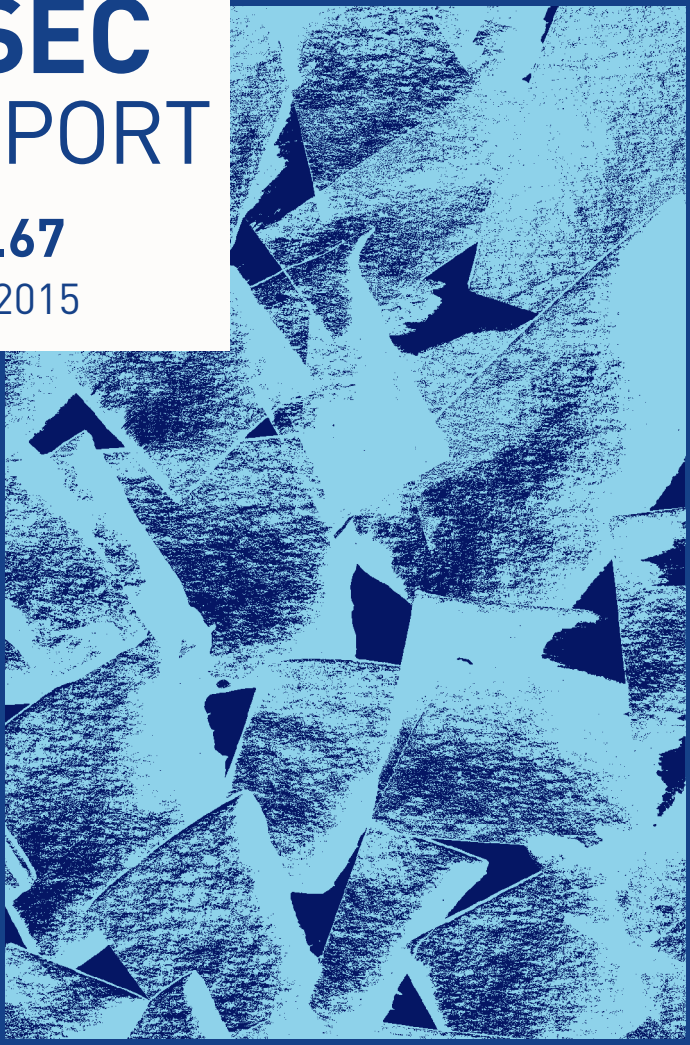
Security Trend

ASEC REPORT

VOL.67

July, 2015



AhnLab

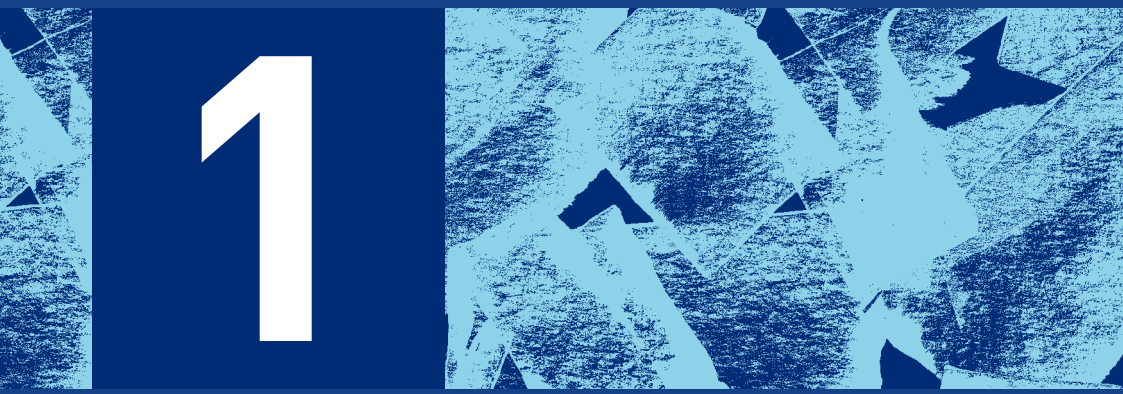
ASEC REPORT

VOL.67 July, 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 June 2015

Table of Contents



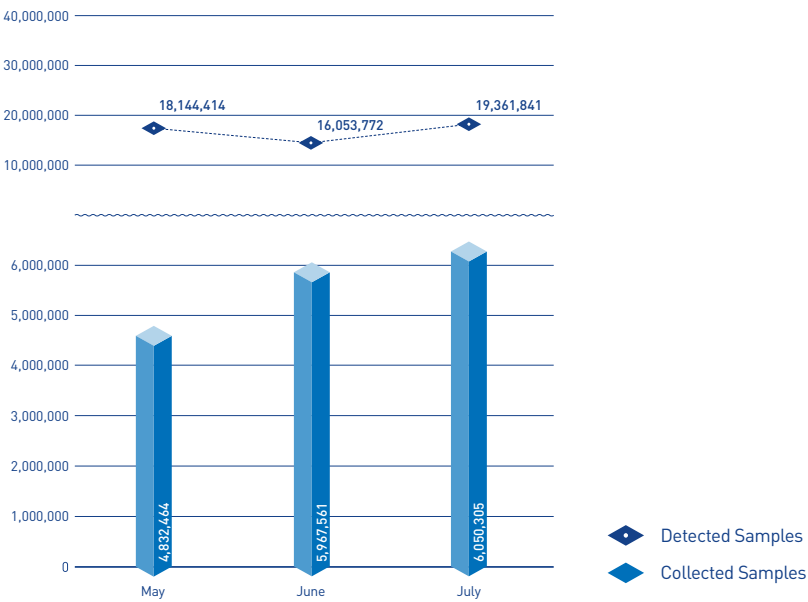
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

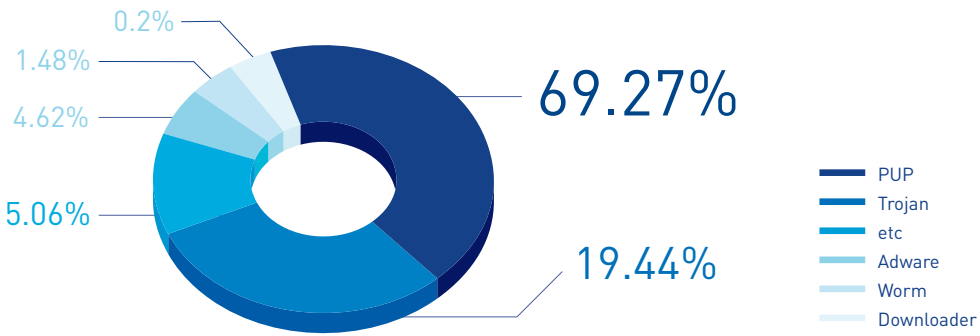
According to the ASEC (AhnLab Security Emergency Response Center), 19,361,841 malware were detected in July 2015. The number of detected malware increased by 3,308,069 from 16,053,772 detected in the previous month as shown in Figure 1-1. A total of 6,050,305 malware samples were collected in July.



[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 July 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 69.27% of the total. It was followed by Trojan (19.44%) and Adware (4.62%).



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

Table 1-1 shows the Top 10 malware threats in July categorized by alias. PUP/Win32.BrowseFox was the most frequently detected malware (4,052,984), followed by PUP/Win32.MicroLab (1,310,818).

