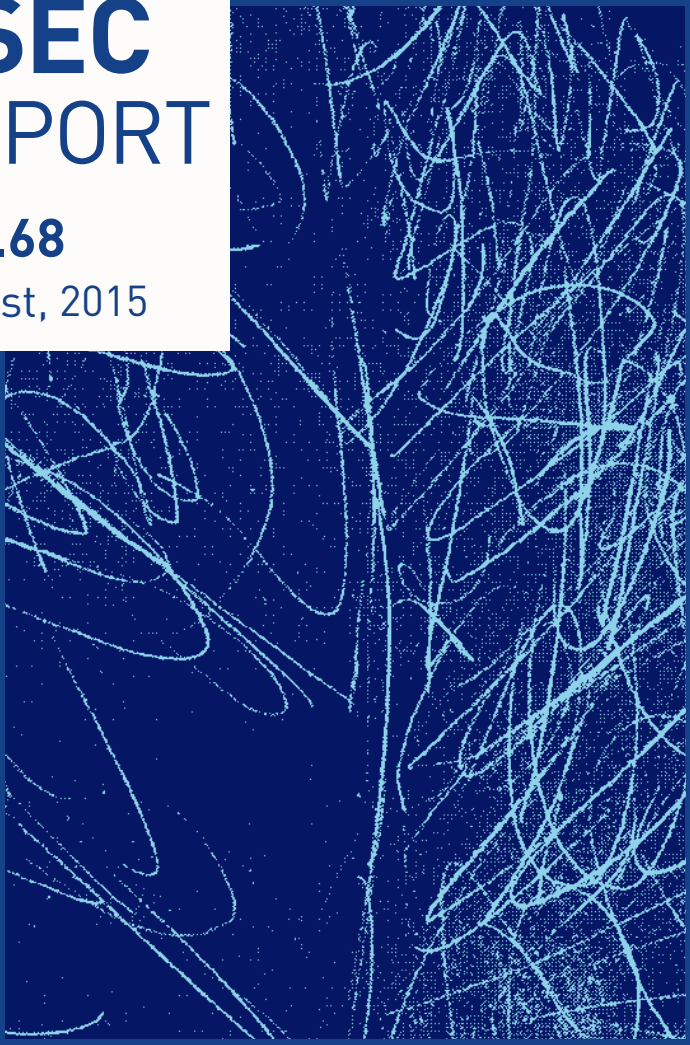
Security Trend

# ASEC REPORT

## VOL.68

August, 2015



AhnLab

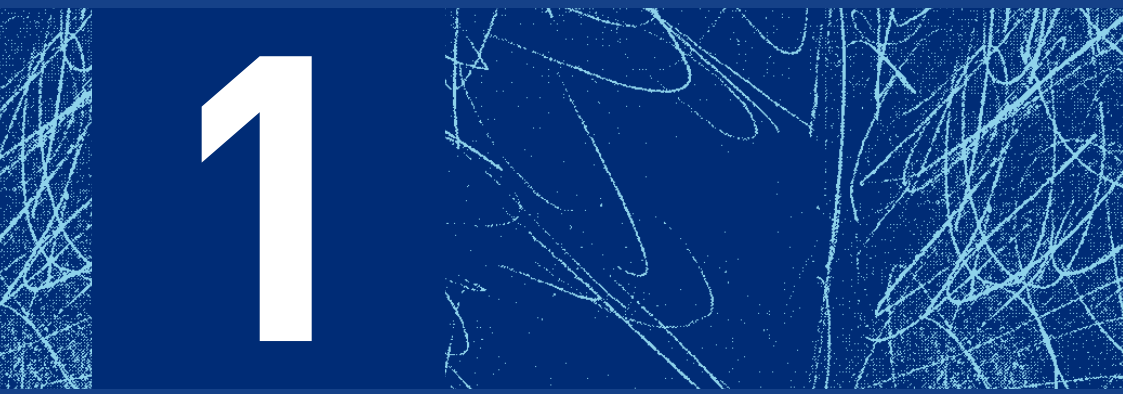
# ASEC REPORT

**VOL.68** August, 2015

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 2015

Table of Contents



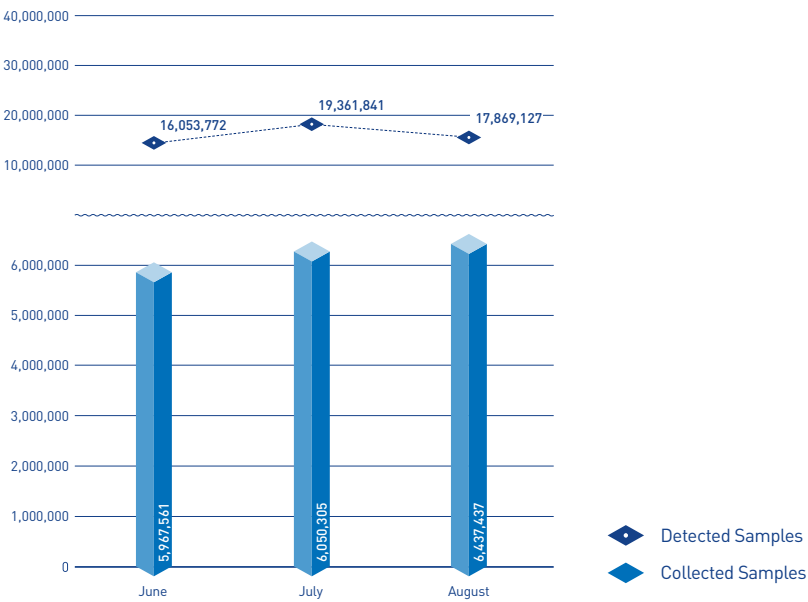
# 1

# SECURITY STATISTICS

## SECURITY STATISTICS

# 01
# Malware Statistics

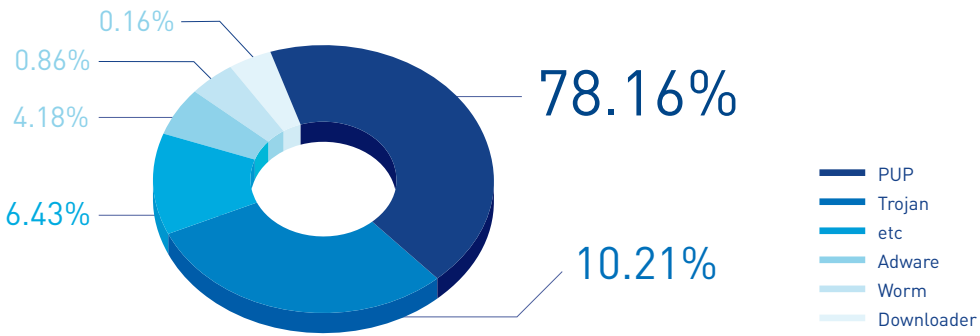
According to the ASEC (AhnLab Security Emergency Response Center), 17,869,127 malware were detected in August 2015. The number of detected malware decreased by 1,492,714 from 19,361,841 detected in the previous month as shown in Figure 1-1. A total of 6,437,437 malware samples were collected in August.




[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 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 78.16% of the total. It was followed by Trojan (10.21%) and Adware (4.18%).




[Figure 1-2] Proportion of Malware Type in August 2015

Table 1-1 shows the Top 10 malware threats in August categorized by alias. Trojan/Win32.Gen was the most frequently detected malware (254,208), followed by Trojan/Win32.Starter (134,632).

