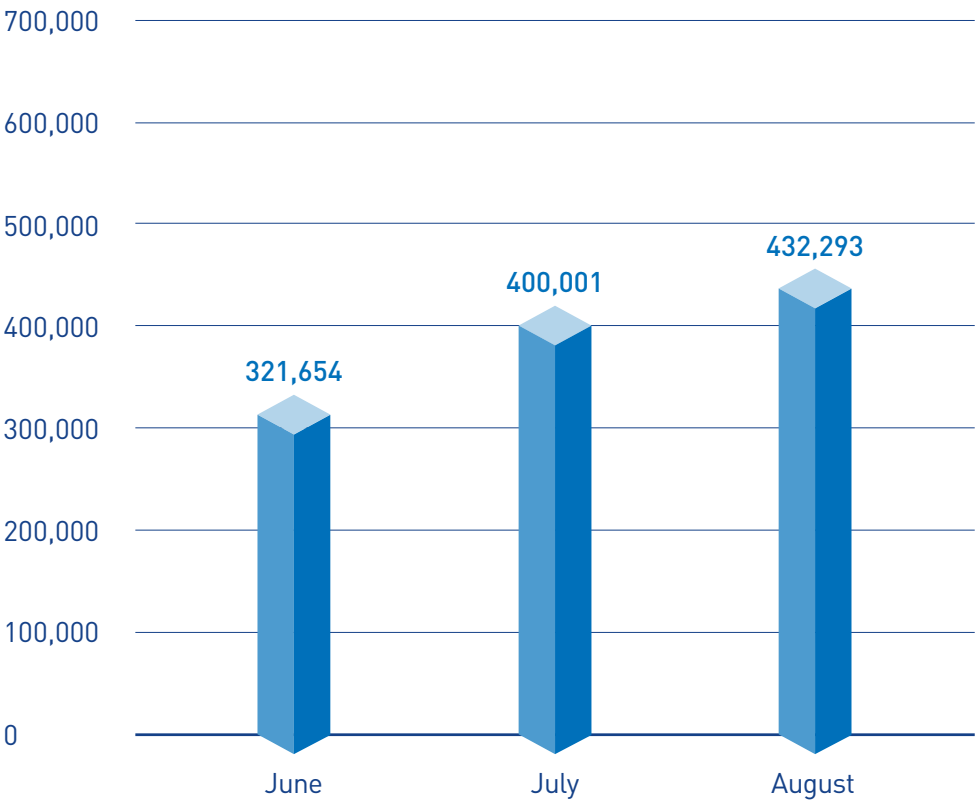

[Figure 1-3] Blocked Malicious Domains/URLs in August 2016

* "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 August 2016, 432,293 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 August 2016. Android-PUP/SmsPay was the most distributed malware with 154,907 of the total.

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

| Rank | Alias from AhnLab | No. of detections |
|---|---|---|
| 1 | Android-PUP/SmsPay | 154.907 |
| 2 | Android-PUP/Shedun | 76.665 |
| 3 | Android-PUP/SmsReg | 27.492 |
| 4 | Android-Trojan/AutoSMS | 26.924 |
| 5 | Android-PUP/Noico | 20.143 |
| 6 | Android-PUP/Zdpay | 10.664 |
| 7 | Android-Trojan/Agent | 7.728 |
| 8 | Android-Trojan/Shedun | 7.573 |
| 9 | Android-Trojan/Hidap | 6.006 |
| 10 | Android-AppCare/Agent | 5.030 |

# 2

# SECURITY ISSUE

Ransomware Disguised as PokemonGo to Catch Users

SECURITY ISSUE

# Ransomware Disguised as PokemonGo to Catch Users

As ransomware continues to spread using increasingly devious methods, a recent spate of attacks has revealed ransomware disguised as PokemonGo, the popular augmented reality (AR) game, threatening unsuspecting users.


Figure 2-1 | Ransomware disguised as PokemonGo

This malware hides itself behind the icon of a game character as shown in Figure 2-1, but is in fact ransomware that encrypts document files in an infected PC. Running the file crates additional malicious files in the startup programs folder, and it self-duplicates itself into every root directory in the system.

Figure 2-2 | Autorun program planted

The malware thus is executed automatically at every system reboot, and modifies the system's registry as shown in Table 2-1. A "Hack3r" registry is added onto UserList, creating an administrator account under that handle.

Table 2-1 | Modified administrator account registry information

| |
|---|
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList |
| **Hack3r = "0"** |

The registry value is assigned as "0" to make the account invisible to the user, creating a hidden "Hack3r" admin account. The malware then attempts to connect to the address indicated in Table 2-2.