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

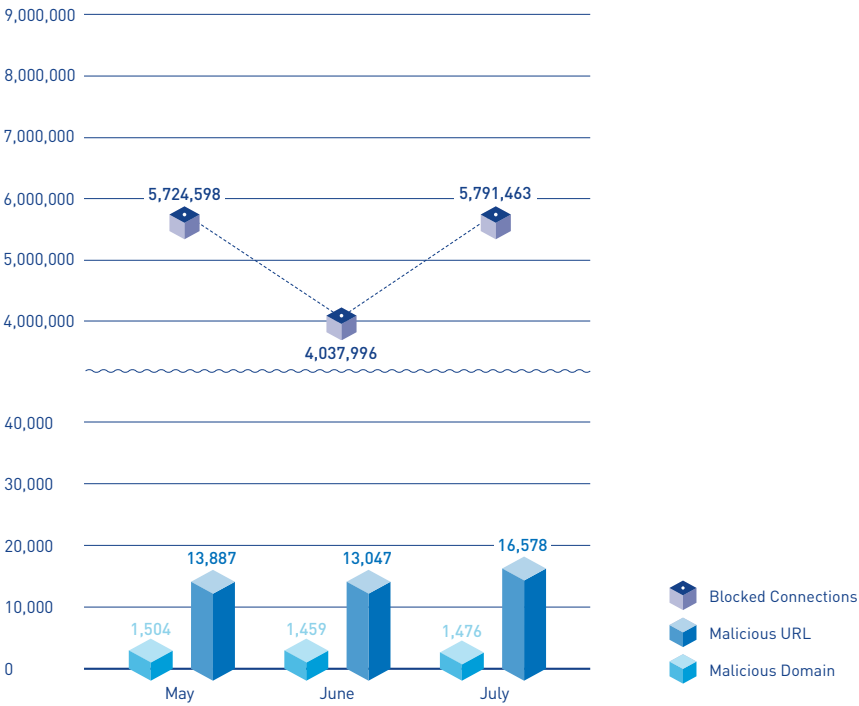
Rank	Alias from AhnLab	No. of detections
1	PUP/Win32.BrowseFox	4,052,984
2	PUP/Win32.MicroLab	1,310,818
3	PUP/Win32.Helper	764,824
4	PUP/Win32.Enumerate	567,644
5	PUP/Win32.Winexpand	520,237
6	PUP/Win32.SubShop	512,323
7	PUP/Win32.MyWebSearch	481,955
8	PUP/Win32.CrossRider	436,116
9	PUP/Win32.WindowsTap	388,610
10	PUP/Win32.SearchProtect	350,761

SECURITY STATISTICS

02

Web Security Statistics

In July 2015, a total of 1,476 domains and 16,578 URLs were comprised and used to distribute malware. In addition, 5,791,463 malicious domains and URLs were blocked.



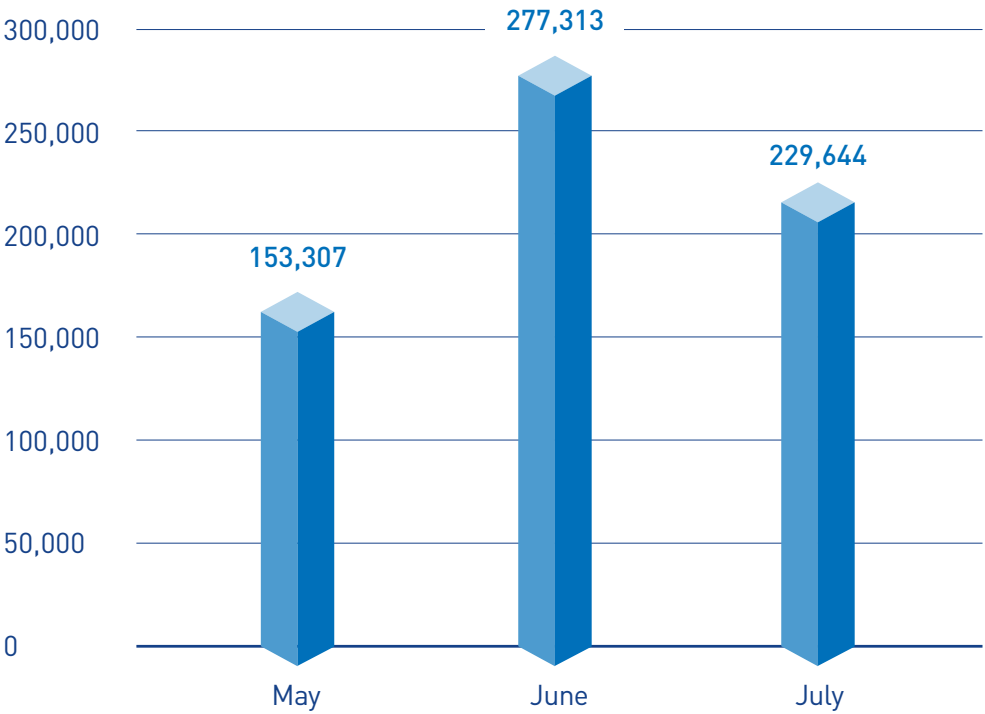
[Figure 1-3] Blocked Malicious Domains/URLs in July 2015

* "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 July 2015, 229,644 mobile malware were detected as shown in Figure 1-4.