[Table 1-1] Top 10 Malware Threats in August 2015 (by Alias)

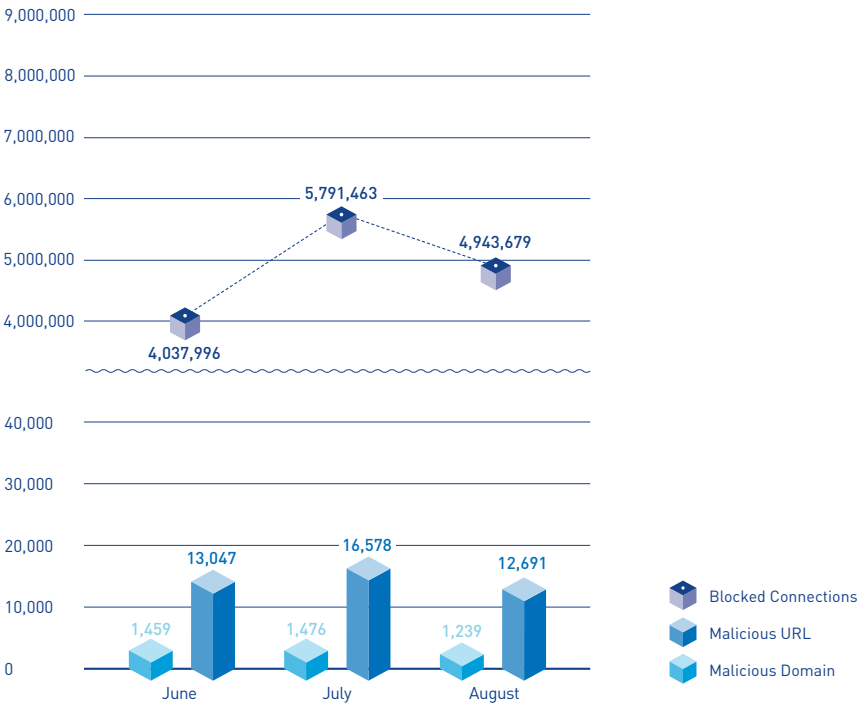
| Rank | Alias from AhnLab | No. of detections |
|---|---|---|
| 1 | Trojan/Win32.Gen | 254,208 |
| 2 | Trojan/Win32.Starter | 134,632 |
| 3 | Malware/Win32.Generic | 126,479 |
| 4 | Trojan/Win32.Agent | 92,959 |
| 5 | Malware/Win32.SAPE | 92,643 |
| 6 | Unwanted/Win32.Exploit | 73,052 |
| 7 | Trojan/Win32.Banki | 53,313 |
| 8 | Adware/Win32.Agent | 49,843 |
| 9 | Trojan/Win32.Buzus | 42,509 |
| 10 | HackTool/Win32.Crack | 42,505 |

## SECURITY STATISTICS

# 02

# Web Security Statistics

In August 2015, a total of 1,239 domains and 12,691 URLs were comprised and used to distribute malware. In addition, 4,943,679 malicious domains and URLs were blocked.



