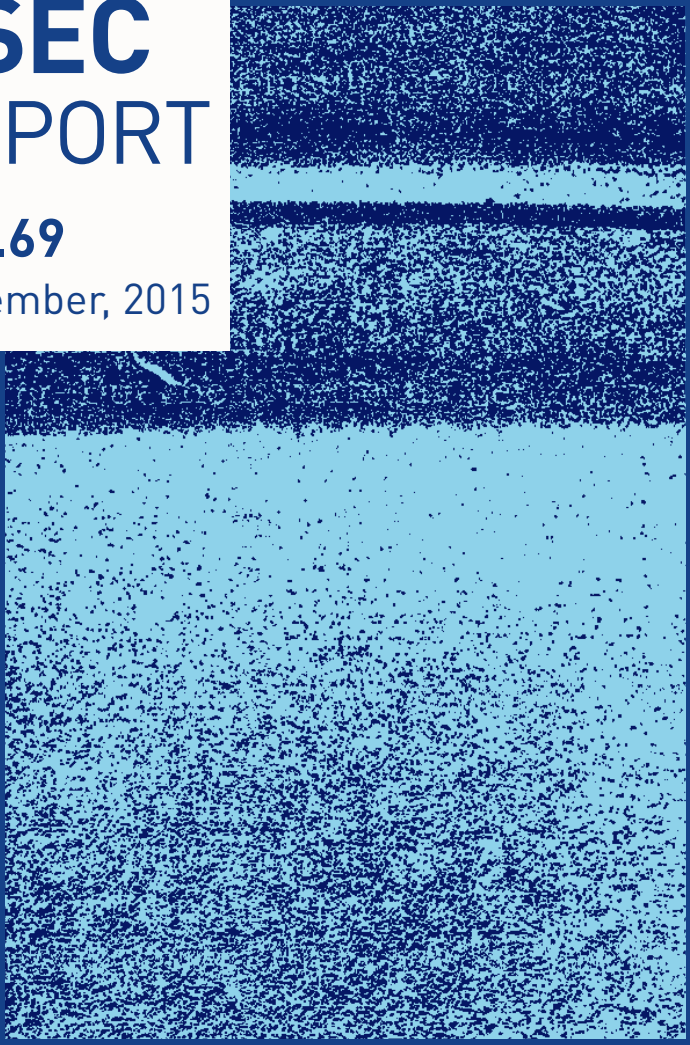
Security Trend

ASEC REPORT

VOL.69

September, 2015



AhnLab

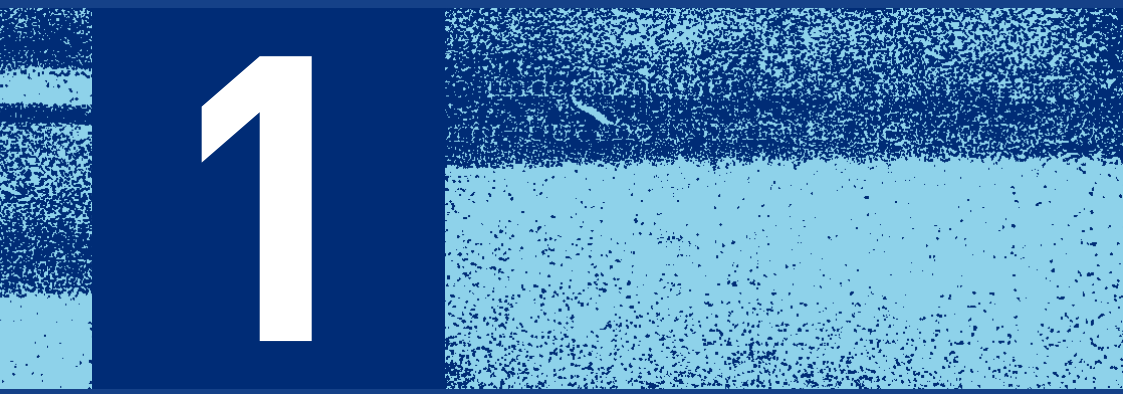
ASEC REPORT

VOL.69 September, 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 September 2015