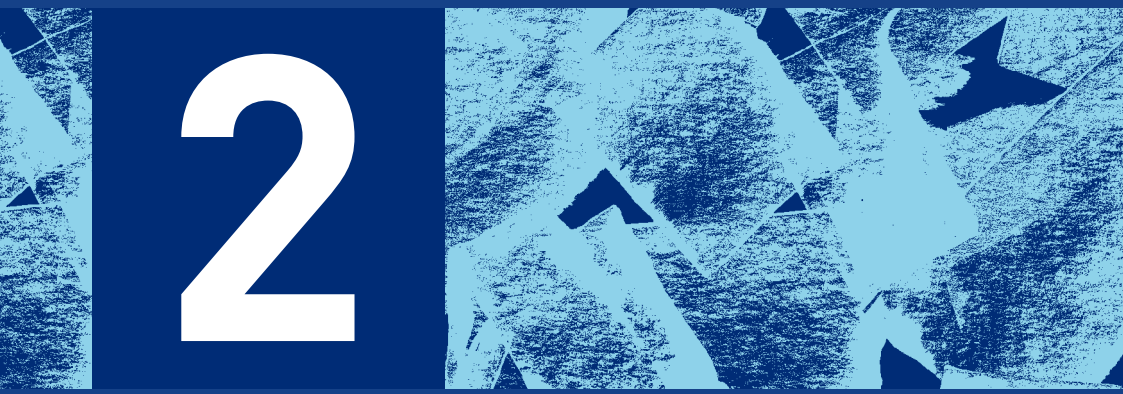


[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in July 2015. Android-PUP/Zdpay was the most distributed malware with 32,536 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/Zdpay	32,536
2	Android-PUP/Mulad	32,261
3	Android-Trojan/SmsPay	24,041
4	Android-Trojan/SmsReg	21,903
5	Android-PUP/FakeInst	17,260
6	Android-Trojan/Opfake	10,790
7	Android-PUP/Noico	8,767
8	Android-PUP/AutoSMS	8,338
9	Android-Trojan/SmsSpy	7,685
10	Android-PUP/SmsSend	4,578



2

SECURITY ISSUE

Pharming Malware Found that Corrupts Browser "Bookmarks"

SECURITY ISSUE

Pharming Malware Found that Corrupts Browser "Bookmarks"

A new type of "pharming" malware has recently been discovered that corrupts the addresses of bookmarked web pages to lure users into landing on fake sites, requiring vigilance from users. The malware takes advantage of the fact that many users keep banks and other financial sites bookmarked for regular visits.

"Pharming" is a type of cyber attack that infects a user's computer with malware, redirecting the user when he or she attempts to access a bank's website and stealing financial information. The newly-discovered pharming malware that corrupts the bookmarked addresses of financial websites is discovered in the form of an executable file, as show in Figure 2-1.

Figure 2-1 | File "exp.exe"

Running "exp.exe" creates and executes the files '4.exe' and '5.exe' in a predetermined path, as shown in Figure 2-2.

Figure 2-2 | Files "4.exe" and "5.exe"

Executing "4.exe" directs the system to the web page "user.qzone.qq.com" and calls the URL of a fake website and counter page.

```
[Fake Web page URL Information]
... above omitted
<title>my********.com [http://3********4.qzone.qq.com]
</title>
... below omitted
```

```
[Counter Page URL information]
... above omitted
<title>s********1.com [http://5******2.qzone.qq.com]
</title>
... below omitted
```

The malware also accesses "www.get-ip.me" to collect the user's IP address, and receives the system's OS information.

['www.get-ip.me' Information]

... above omitted
Your public IP address is: <h2>1**.***.***.164</h2>
... below omitted

Figure 2-3 | Collecting OS information

Then, the malware checks the location where the web browser's bookmark file is stored in order to alter the URLs.

