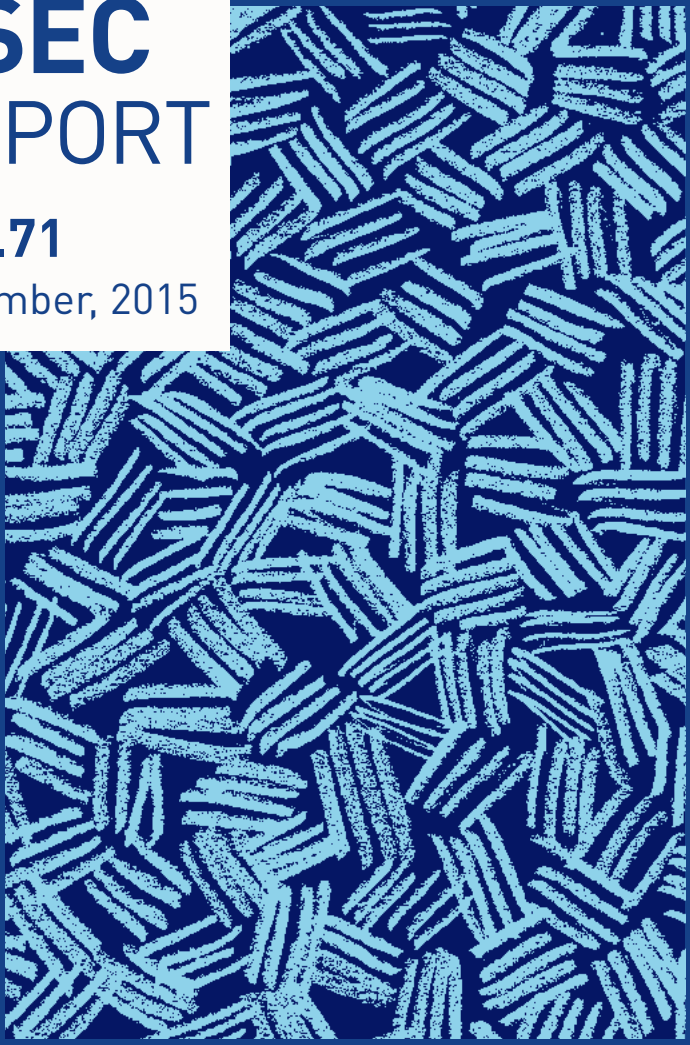
Security Trend

ASEC REPORT

VOL.71

November, 2015



AhnLab

ASEC REPORT

VOL.71 November, 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 November 2015

Table of Contents

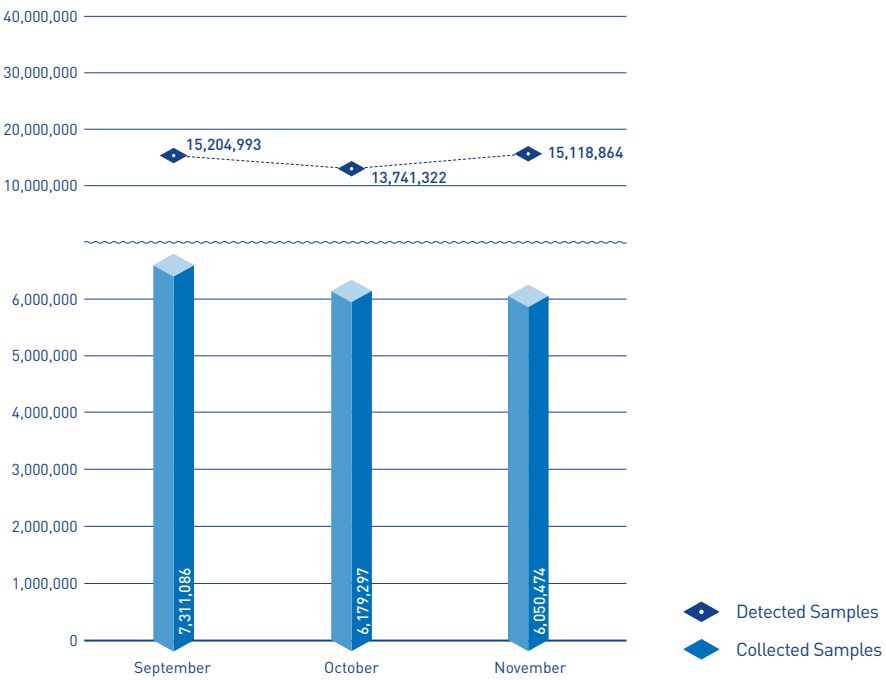
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

