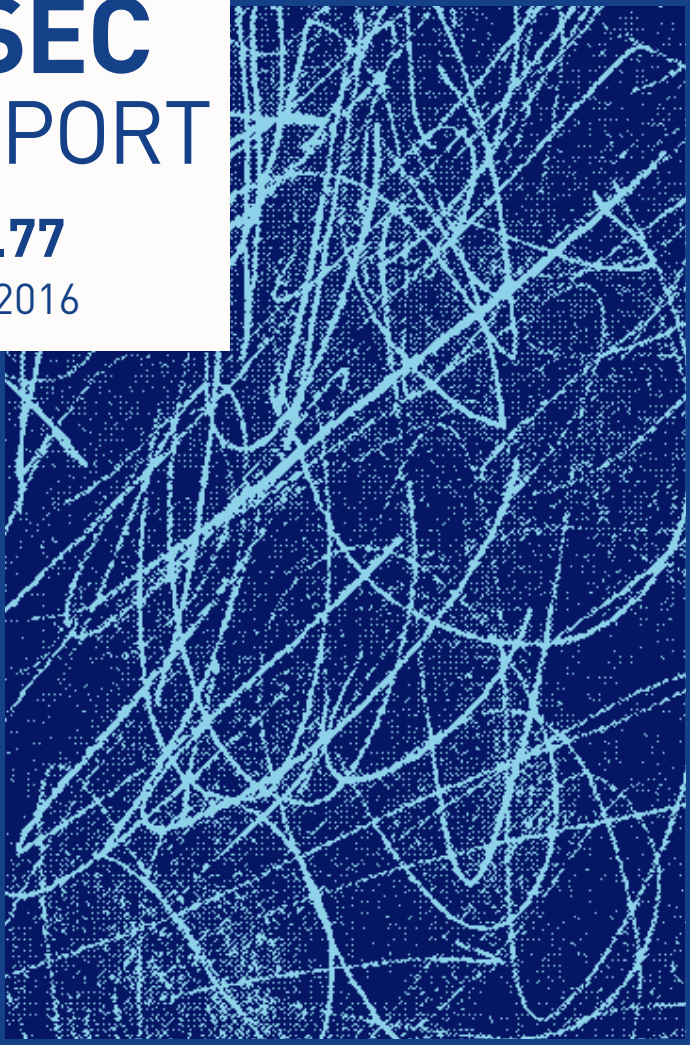
Security Trend

ASEC REPORT

VOL.77

May, 2016



AhnLab

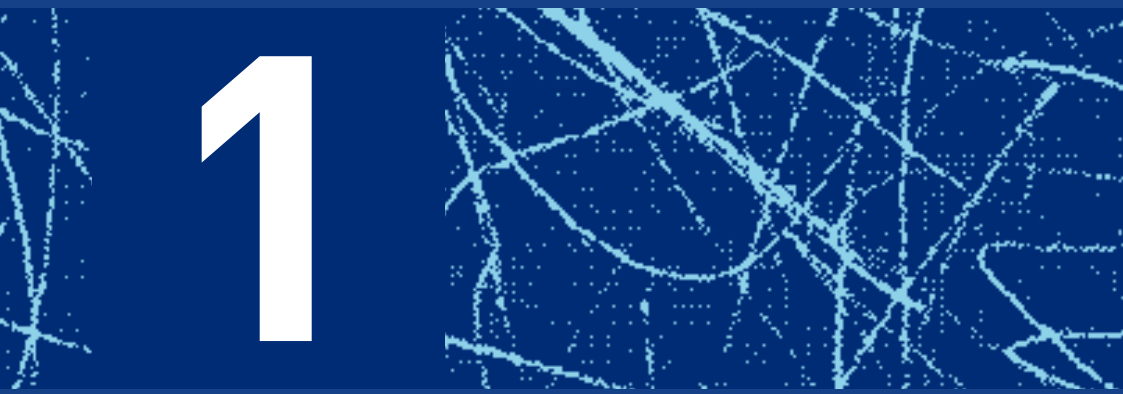
ASEC REPORT

VOL.77 May, 2016

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 2016

Table of Contents



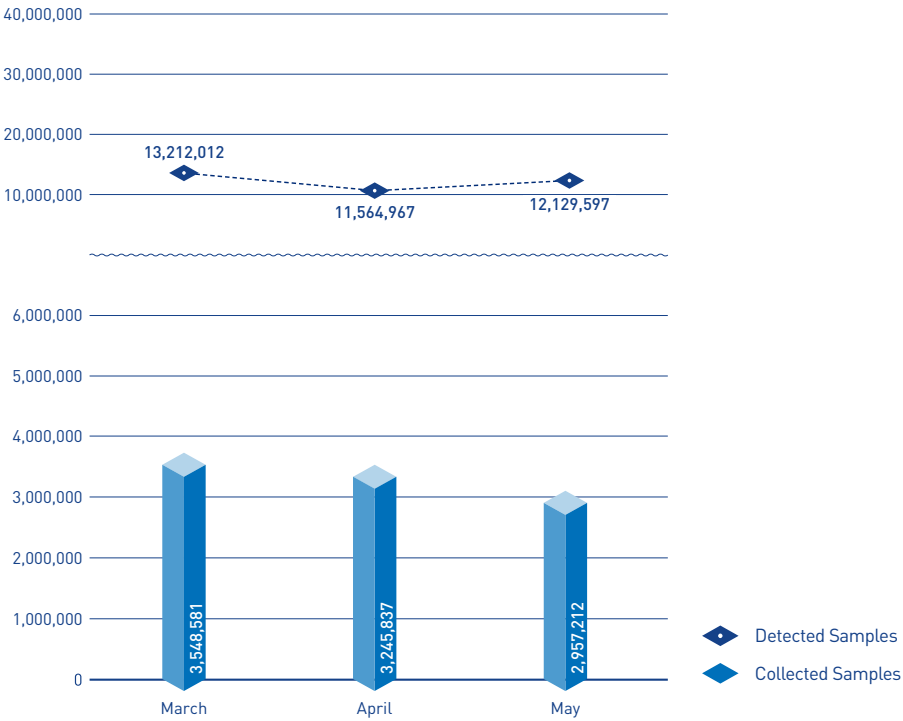
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

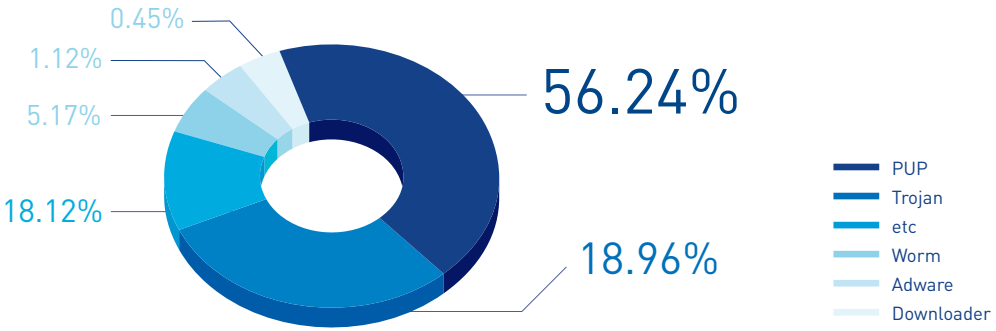
According to the ASEC (AhnLab Security Emergency Response Center), 12,129,597 malware were detected in May 2016. The number of detected malware increased by 564,630 from 11,564,967 detected in the previous month as shown in Figure 1-1. A total of 2,957,212 malware samples were collected in May.



[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 2016. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 56.24% of the total. It was followed by Trojan (18.96%) and Worm (5.17%).