Table 2-1 | Bookmark File Locations by Browser

Operation System	Browser	Bookmark File Path
Windows 7 / 8	Chrome	C:\User\[User ID]\AppData\Local\ Google\Chrome\User Data\Default\Bookmarks
	Internet Explorer	C:\User\[User ID]\ Favorites\
Windows XP	Chrome	C:\Documents and Settings\[User ID]\Local Settings\Application Data\Google\ Chorme\User Data\ Default\Bookmarks
	Internet Explorer	C:\Documents and Settings\[User ID]\ Favorites\

After collecting and checking the URLs, the malware then swaps them with the address of a fake web page if there are keywords such as "bank" in the URLs. Also, the IP address and OS information are sent to the counter page. The creator of the malware uses such a counter page to keep track of the number of infected systems.

Figure 2-4 | Network information being transmitted

Once the user accesses the fake website of the financial institution using the corrupted bookmark URL, a counterfeit site that deliberately emulates the real site is displayed to the user. When the user clicks any button on the fake page, a popup window appears demanding "additional confirmation to ensure a secure online banking transaction." Clicking "OK" leads to a page that lures the user to enter personal and financial information.

Labeled with spurious titles such as "Taking Caution Against Bank Frauds," the page in fact not only demands the user's name, national identification number and mobile phone number but also critical personal information including account number, PIN, user ID and password, authentication certification password, and security card number. Any

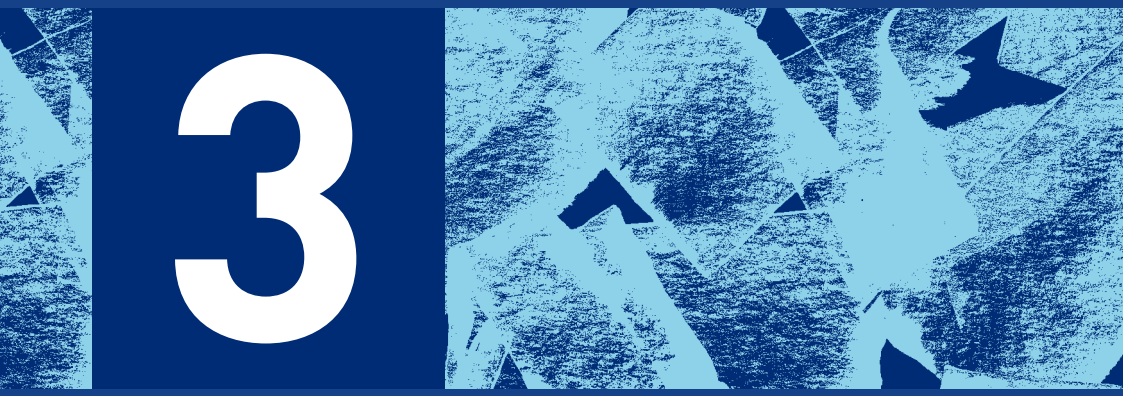
information entered into the fake page by the user is sent directly to the attacker.

It has actually been a decade since pharming malware first appeared, with the first case reported in 2011 and the number of attacks steadily rising since then. Recently these types of malware are becoming more advanced in order to bypass security solutions such as anti-virus software and deceive users. The most recent variant of pharming malware that alters bookmarks differs from traditional malware by not registering the malware as a startup application or in the service domain. Since the malware does not reactivate itself after the initial execution, the infection is harder to detect.

The corresponding alias from V3, AhnLab anti-virus products, is as below:

< Alias from V3 Products >

Trojan/Win32.Banki (2015.07.04.01)



3

IN-DEPTH ANALYSIS

'Cryptolocker' Claws Its Way into Smart Phones

SECURITY ISSUE

‘Cryptolocker’ Claws Its Way into Smart Phones

Of all the security threats that broke the surface in 2015, "Ransomware" is without a doubt one of the most high-profile. In South Korea, uproar was caused last April by a "Cryptolocker" ransomware that was distributed via a banner link on a popular community site. Notably, the ransomware supported Korean language, indicating that it had been designed to target users in a certain geographic region.

The threat has recently become even more serious with the appearance of ransomware that targets Android-based smart phones. This report presents the structure and modus operandi of recently-discovered mobile ransomware.