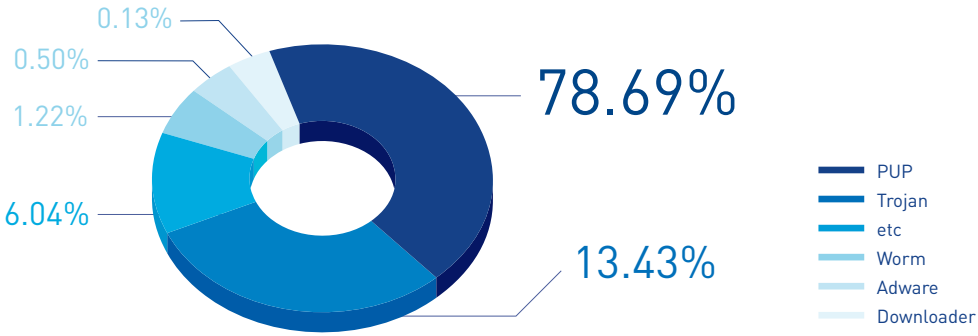
According to the ASEC (AhnLab Security Emergency Response Center), 15,118,864 malware were detected in November 2015. The number of detected malware increased by 1,377,542 from 13,741,322 detected in the previous month as shown in Figure 1-1. A total of 6,050,474 malware samples were collected in November.



[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 November 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 78.69% of the total. It was followed by Trojan (13.43%) and Worm (1.22%).



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

Table 1-1 shows the Top 10 malware threats in November categorized by alias. Trojan/Win32.Starter was the most frequently detected malware (163,725), followed by Trojan/Win32.Agent (123,725).

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

Rank	Alias from AhnLab	No. of detections
1	Trojan/Win32.Starter	163,725
2	Trojan/Win32.Agent	123,725
3	Malware/Win32.Generic	112,866
4	Trojan/Win32.Teslacrypt	80,540
5	Trojan/Win32.Gen	77,381
6	ASD.Prevention	68,510
7	Worm/Win32.IRCBot	58,657
8	Trojan/Win32.Neshta	56,148
9	Unwanted/Win32.Exploit	55,902
10	Trojan/Win32.Banki	53,502

SECURITY STATISTICS

02
Web Security Statistics

In November 2015, a total of 1,318 domains and 10,029 URLs were comprised and used to distribute malware. In addition, 4,399,439 malicious domains and URLs were blocked.

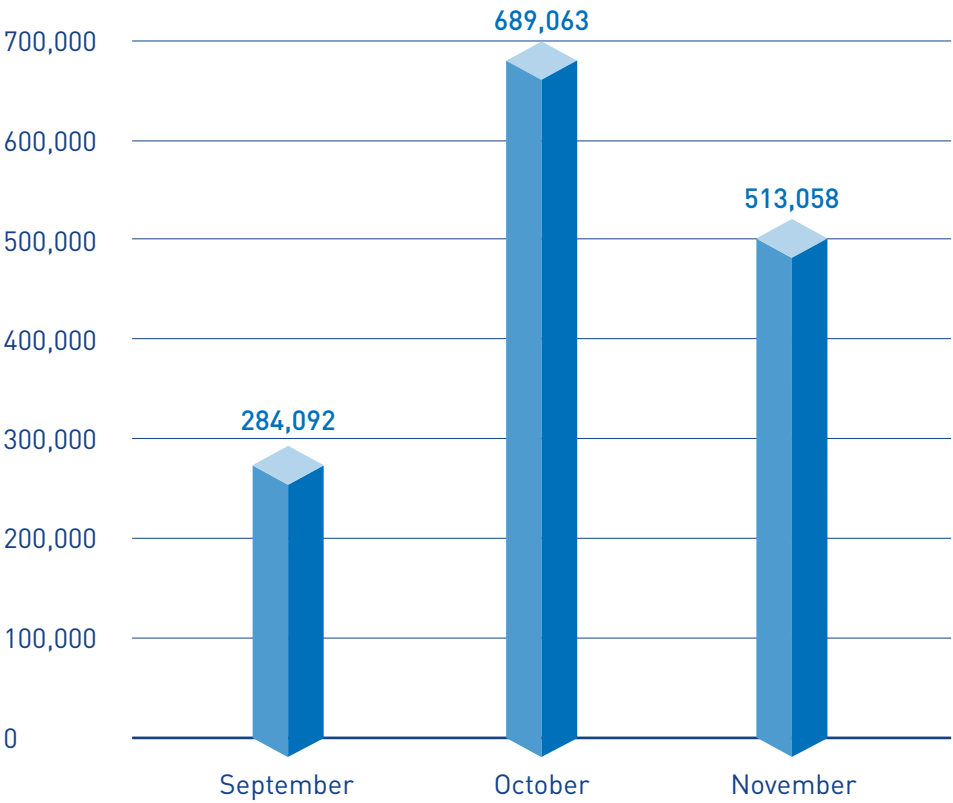
[Figure 1-3] Blocked Malicious Domains/URLs in November 2015

