Security Trend

ASEC REPORT

VOL.65

May, 2015

AhnLab

ASEC REPORT

VOL.65 May, 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 May 2015

Table of Contents

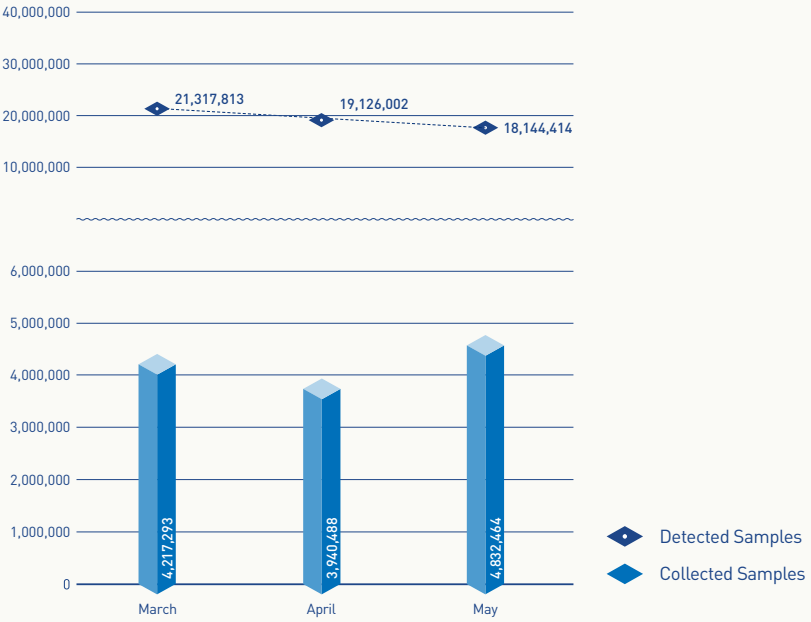
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

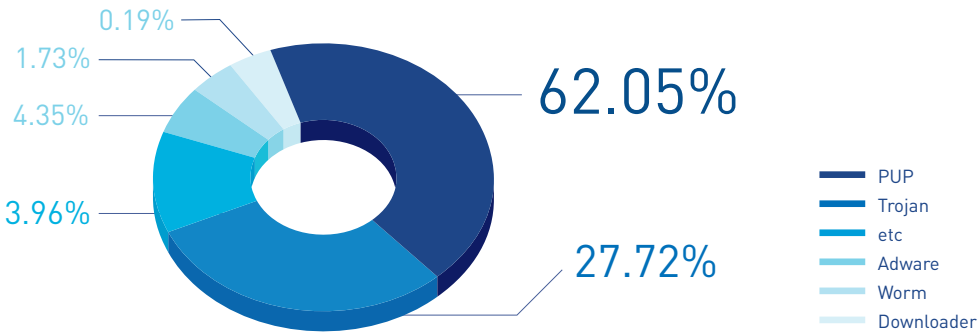
According to the ASEC (AhnLab Security Emergency Response Center), 18,144,414 malware were detected in May 2015. The number of detected malware increased by 981,588 from 19,126,002 detected in the previous month as shown in Figure 1-1. A total of 4,832,464 malware samples were collected in May.



[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 May 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 62.05% of the total. It was followed by Trojan (27.72%) and Adware (4.35%).



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

Table 1-1 shows the Top 10 malware threats in May categorized by alias. PUP/Win32. BrowseFox was the most frequently detected malware (2,155,648), followed by PUP/ Win32.MicroLab (1,563,164).