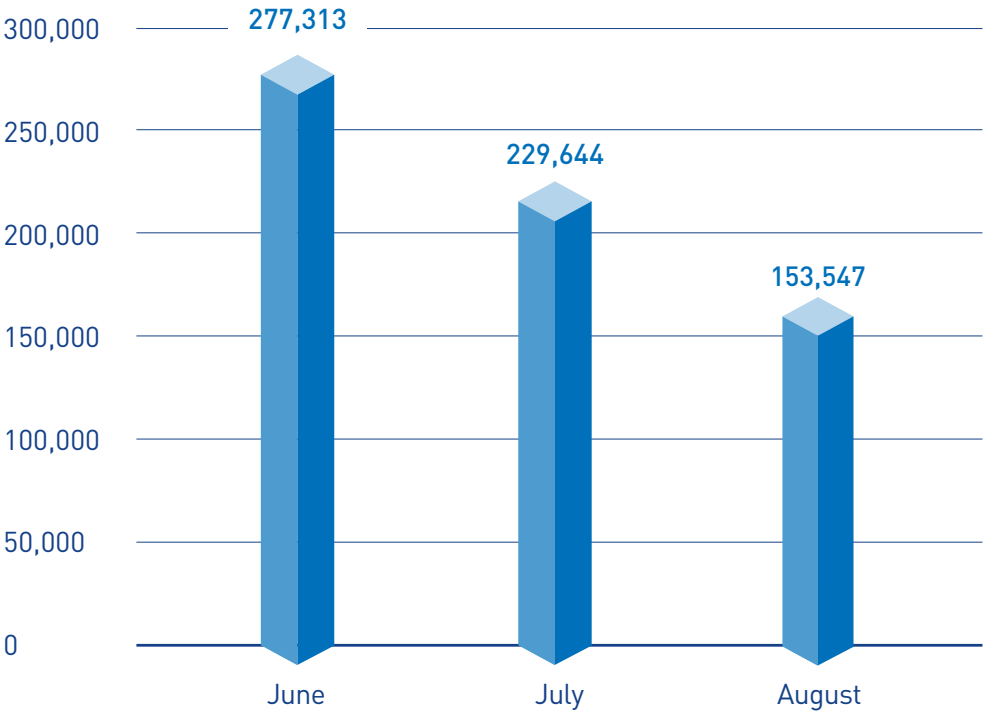

[Figure 1-3] Blocked Malicious Domains/URLs in August 2015

* "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 2015, 153,547 mobile malware were detected as shown in Figure 1-4.

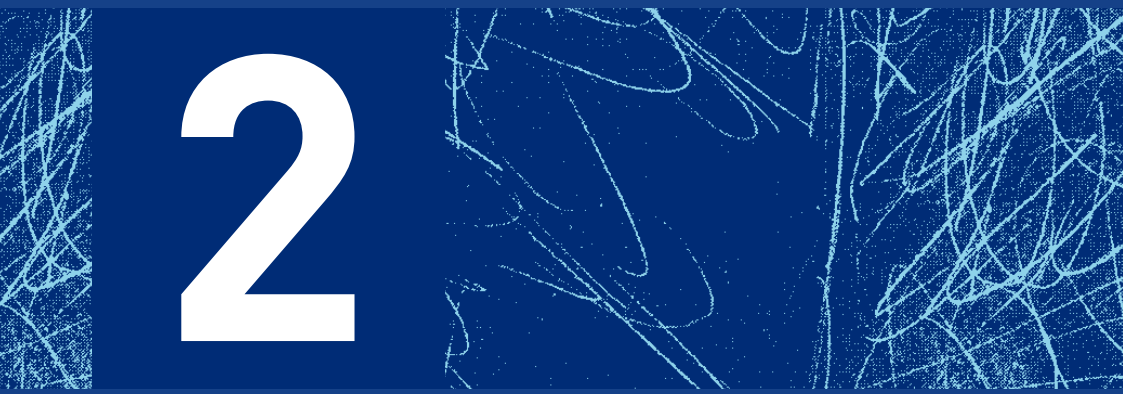



[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in August 2015. Android-PUP/SmsPay was the most distributed malware with 47,217 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 | 47,217 |
| 2 | Android-PUP/SmsReg | 19,437 |
| 3 | Android-PUP/Zdpay | 8,579 |
| 4 | Android-PUP/Dowgin | 7,259 |
| 5 | Android-Trojan/FakeInst | 7,019 |
| 6 | Android-Trojan/Slocker | 6,007 |
| 7 | Android-PUP/Noico | 5,952 |
| 8 | Android-PUP/AutoSMS | 3,843 |
| 9 | Android-PUP/Chepa | 3,240 |
| 10 | Android-Trojan/SMSAgent | 3,205 |



# 2

# SECURITY ISSUE

Sophisticated PUPs Using Social Issues as Click Bait On the Rise

SECURITY ISSUE

# Sophisticated PUPs Using Social Issues as Click Bait On the Rise

A recent string of potentially unwanted programs (PUPs) distributed using videos related to celebrities or social issues have been spotted. PUPs designed to make them difficult to erase by the user appeared earlier, but the new batch of PUPs utilize social engineering methods that had been used primarily to spread malware, indicating that PUPs are becoming increasingly sophisticated.