* "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 November 2015, 513,058 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 November 2015. Android-PUP/SmsPay was the most distributed malware with 127,427of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	127,427
2	Android-PUP/SmsReg	125,621
3	Android-Trojan/FakeInst	66,462
4	Android-PUP/Noico	27,590
5	Android-Trojan/Opfake	19,403
6	Android-Trojan/SMSAgent	13,043
7	Android-PUP/Zdpay	10,381
8	Android-PUP/Dowgin	9,925
9	Android-Trojan/SmsSend	7,727
10	Android-Trojan/SmsSpy	6,687

2

SECURITY ISSUE

DroidJack Malicious App Invades Europe

SECURITY ISSUE

DroidJack Malicious App Invades Europe

In late October of 2015, British police arrested a 28 year-old man "under suspicion of computer misuse act offenses." According to BBC reports, the man had purchased a malicious mobile app called "DroidJack." German and Swiss authories also carried out house searches of people suspected of purchasing the malicious app, arresting over ten people who were charged with the purchase or use of the app. The arrests were part of "Operation DroidJack," a joint effort to stamp out cyber crime by police in Germany, France, the United Kingdom, Belgium, Switzerland and the United States.

Figure 2-1 | BBC News article on "Operation DroidJack"

DroidJack is a type of malicious spyware called Remote Access Trojan (RAT) targeting Android-based smart phones that monitors the data traffic on the phone, eavesdrops on conversations, and steals camera information and other key data from the phone. DroidJack can be purchased online for about $210 (€190), and demands the following user information after being purchased.

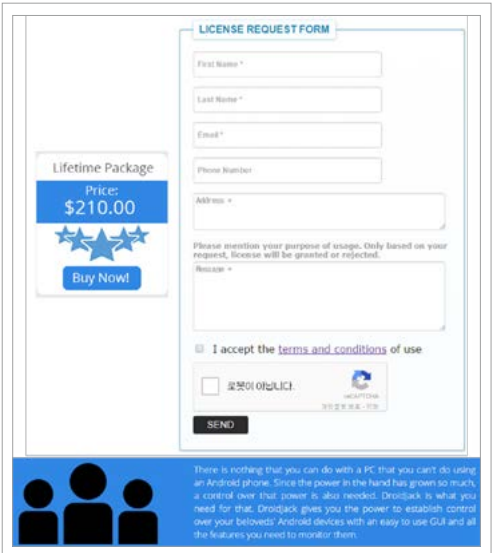


Figure 2-2 | Features and price of DroidJack v2.6

DroidJack enables APK builds and contains features that hijacks the targeted smart phone's information and monitors the phone's activities. DroidJack's main functions can be listed as follows:

- apk file builder
- Hijack files stored on the smart phone
- Send files to the smart phone
- Hijack SMS
- Send SMS
- Hijack call history
- Hijack contact list
- Eavesdrop and record using the smart phone's mic
- Hijack internet browsing history and bookmark information
- Hijack location data
- Run apps, hijack app information
- Hijack IMEI, MAC, mobile service provider information, rooting information, etc.