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

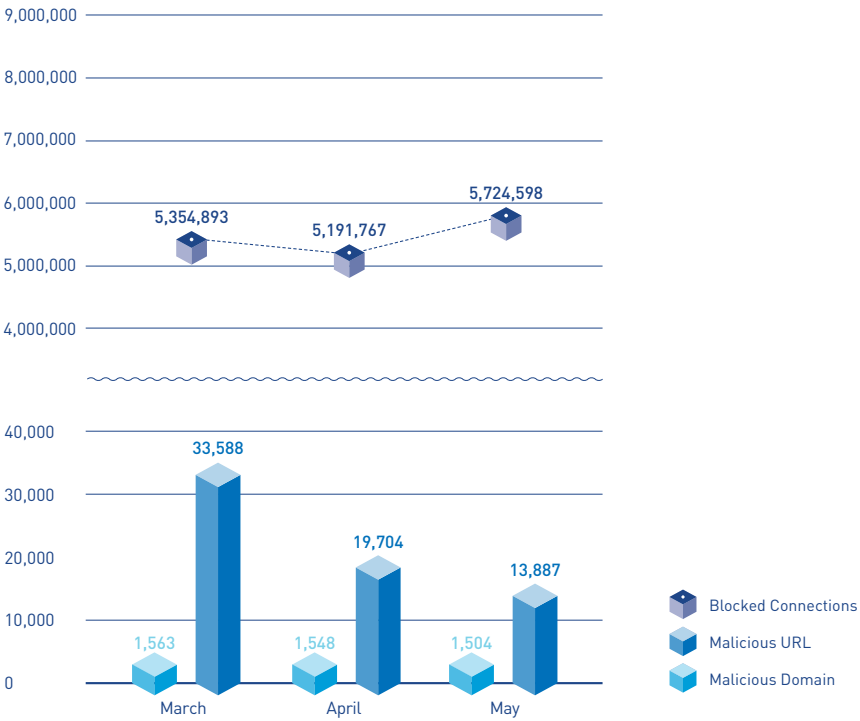
Rank	Alias from AhnLab	No. of detections
1	PUP/Win32.BrowseFox	2,155,648
2	PUP/Win32.MicroLab	1,563,164
3	PUP/Win32.MyWebSearch	1,097,760
4	PUP/Win32.Enumerate	830,077
5	PUP/Win32.Helper	756,388
6	PUP/Win32.MultiPlug	437,970
7	PUP/Win32.SubShop	371,442
8	PUP/Win32.WindowsTap	362,236
9	PUP/Win32.CloverPlus	335,107
10	PUP/Win32.WindViewer	286,775

SECURITY STATISTICS

02

Web Security Statistics

In May 2015, a total of 1,504 domains and 13,887 URLs were comprised and used to distribute malware. In addition, 5,724,598 malicious domains and URLs were blocked.



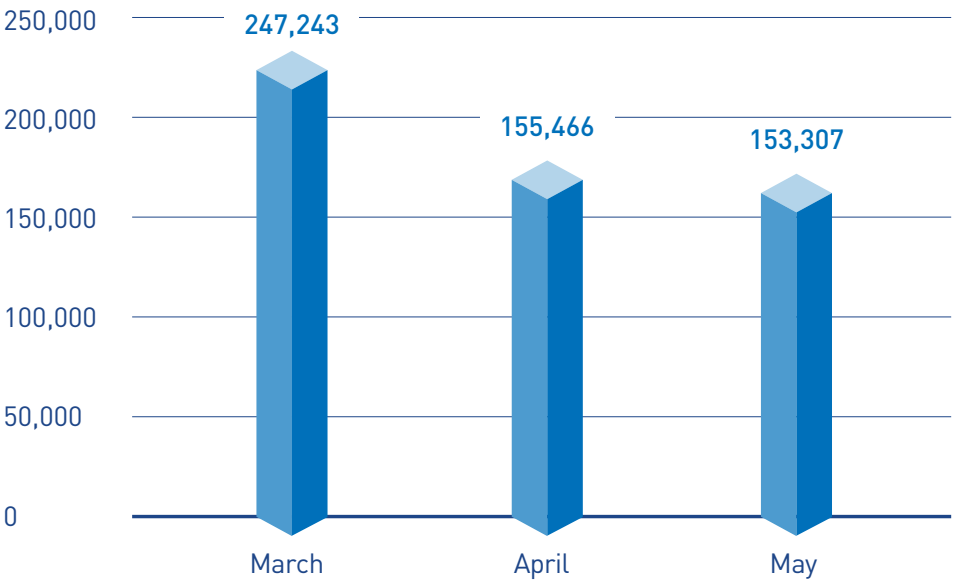
[Figure 1-3] Blocked Malicious Domains/URLs in May 2015

* "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 May 2015, 153,307 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 May 2015. Android-PUP/SmsReg was the most distributed malware with 64,697 of the total, following the previous month.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsReg	64,697
2	Android-PUP/Noico	13,667
3	Android-PUP/Zdpay	11,222
4	Android-Trojan/AutoSMS	8,222
5	Android-PUP/Airpush	6,256
6	Android-PUP/Dowgin	5,668
7	Android-Trojan/FakeInst	3,565
8	Android-PUP/SmsPay	2,880
9	Android-Trojan/SmsSpy	2,389
10	Android-PUP/Wapsx	2,178

2

SECURITY ISSUE

Ransomware, Now Coming to a Mobile Near You

SECURITY ISSUE

Ransomware, Now Coming to a Mobile Near You

Ransomware such as CryptoLocker, which has been gaining notoriety recently, are increasing in both number as well as technical sophistication. Ransomware is a type of cyber threat that attacks a system by encrypting its files and demanding a ransom for their restoration. A ransomware infection not only renders a system's files unusable but can also result in serious lasting damage as there is no guarantee that the infected files will be restored even once the ransom has been paid.