Table of Contents



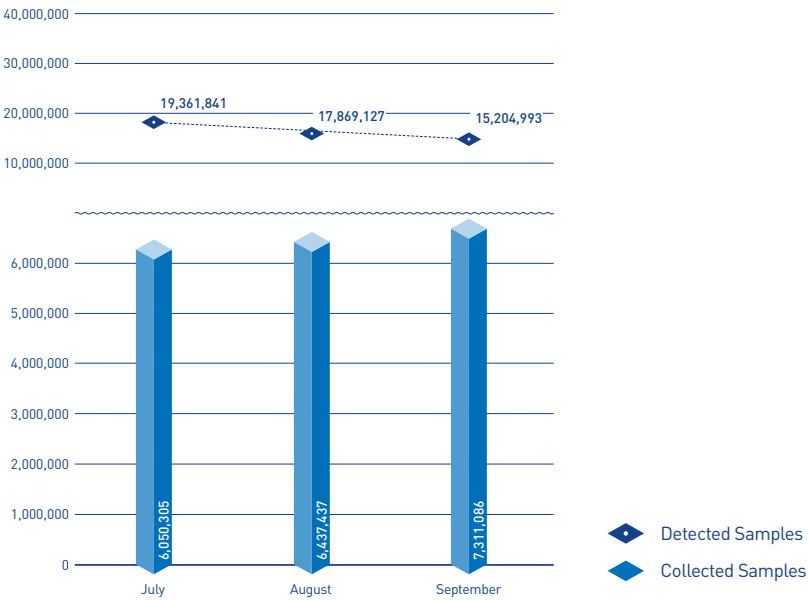
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

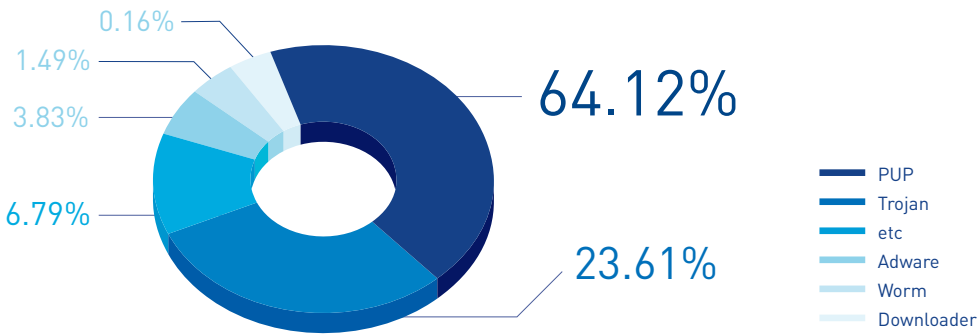
According to the ASEC (AhnLab Security Emergency Response Center), 15,204,993 malware were detected in September 2015. The number of detected malware decreased by 2,664,134 from 17,869,127 detected in the previous month as shown in Figure 1-1. A total of 7,311,086 malware samples were collected in September.



[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 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 64.12% of the total. It was followed by Trojan (23.61%) and Adware (3.83%).



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

Table 1-1 shows the Top 10 malware threats in September categorized by alias. Trojan/Win32.Gen was the most frequently detected malware (224,589), followed by Trojan/Win32.Starter (152,154).