DroidJack provides a console screen as shown below to monitor the infected smart phone. The console allows the attacker to record the phone's conversations, track the phone's location, check SMSs, hijack browser history, and carry out a variety of other nefarious actions.

Figure 2-3 | DroidJack v2.6 builder and monitoring console

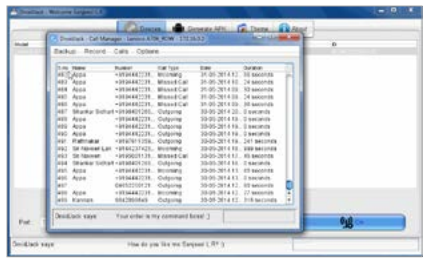


Figure 2-4 | DroidJack's call history tracking

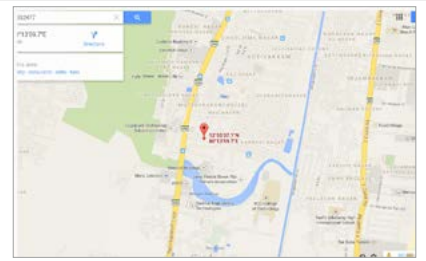


Figure 2-5 | DroidJack's GPS information detection

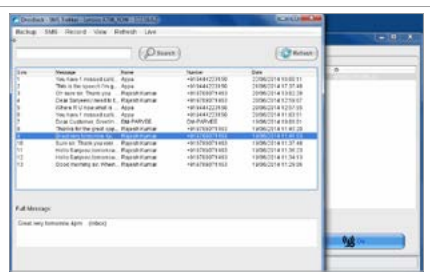


Figure 2-6 | DroidJack's SMS tracking

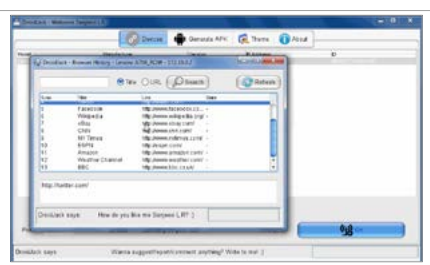


Figure 2-7 | DroidJack's browser history tracking

Malicious apps targetting Android phones are usually disguised as icons for Google, or utilities and well-known games that often trick unsuspecting users into installing them. DroidJack is also distributed in the guise of a variety of apps, and AhnLab has listed some of the common icons used to hide DroidJack in Figure 2-8 below (*Note that some of these apps were created for testing as well).

Figure 2-8 | List of fake icons used by DroidJack

Drawing from the list above, let us examine DroidJack disguised as the icon for "Agar.io," a famous mobile game.

The malicious app, which disguises itself as the icon for Agar.io, a game, first demands the permissions during the installation process. Executing the app removes the icon as an attempt to erase any traces of its presence on the smart phone.

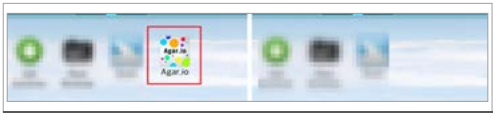


Figure 2-9 | Installation icon (left) / the icon removed following installation and execution (right)

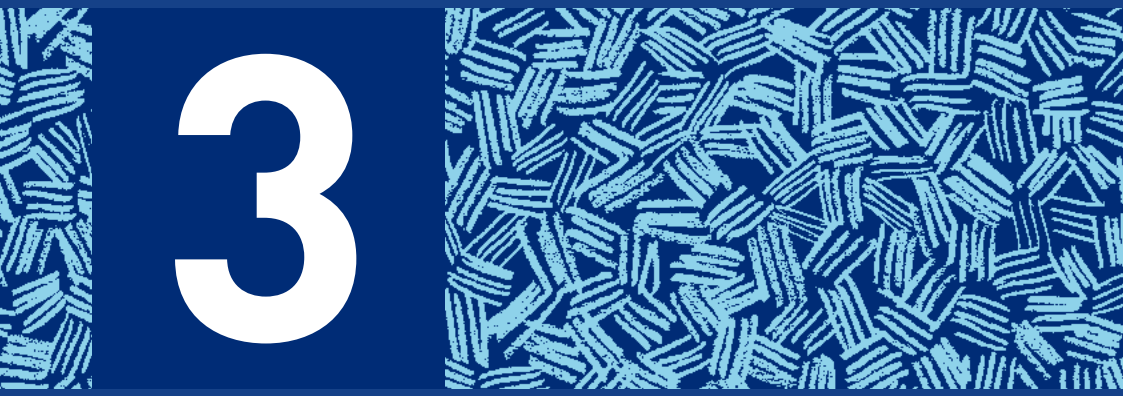
Figure 2-9 shows the malicious app disguised as Agar.io installed on the smart phone. The app secures a number of rights needed for its malicious activities during the installation process. Once completed, the app removes its own icon to prevent the user from detecting the precense of the app on the phone.