While PUPs technically are not malware, they are just as unwelcome to the user since they slow down PCs or repeatedly display advertising popup windows. The PUPs most recently discovered were distributed using videos featuring celebrities, terrorist bombings or other social issues as shown below.

As shown in Table 2-1, the PUP creator used issues that were featured prominently in the news at the time of PUP's creation. The date of creation and distribution corresponds with the time of the incident or issue being used by the PUP. These tend to be the dates when the number of news stories as well as public interested in the issue are at their highest.

Table 2-1 | Date of PUP file creation

| Date of PUP file creation | Date of Creation |
|---|---|
| (Celebrity A)_meltdown_video.exe | Aug 11, 2015 14:00 |
| (Celebrity B)_teaser video.exe | Aug 11, 2015 15:00 |
| (Actress A)_video.exe | Aug 18, 2015 16:00 |
| Bangkok terrorist bombing_video.exe | Aug 18, 2015 12:00 |

When the files disguised as videos about prominent social issues, the file "snbsetip.exe" is created in the path "C:\Windows," then executed.

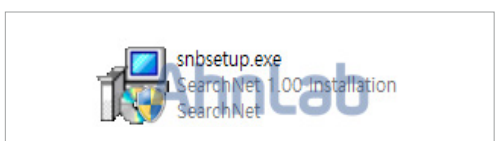



Figure 2-1 | snbsetup.exe file

When "snbsetupe.exe" is executed, unwanted programs are installed in the following paths, then run.

Table 2-2 | File creation information

C:₩Program Files₩SearchNet₩searchnet.exe
C:₩Program Files₩SearchNet₩usearchnet.exe
C:₩Program Files₩SearchNet₩Uninstall.exe
C:₩Program Files₩SearchNet₩utildownload.exe

In addition, these files are registered as startup programs as indicated in Table 2-3, to make the system run these unwanted files at system startup.

Table 2-3 | startup program information

HKCU₩Software₩Microsoft₩Windows₩Current Version₩Run₩searchnet
–〉 "C:₩Program Files₩SearchNet₩searchnet.exe"
HKCU₩Software₩Microsoft₩Windows₩Current Version₩Run₩usearchnet
–〉 "C:₩Program Files₩SearchNet₩usearchnet.exe"

When the file "utildownload.exe" is executed, a download screen appears. The End User License Agreement (EULA) for the unwanted program is displayed in the lower left corner of this window, and a button for opening the file appears on the right.

When the user clicks "open," the file "UtilDownLoad.exe" runs Internet Explorer and connects to the webpage containing the video of the relevant issue. The page for the video, as shown below, is an ordinary webpage containing information related to the social issue, making it difficult for the user to realize that an unwanted program has been installed in his or her system.