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

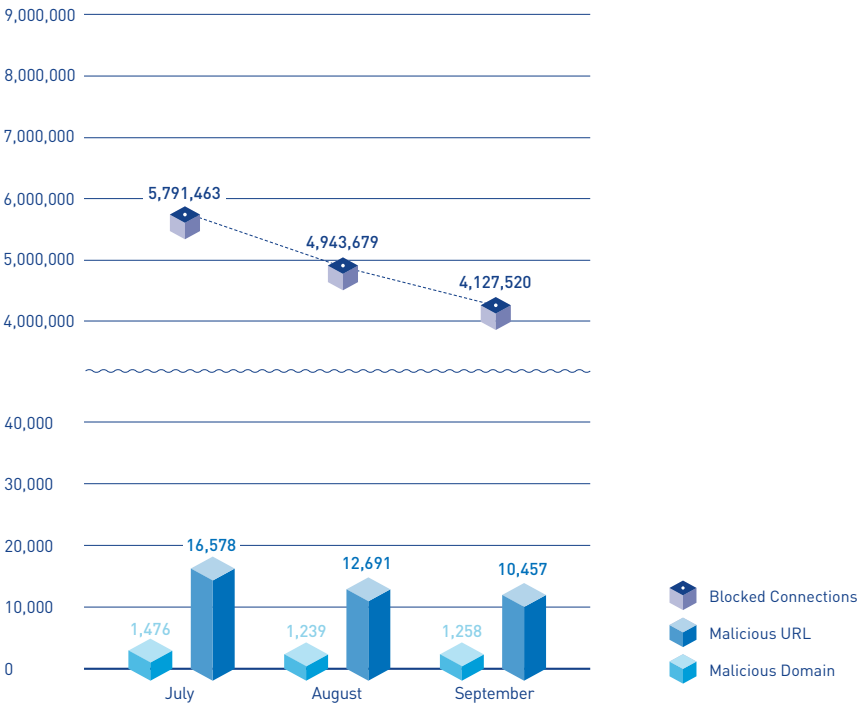
Rank	Alias from AhnLab	No. of detections
1	Trojan/Win32.Gen	224,589
2	Trojan/Win32.Starter	152,154
3	Trojan/Win32.Agent	95,593
4	Trojan/Win32.Banki	62,699
5	Unwanted/Win32.Exploit	60,256
6	Worm/Win32.IRCBot	50,232
7	Malware/Win32.Generic	44,228
8	Unwanted/Win32.Keygen	41,269
9	Trojan/Win32.Generic	40,447
10	HackTool/Win32.Crack	40,339

SECURITY STATISTICS

02

Web Security Statistics

In September 2015, a total of 1,258 domains and 10,457 URLs were comprised and used to distribute malware. In addition, 4,127,520 malicious domains and URLs were blocked.



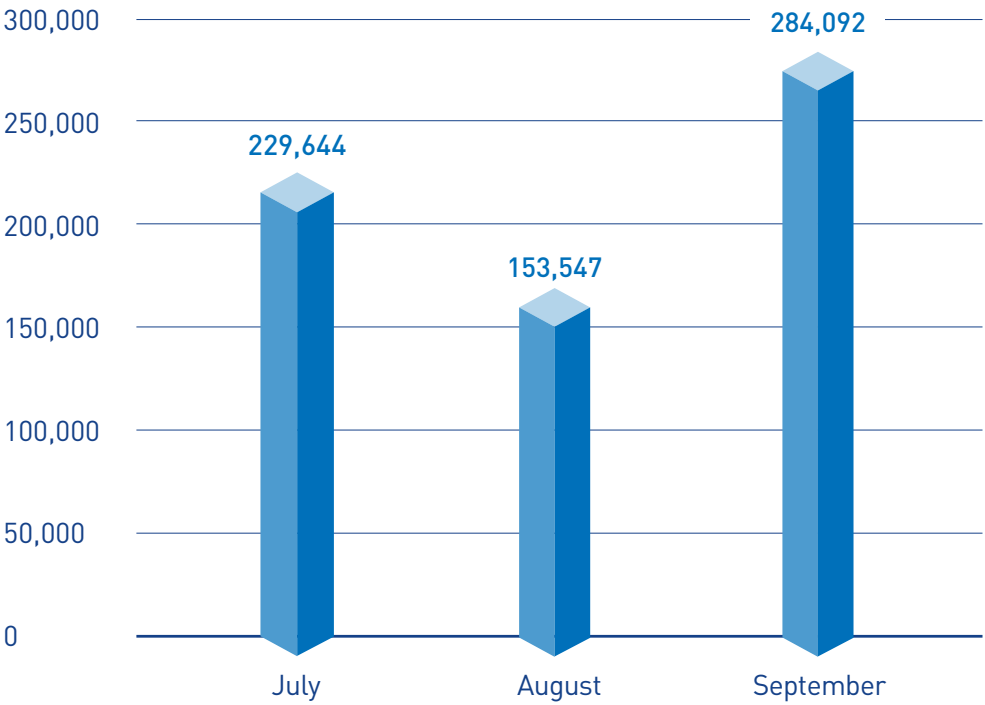
[Figure 1-3] Blocked Malicious Domains/URLs in September 2015