PC users were the main targets of ransomware until recently; smart phones, however, are increasingly becoming attractive targets for attackers. There are as many smart phone users today as PC users, and vast amounts of personal information and important data are stored on mobile devices.

Various types of mobile ransomware applications targeting Android mobile phones have begun to appear. These types of ransomware either make the devices inoperable or encrypt the data stored in them. This article presents three types of mobile ransomware that have appeared recently.

1. Android-Trojan/Koler: Impersonating the FBI

Android-Trojan/Koler is a ransomware application that lures victims with child pornography, often disguised as an application named "PornDroid". Other common names include "Videos" or "Sex Tube."

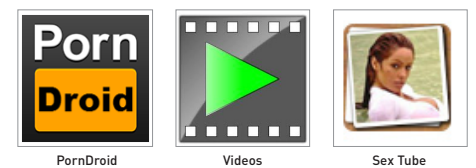


Figure 2-1 | Fake icons frequently employed by Android-Trojan/Koler

This article shows the detail how the fake app "PornDroid, which is the Android-Trojan/Koler ransomware, works.

This ransomware activates immediately after installation is complete, and displays a screen that is labeled "Package installation." This malicious app claims itself to be from Google and tricks the user into giving it device administrator (admin) permission, then takes a photograph using the onboard camera. The photograph is used later to demand a ransom from the user.

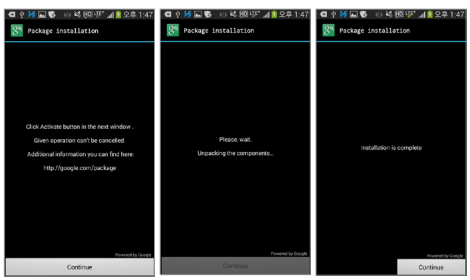


Figure 2-2 | Malicious app activation being disguised as a normal installation process

After a period of time has expired after installation, the malicious app deactivates the device's normal lock screen and then locks the display, preventing the user from controlling the device. The home key and other buttons are either disabled or rendered useless because the malicious app's display screen is fixed on the forefront of the display and overlaps any normal screen output.

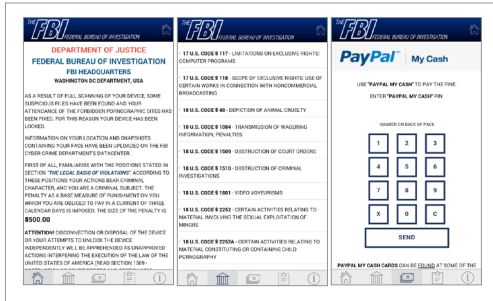


Figure 2-3 | Fake warming message claiming to be from the FBI

The malware app locks the screen with a display shown in Figure 2-3 above, claiming to be a message from the FBI and stating that "the user has been restricted due to access to child pornography, and a fine must be paid." Along with the warning, the malicious app scans contact information or Web browsing history from the device and displays them to the screen.

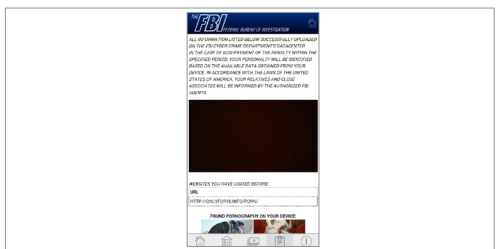


Figure 2-4 | Pornographic images and a picture of the user taken by the phone are displayed

The app also displays a picture taken by the device's front-facing camera, along with pornographic images.

2. Android-Trojan/Simplelocker: Mobile ransomware that encrypts stored data

Android-Trojan/Simplelocker is a ransomware that encrypts the files stored on the device to prevent their access. Certain files stored in the external storage of the device are encrypted, and the original files deleted to prevent the user from accessing the data.