Figure 2-2 | Webpage containing a video about the social issue

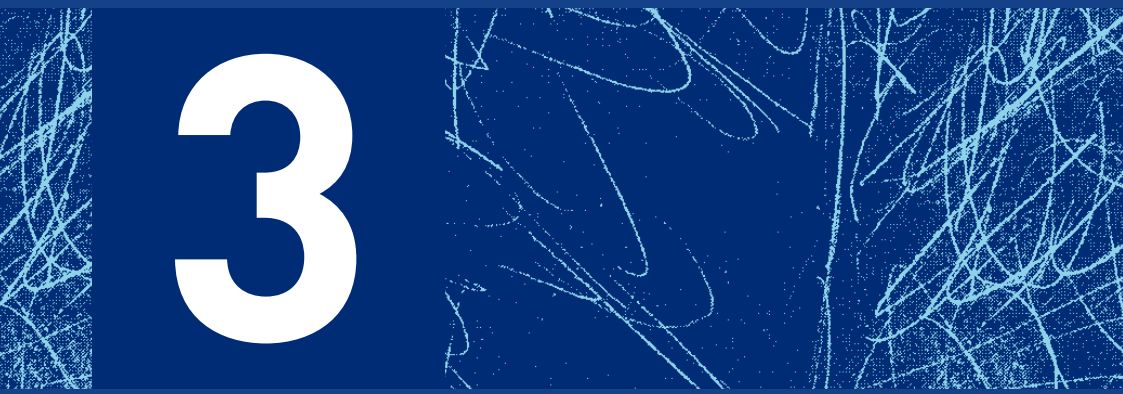
The primary purpose of these unwanted programs is the exposure of advertising for monetary again. The unwanted program monitors websites the user usually visits, and inserts advertisements onto the browser when the user visits search sites such as google.

Since distribution is the primary goal of these unwanted programs, there is no further maintenance or update after they are created. These unwanted programs are widely distributed to a large number of users, and no security updates are ever carried out. They can thus provide extremely useful channels of distribution

of malware, so it is recommended that users be very cautious.

The corresponding aliases from V3 are as below:

**< Aliases from V3 products >**
PUP/Win32.Toolbar (2015.08.18.05)
Trojan/Win32.Infostealer (2015.08.20.08)



# 3

# IN-DEPTH ANALYSIS

Ransomware Disguised as Windows 10 Update

SECURITY ISSUE

# Ransomware Disguised as Windows 10 Update

Windows 10, marking the final iteration of Microsoft's Windows OS, was released on August 29. The new release seems to have piqued the interest of not only users but malware creators, since ransomware disguised as Windows 10 updates appeared only days later via email distribution.

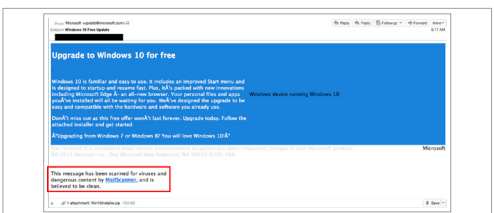



Figure 3-1 | Email containing the malware (*Source:Cisco Blogs)

Using the fake sender information and the main body of the email, the attacker tries to deceive the user into reading the email, downloading the attachment and then executing it without suspicion. Indeed even the icon of the malware in the email uses the Windows logo as shown in Figure 3-2, ensuring that unless the user has a habit of being extra vigilant, the mouse pointer will be moving towards the file without a second thought.


Figure 3-1 | Malware disguised as a Windows10 update file

Running the malware executes not the Windows 10 update the user has expected but a ransomware, encrypting the files in the user's system. The ransomware duplicates itself as the file "lrxjxii.exe" in the path <C:\DOCUME~1\[User Account]\LOCALS~1\Temp\>, and adds itself to the registry to ensure that it runs at startup.


Figure 3-3 | Desktop image after the ransomware infection

The ransomware encrypts the files stored in the system and displays instruction on restoring the files, as shown in Figure 3-3. While there are no distinguishing features compared to other ransomware, the social engineering method employed by the malware in this case indicates that attackers are becoming smarter and that ultimately people are the weakest link in security.

Users who stay on top of Windows security patches or are familiar with updates for popular programs such as Adobe and Java may minimize their exposure to these kinds of malware. As you can see in this case, however, downloading and running email-borne malware is like flinging the doors that has been shut tight with security patches wide open at the slightest knock by a delusive malware. This is the reason why the basic tenet of security, "Do not download or open files contained in email," is emphasized so often.

The corresponding alias from V3 is as below:

**<Alias from V3 products>**

Trojan/Win32.CTBLocker (2015.08.03.03)

AhnLab

# ASEC REPORT

VOL.68
August, 2015

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