* "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 September 2015, 284,092 mobile malware were detected as shown in Figure 1-4.

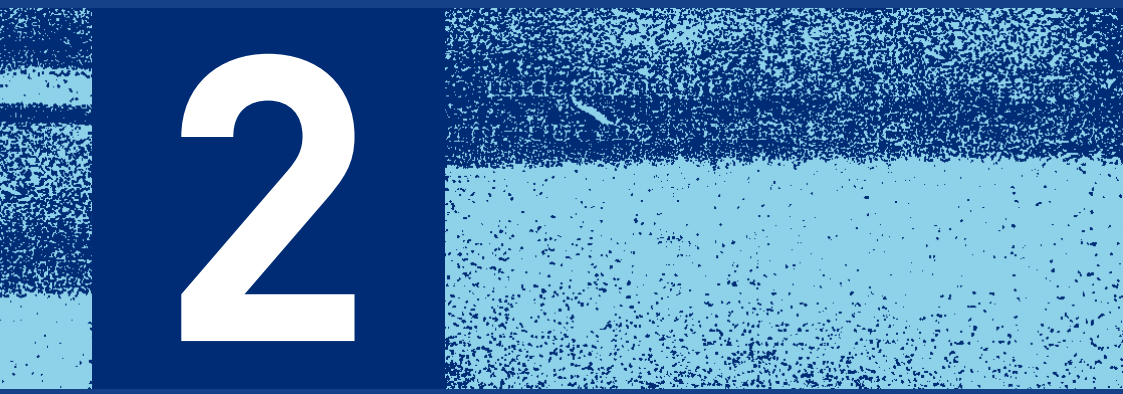


[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in September 2015. Android-PUP/SmsPay was the most distributed malware with 98,592 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	98,592
2	Android-PUP/Noico	27,320
3	Android-PUP/SmsReg	22,747
4	Android-PUP/Chepa	16,922
5	Android-Trojan/FakeInst	16,527
6	Android-PUP/Dowgin	9,610
7	Android-Trojan/SmsSpy	6,874
8	Android-Trojan/SMSAgent	6,818
9	Android-PUP/Zdpay	6,316
10	Android-Trojan/Opfake	4,720



2

SECURITY ISSUE

Malware Disguised as Illegal Game-related Software

SECURITY ISSUE

Malware Disguised as Illegal Game-related Software

Recently, malware disguised as illegal hacks and other related software for popular games have been discovered, requiring users to exercise special caution. Figure 2-1 shows an illegal program for the game Grand Theft Auto (GTA), one of numerous game hacks, cheat keys, macros, trainers and other exploits that some unscrupulous users employ to give themselves an edge over online opponents. These programs are easily obtainable on the internet and through file-sharing sites, and the malware creators are taking advantage of this fact to design and distribute malware disguised as such illegal programs.

Figure 2-1 | Malware disguised as illegal game exploit software

This malware disguised as an illegal hack actually executes the game-related program when run by the user to escape scrutiny. The malware then attempts to create a new file, change the registry and establish a network connection.

Table 2-1 | Newly created files
C:\Documents and Settings\Administrator\Application Data\0.exe
C:\Documents and Settings\Administrator\Application Data\1.exe
C:\WINDOWS\system32\huppug(random name).exe

The malware creates the files 0.exe and 1.exe. The file 0.exe duplicates itself to write a malicious file in the path %system32%. The new file 1.exe is the game hack program shown in Figure 2-1.