[Figure 1-2] Proportion of Malware Type in May 2016

Table 1-1 shows the Top 10 malware threats in May categorized by alias. Trojan/Win32.Starter was the most frequently detected malware (213,200), followed by Malware/Win32.Generic (151,489).

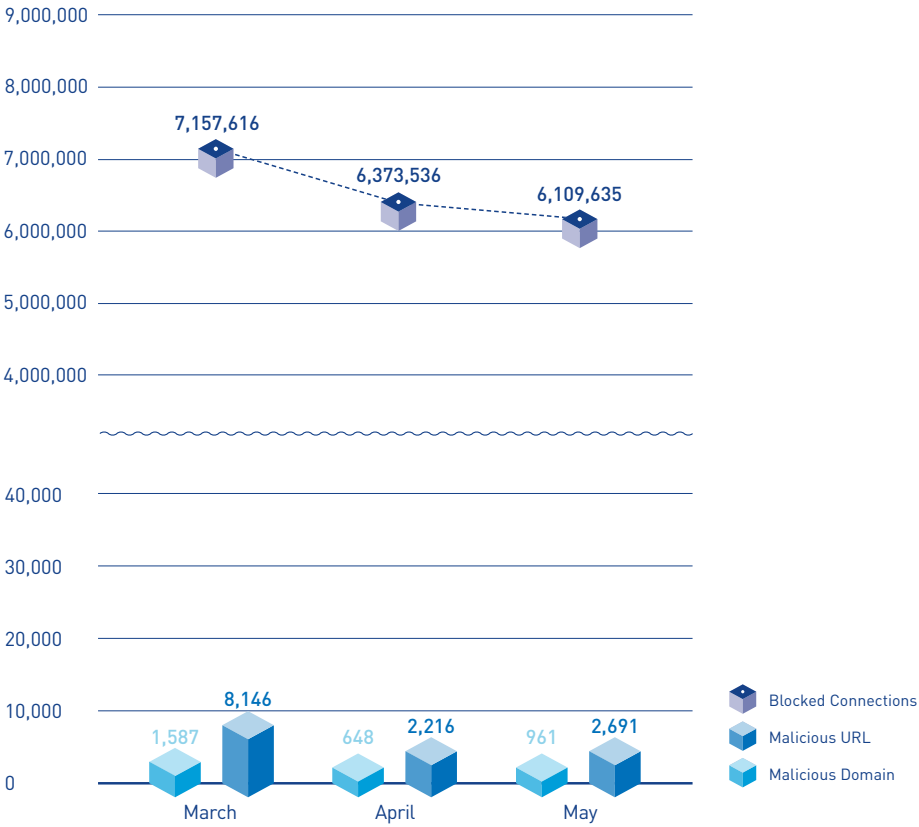
[Table 1-1] Top 10 Malware Threats in May 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
1	Trojan/Win32.Starter	213,200
2	Malware/Win32.Generic	151,489
3	ASD.Prevention	133,951
4	Unwanted/Win32.HackTool	98,724
5	Trojan/Win32.Agent	91,622
6	Trojan/Win32.Neshta	88,477
7	Trojan/Win32.Banki	71,483
8	HackTool/Win32.Crack	61,015
9	Unwanted/Win32.Keygen	58,669
10	Trojan/Win32.Gen	46,207

SECURITY STATISTICS

02
Web Security Statistics

In May 2016, a total of 961 domains and 2,691 URLs were comprised and used to distribute malware. In addition, 6,109,635 malicious domains and URLs were blocked.