Figure 2-5 | Fake icon employed by Android-Trojan/Simplelocker

The malicious app usually masks itself as Flash Player, sometimes using a similar icon and the name Video Player. The malicious app uses SMS or http to communicate with the C&C server. When installed, the malware demands device admin permission, and attempting to run the app after installation results in no visible response.

The app begins encrypting the files on the device. The encryption key is contained in the code. A string in the code is hashed with SHA-256, and the resulting value is used to generate a key. Files on the device are encrypted using the generated key then changed to .enc extensions, after which the original files are deleted. The app will attempt to encrypt files with extensions such as jepg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp, and mp4 found on the device's external storage.

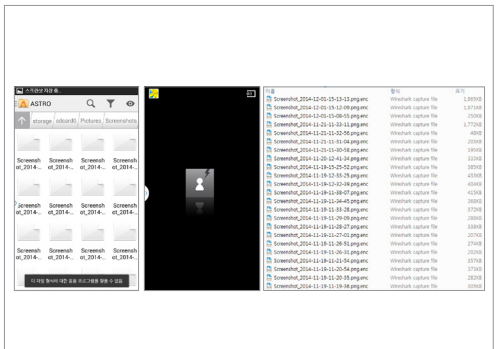


Figure 2-6 | Data encrypted by the malicious app

3. Android-Trojan/Slocker: Targeting Russian smart phone users

Unlike most malicious app that uses English as its interface language, Android-Trojan/Slocker is a ransomware app that uses Russian.

This malicious app does not have a data encryption feature, but prevents normal use of the mobile device by locking the screen with its own display in the foreground.

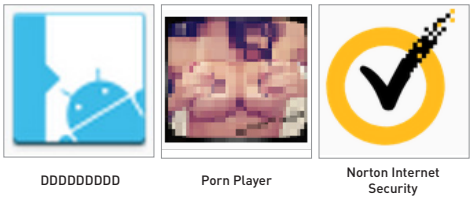


Figure 2-7 | Fake icons employed by Android-Trojan/Slocker

Android-Trojan/Slocker often disguises as a security application, or uses deceptive names such as Flash Player. The malicious app has recently been found disguising itself as an adult app named Porn Player, or uses alphabetical names such as DDDDDDDDD or AAAAAAAAA. Let's examine a variation with the name "DDDDDDDDD".

Like other types of malicious app, this malicious app demands admin permission, and especially Android system security admin. Once permission for admin is given, a Russian-language screen is displayed as shown in Figure 2-8, stating that the device will be unlocked if a monetary payment is made and giving detailed instructions. This screen is locked on the forefront of the display, covering any other displays or actions produced by pressing on the home button, preventing the normal use of the device.

Figure 2-8 | Russian-language screen demanding a payment within a timeframe

Ransomware is difficult to remove once it is installed, and important data can be lost if the ransomware encrypts files on the system. Users can easily be tricked into installing these types of attack as most malicious app disguise as well-known apps, so the user should carefully check reviews and other information about the app and take care not to install apps from an uncertain origin. Mobile anti-virus application such as V3 Mobile should be employed to monitor the smart phone during regular use against malware infections.

The following In-Depth Analysis presents how to deal with mobile ransomware that target Android smart phones.

3

IN-DEPTH ANALYSIS

How to Remove Mobile Ransomware Applications

SECURITY ISSUE

How to Remove Mobile Ransomware Applications

Most of the ransomware apps mentioned in the Security Issue above lock its own screen on the device's forefront, covering every other display and preventing the normal use of the phone. The screen returns even if the device is rebooted, and cannot be removed or shut down like normal applications. For now, two solutions are available: removal through safe mode, and removal using ADB.

In this regard, this article examines how to deal with mobile ransomware such as Android ransomware Android-Trojan/Koler, Android-Trojan/Simplelock and Android-Trojan/Slocker.

1. Removal by booting in safe mode

Simpler ransomware can be removed by booting the device in safe mode, which deactivates all applications except the basic system applications on the device. Since ransomware is not a system application, they will not run if the device is booted in safe mode.

However, applications that have admin control cannot be removed. In this case, it requires disabling admin control before deleting the malicious app.

Some ransomware, however, will lock the screen again with its display if the use attempts to remove device admin permission, preventing the user from taking control of the device and removing the malicious app.