Table 2-2 | Registry information
HKLM\SYSTEM\ControlSet001\Services\Nationaling
"ImagePath" = "C:\WINDOWS\system32\huppug.exe"
"DisplayName" = "Nationalbjf Instruments Domain Service"
"ObjectName" = "LocalSystem"

The malicious file thus alters the registry to ensure that it continues to run even when the system is restarted, registering

a service called "Nationaling."

The malware attempts to connect to the following IP address and network:

```
2*1.2**.1*8.**5:1**6
2*1.2**.1*8.**5:5**0
```

As noted above, the malware attempts to connect to certain IP addresses. It is presumed that the malware is designed to download additional malware and steal personal information via the connection. However, the network connection did not occur when AhnLab's security researchers conducted the analysis.

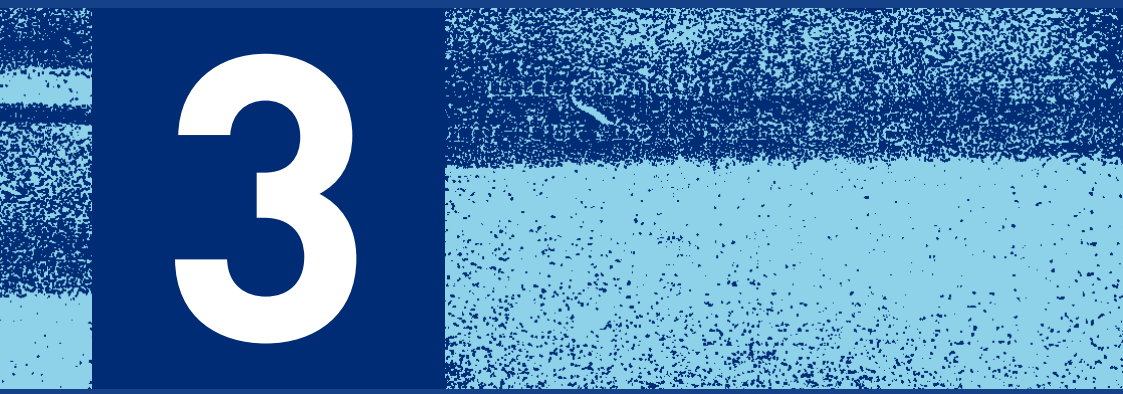
As shown by this example, malware are being increasingly designed to execute an ordinary and intended file in addition to the malicious file, making it difficult for the user to realize that the file he or she has downloaded is malware. Thus, users are advised to avoid illegally downloading software or running illegal programs in order to avoid damages caused by malware.

The corresponding aliases from V3 are as below:

< Aliases from V3 products >

Win-Trojan/Malpacked5.Gen (2015.09.19.00)

Dropper/Win32.Agent (2015.09.24.09)



3

IN-DEPTH ANALYSIS

Ransomware Disguised as Pornographic Content

SECURITY ISSUE

Ransomware Disguised as Pornographic Content

The recent security breach of the Ashley Madison, American extramarital affair website, aroused controversy and highlighted the inundation of the internet with adult material and subjects. Cyber attacks using such adult content have been steadily rising, and recently a ransomware app has appeared that disguises itself as pornography.

Figure 3-1 | Icon for the ransomware app

The malicious app disguises itself as adult content as shown in Figure 3-1. Unlike existing ransomware, this app does not encrypt the data stored in the mobile phone. Instead, it restricts the user's access to the phone. The app automatically runs when the phone is turned on, and locks the screen with its own display to prevent the user from controlling the smart phone. The attacker demands a ransom for removing the ransomware app.

The app requests permissions normally not required for viewing videos, including button lock, control for apps running in the background, and system settings. The malicious app also requests permissions for accessing personal information stored on the phone as well as system information.