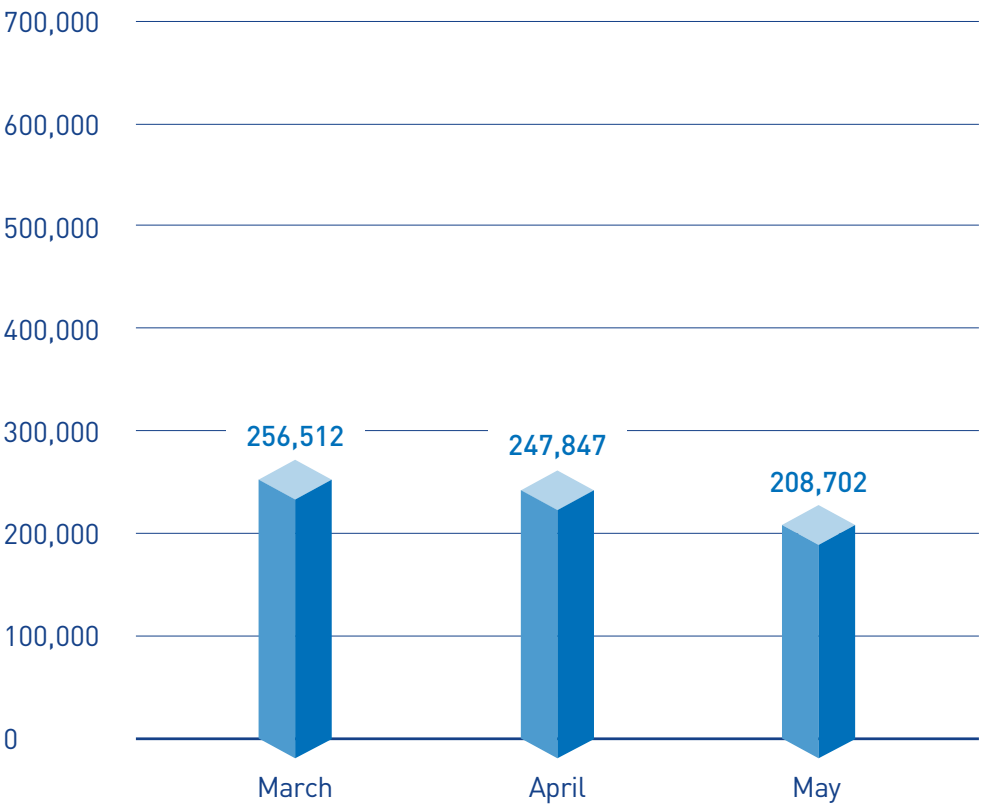
[Figure 1-3] Blocked Malicious Domains/URLs in May 2016

* "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 2016, 208,702 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 2016. Android-PUP/SmsPay was the most distributed malware with 37,247 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsPay	37,247
2	Android-PUP/SmsReg	16,834
3	Android-Trojan/Moavt	15,851
4	Android-PUP/Zdpay	12,246
5	Android-PUP/Noico	12,216
6	Android-PUP/Shedun	11,340
7	Android-Trojan/Hidap	8,566
8	Android-PUP/Dowgin	7,943
9	Android-Trojan/SmsSpy	7,477
10	Android-Trojan/Agent	7,336

2

SECURITY ISSUE

Js/AutoRun Malware Continues to Surface

SECURITY ISSUE

Js/AutoRun Malware Continues to Surface

With the appearance of ransomware written in JavaScript (JS) being discovered recently, a string of JS AutoRun malware have been observed being spread across the internet.

Malware created as a script file can be written with simple code, taking the form of a type of text file rather than a standardized format, and thereby eluding detection by security solutions. This appears to have resulted in the unchecked proliferation of malware written in JavaScript.

The following is a case of frequently discovred AutoRun malware in JS format.

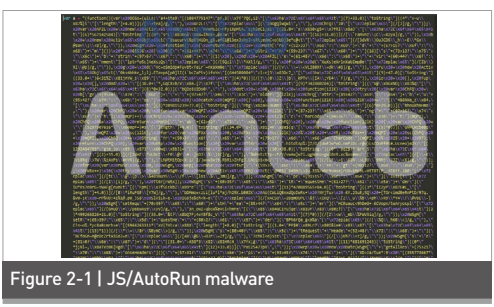


Figure 2-1 | JS/AutoRun malware

The obfuscated JS/AutoRun malware that has been found recently uses ActiveXObject, used to support ActiveX on Internet Explorer, to run the code.