As can be seen in the case of DroidJack, malicious apps have recently evolved to disguise itself as a well-known app familiar to the user to install itself on the phone, hijacking important information and malappropriating the smart phone's functions. It is advisable to use mobile anti-virus apps, such as V3 Mobile Security in order to prevent mobile malicious apps from infecting the phone.

The corresponding alias from V3 Mobile products, AhnLab's mobile anti-virus program, is as below:

<Alias from V3 Mobile products>

Android-Trojan/Sandrorat



3

IN-DEPTH ANALYSIS

Notorious Ransomwares: TeslaCrypt vs. CryptoWall

IN-DEPTH ANALYSIS

Notorious Ransomwares: TeslaCrypt vs. CryptoWall

With ransomware becoming an increasingly serious security threat, TeslaCrypt and CryptoWall were found to have caused the highest number of infections in South Korea in November.

First discovered in 2013, CryptoWall has continued to evolve and, as shown in Figure 3-1, encrypts the files on the user's PC using an RSA key and demands a payment for restoring the files. The ransomware continues to be "upgraded," with CryptoWall 3.0 being discovered in January of 2015, just two years after the ransomware was first spotted, and a new incarnation appeared in just ten months since then in November.

TeslaCrypt was first found in South Korea around February or March, 2015. The most recent version of TeslaCrypt encrypts a system's files and uses an "*.ccc" extension, leading some people to call it "CCC ransomware."

Figure 3-1 | CryptoWall 2.0, 3.0 and the latest version

Figure 3-2 | TeslaCrypt 2.0 encoding and ransom demand .html file (text removed for only CryptoWall version)

Earlier version of TeslaCrypt used the same output message used by "CryptoLocker." TeslaCrypt 2.0 was also found to be using the same .html

file that contains the infection message for CryptoWall. Like CryptoLocker, TeslaCrypt uses AES key to encrypt the files of the target computer even though the actual message displayed to the user states that the RSA encryption has been used.

The similar message leads some users to think that TeslaCrypt is a variant of CryptoWall, and the two can be distinguished using the following indicators:

1. Names of encrypted files following infection

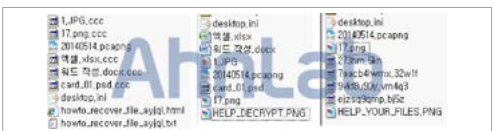


Figure 3-3 | TeslaCrypt(left) / CryptoWall 3.0(center) / CryptoWall 4.0(right)

2. Encoding and ransom demand message file after infection

3. Registry verification

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

<Aliases from V3 products>

Trojan/Win32.Teslacrypt (2015.11.07.02)

Trojan/Win32.CryptoWall (2015.11.11.00)

In addition to CryptoWall and TeslaCrypt, numerous new and existing variants of ransomware continue to be distributed. Newest versions often delete themselves after file encryption has been completed in order to erase traces of the infection. In an increasing number of cases ransomware infections cannot be detected on affected systems.

According to a report published by the Cyber Threat Alliance in October, 2015, CryptoWall 3.0 was distributed via phishing attacks through email (67.3%) and exploit kits (30.7%). In phishing attacks via email, ransomware are often inserted into compressed files such as .zip files. Exploit kits use a method of inserting malware by exploiting weaknesses in the software. To prevent ransomware infections, users should take caution against email from unknown senders or suspicious attachments, and should use the most up-to-date software and security updates to prevent exploit kits from taking advantage of security gaps. Anti-virus programs should be kept up-to-date as well, and users should avoid using file sharing sites or P2P services that frequently serve as routes for distributing ransomware.

AhnLab

ASEC REPORT

VOL.71
November, 2015

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

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