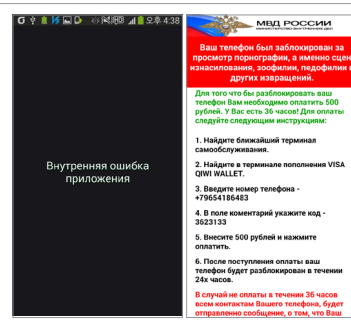


Figure 3-1 | Android-Trojan/Slocker preventing removal of admin permission

In such cases were ransomware cannot be removed using safe mode, ADB must be enlisted to end the ransomware application process and remove it.

2. Removal using ADB

ADB (Android Debug Bridge) is a command line tool that allows the user to communicate with an Android device, and can be used to install or remove apps, run shell commands, and check system loads. Using the ADB, the user connects the device with a PC to end the ransomware's process and remove it.

① Activate USB debugging

To use ADB, Android SDK must first be installed on the PC. Then, USB debugging must be activated on the device. On an infected device, the user must shut down the device and reboot in safe mode.

② Verify device and connect via ADB

Connect the PC and the smart phone with a USB cable, and run the command line prompt and find the subdirectory "Platform-tools" in the Android SDK folder where adb utility is located. Run the "adb devices" command to pull up a list of smart phones detected by the ADB server.

```
C:₩Users₩Jeonggeun₩android-sdks₩platform-tools>adb devices
List of devices attached
3fceb27f        device
```

Figure 3-2 | Device information recognized by the ADB server

to make sure that the device driver has been installed. Then connect using the "adb shell" command.

```
C:₩Users₩Jeonggeun₩android-sdks₩platform-tools>adb shell
shell@hltektt:/ $
```

Figure 3-3 | Connecting using ADB

③ Check ransomware app package name in order to shut down a ransomware app that disturbs removal, the app package name must be checked. The command "am kill-all" could be used to shut down all running apps, but the system window that is needed to delete the app will also be shut down. Thus only the ransomware app must be singled out for shutdown.

First, proceed with the removal process in safe mode including disabling admin control, and once the ransomware application re-launches itself enter the command "dumpsys activity activities | grep –i run" using ADB. This command allows the user to check the activity log of applications currently running on the device, as shown in Figure 3-4.

```
C:₩Users₩Jeonggeun₩android-sdks₩platform-tools>adb shell
shell@hltektt:/ $ dumpsys activity activities | grep -i run
dumpsys activity activities | grep -i run
  Running activities (most recent first):
    Run #2: ActivityRecord{43473c30 u0 com.android.settings/.SettingsReceiverActivity}
    Run #1: ActivityRecord{460749c0 u0 conner.version.mantle/.SandBoardU}
    Run #0: ActivityRecord{42ab88b8 u0 com.sec.android.app.launcher/com.android.launcher2.Launcher
```

Figure 3-4 | Android activity stack of running apps

In Figure 3-4, "com.android.settings", "commer.version.mantle" and "com.sec.android.app.launcher" are the package names, indicating that activities with those package names are currently running.

The command "am force-stop <package name>" can now be used to shut down an application that is running, allowing the user to determine which is the ransomware app that has hijacked his device.

```
shell@hltektt:/ $ am force-stop commer.version.mantle
am force-stop commer.version.mantle
```

Figure 3-5 | A forced shutdown of the app with the package name "commer.version.mantle"

In this example, shutting down the app with the package name "commer.version.mantle" by entering the command "am force-stop commer.version.mantle" shuts down the ransomware application on the device. This reveals that "commer.version.mantle" is the package name for the ransomware.

④ Shut down and remove the ransomware app

Proceed with the shutdown of the ransomware that is blocking the user from removing admin permission. The first step is to deal with admin control. This article shows how to delete Android-Trojan/Slocker.

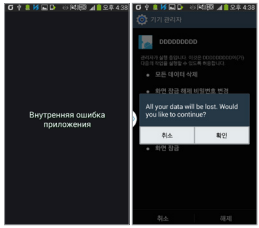


Figure 3-6 | Shutting down a ransomware app that is blocking admin control removal

The ransomware app's display screen will reappear if an attempt is made to remove admin permission from the app. Shut down the app by using the "am force-stop <package name>" command. Once the ransomware app's screen lock disappears, the admin permission removal process can continue. If the ransomware screen should appear again, the same method can be used to force a shutdown and continue.

The mobile ransomware application can be deleted once device admin permission is removed. An alternative method for dealing with ransomware app that encrypts data is to back up the app and extract the encryption key from the app itself, and use it to restore affected files.

AhnLab

ASEC REPORT

VOL.65
May, 2015

Contributors **ASEC Researchers**
Editor **Content Creatives Team**
Design **Design Team**

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