Last July, AhnLab detected a smart phone ransomware that holds a smart phone user's data hostage demanding payment for its release, and shared this information with security authorities and issued a warning to users. The attacker created and distributed a malicious app called "Adobe Flash" that tries to disguise as the authentic "Adobe Flash Player." The malicious app demands excessive permission and administrator settings during its installation process; if the user does not pay careful attention to the name of the app or installs the app despite the unusual demands, the phone becomes infected with ransomware.

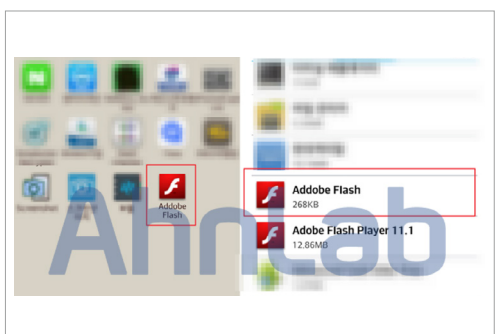


Figure 3-1 | Malicious app (left) and the list of installed applications (right)

Permission information regarding the installation of an app can be verified by checking AndroidManifest.mxl, and the manifest information for this malicious app is as shown below in Figure 3-2.

Let's now examine this app's installation process as well as the permissions it demands. First, the app asks for permissions for network communication, phone calls and system tools, as well as phone manager (device manager).

This app compiles the server addresses in the resource domain as well as the codes in com.lock.a.fclass to transmit the following information to the hacker:

- OS version
- Smart phone model name
- IMEI (International Mobile Equipment Identity)
- Country information

Figure 3-3 | Information collected and sent (server address)

Figure 3-4 shows the network packet that transmits the information collected by the malicious app.

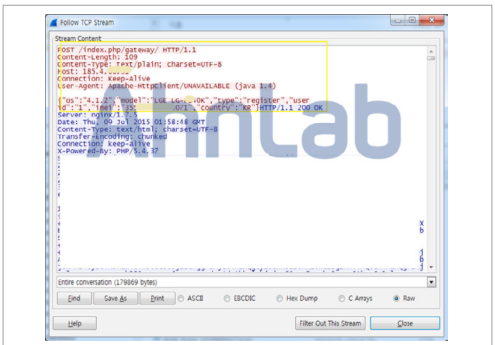


Figure 3-4 | Transmission packet sending the smart phone's information

Also, the smart phone displays a file as shown in Figure 3-5 claiming that "the files on the smart phone have been encrypted and the phone locked, and a payment of $100 must be paid within a certain period of time in order to restore the phone." Once this malicious app infects the phone, it locks the phone and prevents the user from switching out of the display screen or operating the phone.

Figure 3-5 | Ransomware infection by a malicious app

Besides, an interesting feature of this app has been discovered. The ransomware is not activated if the smart phone's country information is set to Russia. Figure 3-6 shows the malicious app's code that checks the phone's country information.

Figure 3-6 | Malicious app's code that checks country information

Once the smart phone is infected by ransomware, the user can no longer control the phone. In most cases, removing the malicious app or running existing apps becomes impossible. When an infection by the recently-found "Adobe Flash" malicious app occurs, the user needs to boot the phone in "safe mode" and access the [settings] - [device administrator] to disable the malicious app that contains the ransomware. The app can then be removed using the application manager. Note that different manufactures may use different methods for booting the phone in safe mode, and the devices' manual should be consulted for instructions.

Users are required carefully checking reviews when downloading an app in order to minimize exposure to increasingly serious security threats that target smart phones. The same applies for apps downloaded via the official app market. Users should also avoid clicking URLs contained in text messages (SMS). The use of mobile anti-virus application such as V3 Mobile is highly recommended.

The corresponding alias from V3, AhnLab anti-virus products, is as below:

< Alias from V3 Products >

Android-Trojan/Slocker

AhnLab

ASEC REPORT

VOL.67
July, 2015

Contributors ASEC Researchers
Editor Content Creatives Team
Design Design Team

Publisher AhnLab, Inc.
Website www.ahnlab.com
Email global.info@ahnlab.com