Table 2-1 | JS/AutoRun malware's ActiveXObject functions

ActiveXObject("Wscript.shell")w
ActiveXObject("Scripting.FileSystemObject")
ActiveXObject("Shell.Application");
ActvieXObject("MSXML2.ServerXMLHTTP.6.0)
ActiveXObject("ADODB.Stream")

This particular malware uses the functions in table 2-1 to create files and run the code. In addition, it copies the normal wscript.exe file into a randomly-named file, and drops it into its own folder and runs it. Then, the malware modifies registry values and marks the files and folder as hidden.

The malware also attempts to connect to one of the normal URLs listed on table 2-2 to check whether the infected PC is

internet capable. The presence of code that tries to randomly access the C&C server periodically has also been found.

Table 2-2 | Network connection information

Normal URLs
www.microsoft.com
www.google.com
www.bing.com
C&C Servers
bel*****dn.com
urchin******etry.com
95.153.**.**
95.153.**.**

In addition, a command is issued to shut down any of the processes listed in table 2-3 if and when any of them are executed.

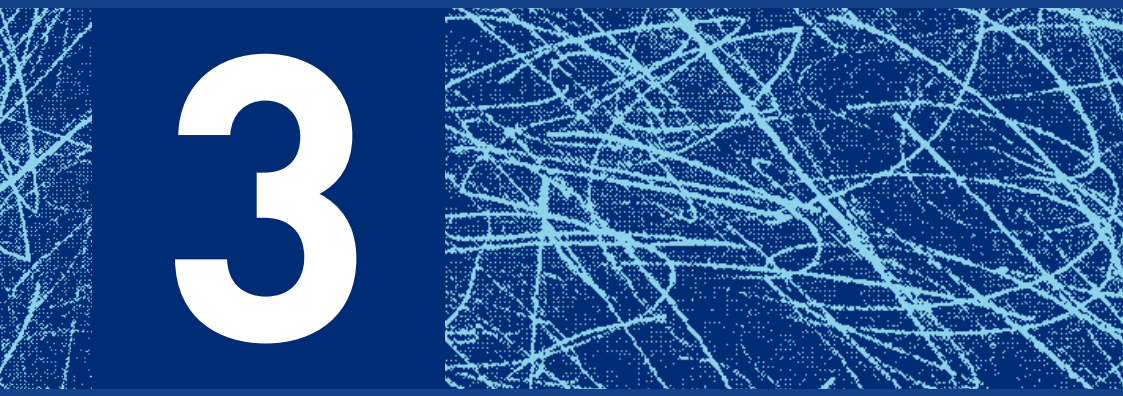
Table 2-3 | List of processes that targeted for shutdown

Command
%comspec% /c shutdown /p /f
Processes Targeted for Shutdown
regedit, windows-kb, mrt, rstrui, msconfig, procexp, avast, avg, mse, ptinstall, sdasetup, issetup, fs20, mbam, housecall, hijackthis, rubotted, autoruns, avenger, filemon, gmer, hotfix, klwk, mbsa, procmon, regmon, sysclean, tcpview, unlocker, wireshark, fiddler, resmon, perfmon, msss, cleaner, otl, roguekiller, fss, zoek, emergencykit, dds, ccsetup, vbsvbe, combofix, frst, mcshield, zphdiag

Users should take caution in using USB drives or other portable storage devices, which have been known to be a vector for an infection from this type of AutoRun malware.

The relevant alias identified by V3 products, AhnLab's anti-virus program, is as below:

<Alias identified by V3 products>
JS/Downloader (2016.04.30.00)



3

IN-DEPTH ANALYSIS

TeslaCrypt Decryption Tool

IN-DEPTH ANALYSIS

TeslaCrypt Decryption Tool

The recent rapid proliferation of ransomware is creating havoc across the world. There is generally no way to restore files that have been encrypted by a ransomware. Recovering the files taken hostage by ransomware would require a decryption key, which would be stored, out of reach, in the attacker's server. The problem is compounded by the fact that giving in to the attacker's demands and handing over the ransom is no guarantee that the files will be restored.