The detail of the permissions requested by the ransomware is revealed in the settings file as below:

Table 3-1 | Androidmanifest.xml

```
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
<uses-permission android:name ="com.android.browser.permission.READ_HISTORY_
BOOKMARKS"/>
<uses-permission android:name ="com.sec.android.app.sbrowser.operatorbookmarks.
permission.READ_HISTORY_BOOKMARKS"/>
<uses-permission android:name ="android.permission.RESTART_PACKAGES"/>
<uses-permission android:name ="android.permission.CAMERA"/>
<uses-permission android:name ="android.permission.GET_TASKS"/>
<uses-permission android:name ="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name ="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name ="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name ="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name ="android.permission.CHANGE_WIFI_STATE"/>
```

```
<uses-permission android:name ="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name ="android.permission.KILL_BACKGROUND_
PROCESSES"/>
<uses-permission android:name ="android.permission.READ_CONTACTS"/>
<uses-permission android:name ="android.permission.RECEIVE_BOOT_
COMPLETED"/>
<uses-permission android:name ="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name ="android.permission.INTERNET"/>
<uses-permission android:name ="android.permission.WAKE_LOCK"/>
<uses-permission android:name ="android.permission.ACCESS_NETWORK_STATE"/>
```

One of the permissons requested by the ransomware app is “android.permission. SYSTEM_ALERT_WINDOW," which enables the app to ignore all output screens including the lock screen and instead display its own screen output. Once the ransomware acquires this permission, the smart phone can only display the screen that is being output by the malicious app.

Clicking on the install button of the ransomware will display the installing process, as shown in Figure 3-2. This is not an actual install nation screen, but instead the execution screen of the malicious app.

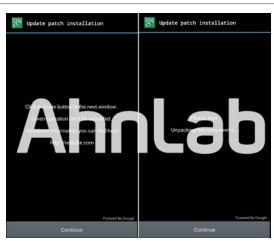


Figure 3-2 | Execution of the malicious app being disguised as an installation process

The fake installation screen includes Google icon as well as the text "Powered by Google" in the lower right corner to trick the user. Once the user unwittingly clicks "Continue" button on the bottom of the screen, the malicious ransomware app receives "Android Device Manager" access. Once this is done, the malicious app cannot be removed until the corresponding permission is disabled.

Figure 3-3 | Ransomware app screen output 1

Figure 3-4 | Ransomware app screen output 2

Once the ransomware executes, the screen as shown in Figure 3-4 is displayed. The app misrepresents itself as the FBI, and demands a ransom for

unlocking the phone by threatening the user for supposedly accessing child pornography.

The malicious ransomware app also uses the front-facing camera to take a photograph of the smart phone user, which is then displayed on the screen along with the ransom note to further threaten the user.

Figure 3-5 | Camera activation code

An even more frustrating situation develops if the user reboots the phone. Previous ransomware apps could be removed if the phone was rebooted in safe mode. However, this app uses the system's PIN function to lock the phone, making it inaccessible unless the PIN is somehow learned. If the phone is not rooted, the only possible solution is a factory reset. Once the phone is reset to factory settings, the PIN as well as all data on the phone are erased. To preserve critical personal information, the user should take caution against installing apps with uncertain origins.

We are now living in a "Mobile-Only" era. We have shifted beyond the age of "Mobile-First," where people reached for their mobile devices instead of their desktop computers, to "Mobile-Only," where our everyday life becomes increasingly tied to mobile devices. The rising number of smart phone subscribers has been accompanied by an increase in malicious apps. While apps on the official market are relatively safer, users should always verify the reviews before downloading apps from the market since malicious apps may also be listed. Clicking on URLs contained in text messages may also install malicious apps onto the smart phone, and caution should be taken against clicking on unknown URLs or installing unverified apps. Security apps designed for mobile devices (mobile AV) or anti-smishing apps should be installed and always kept up to date to create a safer smart phone environment.

The relevant aliases from V3 Mobile, AhnLab's anti-virus app, are as below

< Aliases from V3 products >

Android-Trojan/Lovet

Android-Trojan/Koler

AhnLab

ASEC REPORT

VOL.69
September, 2015

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