Table 2-2 | Network address

| |
|---|
| 10.25.0.169:80 |

The ransomware encrypts various files with the extensions listed in Table 2-3.

Table 2-3 | File extensions targeted for encryption

| |
|---|
| *.txt, *.rtf, *.doc, *.pdf, *.mht, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.png , *.odt, *.jpg, *.png, *.csv, *.sql, *.mdb, *.sln, *.php, *.asp, *.aspx, *.html, *.xml, *.psd, *.htm, *.gif |


Figure 2-3 | Screen displaying the ransomware infection

The ransomware displays an image of the familiar game character and a message in Arabic on the screen of the infected system, as shown in Figure 2-3. The message informs the victim that the files in the PC have been encrypted, with instructions for sending an email to have the files restored. The message on the screen shows that the malware has been designed to target users in Arabic-speaking regions.

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

**<Aliases identified by V3 products>**

Trojan/Win32.Ryzerlo (2016.08.17.00)

Trojan/Win32.Ransom (2016.08.18.04)

# 3

# IN-DEPTH ANALYSIS

## Locky Ransomware Disguised as .DLL File Appears

IN-DEPTH ANALYSIS

# Locky Ransomware Disguised as .DLL File Appears

First discovered in February of 2016, the series of Locky ransomware quickly rose to infamy by causing large swathes of damage to systems across the world. While the ransomware was first found to attach "locky" to the extension of encrypted files, variants of Locky ransomware that modified the extension to "zepto" have also been discovered. These variants were also found to be distributed as script files instead of the traditional document files. Recently, a new type of Locky ransomware used a DLL file instead of an EXE file has been found, requiring users to remain even more vigilant. This article presents the newest variation to the constantly shape-shifting Locky ransomware.

The recently-spotted Locky ransomware using DLL files was distributed in the form of a JavaScript (.js) file embedded in spam emails, a common practice for spreading ransomware. The difference is the downloading of a DLL file into a temp folder when the downloader is executed, which is then run using rundll32.exe as shown in Figure 3-1.

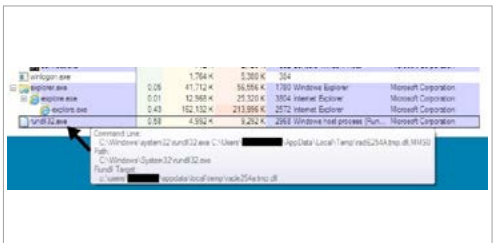


Figure 3-1 | Ransomware infection with rundll32 (*source: malware-traffic-analysis.net)

Running the .js file introduced by the spam email downloads files from the URLs listed in Table 3-1.

Table 3-1 | Malware Distribution URLs

| |
|---|
| sopranolady7.wang/1cntwk5 |
| ihvr.org/txb1n2bm |
| da-fortunato.de/fqjold5 |
| spir.50webs.com/52sc0 |

Ransomware in the form of a DLL file is downloaded at this time to %Temp%, a temporary folder, as shown in Table 3-2.

Table 3-2 | Location of the downloaded DLL file

| |
|---|
| %Temp%\1o0cGXH9d.dll |

When the DLL file is executed, a popup notice as shown in Figure 3-2 displays, indicating that the system has been infected with ransomware.


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

The file names and extensions modified by the Locky ransomware are as shown in Table 3-3.

Table 3-3 | Modified file names and extensions

| |
|---|
| C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-8E79-B65E2228C978.zepto |
| C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-C81F-576C3AC8C83A.zepto |
| C:\Documents and Settings\Default User\Templates\F4D5F460-96E9-FAC1-8CE8-B5606E7172D3.zepto |
| C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-3DFD-709222A3B9BD.zepto |
| C:\Documents and Settings\Administrator\Templates\F4D5F460-96E9-FAC1-8CCB-7E954797747B.zepto |

Variants as well as various existing ransomware continue to present a serious threat to users. Files encrypted by a ransomware attack are mostly impossible to restore. Prevention is thus more critical for protecting a system from ransomware than for any other types of malware. Users should diligently

apply the latest security updates to the operating system and applications, and back up important data on a regular basis.

The relevant aliases of the new variant of Locky ransomware identified by V3 products, AhnLab's anti-virus program, are as below:

**<Aliases identified by V3 products>**

Trojan/Win32.Locky (2016.08.24.05)

JS/Obfus.S111 (2016.08.25.00)

AhnLab

# ASEC REPORT

VOL.80
August, 2016

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