However, the creators of TeslaCrypt, a notorious ransomware, shut down their operation and released the master decoding key. Subsequently, BloodDolly, a TeslaCrypt expert, created and released a tool that uses the key to enable the recovery of files encrypted by TeslaCrypt 3.0 and 4.0

TeslaDecoder can be used to recover files if, in the case of TeslaCrypt 3.0, the files extensions are .xxx, .ttt, .micro or .mp3, and for TeslaCrypt 4.0, if the extension of the encrypted files are identical to the original files' extensions.

Unpacking TeslaDecoder produces the files as shown in Figure 3-1.

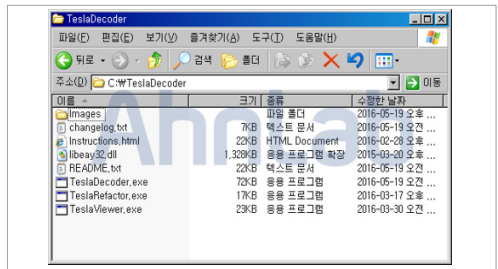


Figure 3-1 | Uncompressing TeslaDecoder

Executing TeslaDecoder.exe to restore encrypted files displays the window shown in Figure 3-2. Click on the "Set key" button to select the file extension that had been altered by TeslaCrypt. For TeslaCrypt 4.0, select <as original>.

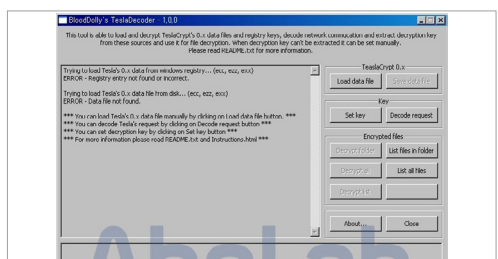


Figure 3-2 | Running TeslaDecoder

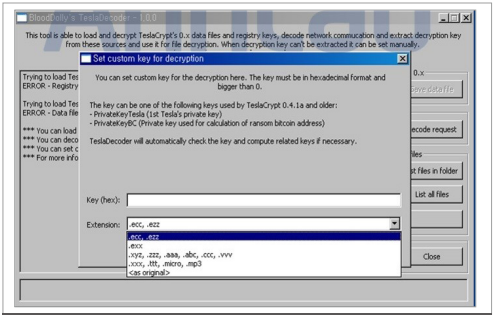


Figure 3-3 | Popup after clicking "Set key"

Figure 3-4 | Popup message on creating backups

A master decryption key is automatically set when the user selects the file extension. The commands below "Encrypted files" can be used to select the files to be decrypted (Decrypt folder, Decrypt all).

When the selection of the files to be restored is complete, the popup message shown in Figure 3-4 is displayed. The message advises the user to back up the encrypted files just to be sure. Clicking "No" restores the files without deleting the encrypted files. In the case of TeslaCrypt 4.0, the encrypted files were observed being backed up and given the file extension *.TeslaBackup.

A test confirmed that files infected by TeslaCrypt 3.0 and 4.0 were all restored to their normal states.

AhnLab also provides TeslaCrypt Decryption Tool via its website for free. The TeslaCrypt decryption tool, however, is just a single ray of hope in the otherwise vicious onslaught of ransomware, and other ransomware continue to cause destruction across the internet. Unlike TeslaCrypt, no recovery methods are known yet for the vast majority of ransomware. Prevention is thus the key in protecting a system and critical data from a ransomware infection, and backups of important data should be made on a regular basis.

AhnLab

ASEC REPORT

VOL.77
May, 2016

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