Security Trend



Ahnlab

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 | 01 Malware Statistics02 Web Security Statistics03 Mobile Malware Statistics | 4 6 7 |
|-----------------------------|---|-------------|
| 2 SECURITY ISSUE | Js/AutoRun Malware Continues to Surface | 10 |
| 3 | TeslaCrypt Decryption Tool | 13 |

IN-DEPTH ANALYSIS



- **01** Malware Statistics
- 02 Web Security Statistics
- **03** Mobile Malware 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.



* "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%).



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 M | alware 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 |
| | | |

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.



* "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.

03

Mobile Malware Statistics

In May 2016, 208,702 mobile malware were detected as shown in Figure 1-4.



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 M | obile 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 |





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.



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.**.** |
| |

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.



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)

Ahnlab





IN-DEPTH ANALYSIS

TeslaCrypt Decryption Tool

ASEC REPORT 77 | Security Trend

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.

| Big(E) B2(E) B2(V) B24(2) E=20(2) SEG(2) SEG(2) Q File P P P P P P Q C:WTestalecoder P P P P P Difference File P P P P P Changeig M M2 E N P P P Indrageig M M2 E N P P P P Indrageig M M2 E N N P P P P P P Instructions.html 20K H1ML Document 20K-06-19 & 2t N N P | 🚞 TeslaDecoder | | | |
|---|-------------------------|--------------------------------------|----------------|--|
| 주 ≾(0) C:WTeslaDecoder Images 37 87 4 282 by 38 018 501 5015 52. 016 5015 52. 016 0 hangelog bt 7/80 542 2016 505-19 52. 016 502. 016 5015 52. 016 5015 52. 016 5015 52. 016 5015 52. 016 5015 52. 016 5015 52. 016 5019 52. 016 5019<52. 016 5019 52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. 016 5019<52. <t< th=""><th>파일(E) 편집(E) 보기(⊻) 클</th><th>즐겨찾기(<u>A</u>) 도구(<u>T</u>) 도움말(</th><th>(<u>H</u>) 🥂</th><th></th></t<> | 파일(E) 편집(E) 보기(⊻) 클 | 즐겨찾기(<u>A</u>) 도구(<u>T</u>) 도움말(| (<u>H</u>) 🥂 | |
| 이름 크기 호류 수정한 남자 □Images 마일 톱더 2016-05-19 오픈 □ changelog brt 768 역소트 문서 2016-05-19 오픈 □ Instructions. Nml 2016 9.27 ○ Instructions. Nml 2016 9.27 ○ Instructions. Nml 2016 9.27 ○ Instructions. Nml 2016 9.26 ○ Instructions. Nml 2016 9.26 ○ Instructions. Nml 2016 9.27 ○ Instructions. Nml 2016 9.26 ○ Instructions. Nml 2016 9.26 ○ Instructions. Nml 2016 9.27 ○ Instructions. Nml 2016 9.27 ○ TestaBecoder.exe 7045 9.88 프고 ID ○ TestaBecoder.exe 7045 9.88 프고 ID 2016-05-19 오르 | 🚱 뒤로 🔹 🕥 - 🏂 🔎 | 검색 😥 폴더 \mid 🍰 🎲 🕽 | × 🍤 💷 · | |
| Images IDB BIC 2016/07-19 ± 2 ± Changelog Att 768< ff 4± E 8.4 2016-07-19 ± 2 ± Instructions.intml 2265 HTML Document 2016-07-19 ± 2 ± Inbesy32.dl 1,3396 8.8 ± 2 ± 2 ± 32 2016-08-19 ± 2 ± Inbesy32.dl 1,3396 8.8 ± 2 ± 2 ± 42 2016-07-19 ± 2 ± Testalbecoder.eve 7265 8.8 ± 2 ± 2 ± 2016-07-19 ± 2 ± Testalbecoder.eve 7265 8.8 ± 2 ± 2 ± 2016-07-19 ± 2 ± | 주소(D) 🗁 C:₩TeslaDecoder | | 💌 🄁 이동 | |
| Changelog tot 7/65 택스트 문서 2016-07-19 오픈 @ Instructions.html 22/65 HTML Document 2016-02-26 오픈 @ IbeayQLdI 1.330K B8 응을 프로그램 참2 2016-07-19 오픈 2 @ IbeayQLdI 22/65 북스트 문서 2016-07-19 오픈 @ IseayCub 22/65 북스트 문서 2016-07-19 오픈 @ IselaFelarton.exe 7/68 응용 프로그램 2016-07-19 오픈 | 이름 ^ | | | |
| e Instructions Mml 22KB HTML Document 2016-17-23 오후 ④ bbasy2 dil 1.339KB 응을 프로그램 확장 2015-09-00 오후 ③ READIAE, bot 22KB 역소트 문서 2016-05-13 오간 □ TestalBecode, exe 17KB 응용 프로그램 2016-05-15 오간 □ TestalBecode, exe 17KB 응용 프로그램 2016-07-15 오후 | | | | |
| ● libeay32.dl 1,338KB 응용 프로그램 확당 2015-03-20 오후 □ READIME.txt 22KB 텍스트 토서 2016-05-19 오갼 □ TeslaDecoder.txe 72KB 용용 프로그램 2016-05-19 오갼 □ TeslaDecoder.txe 17KB 용용 프로그램 2016-07-19 오갼 | | | | |
| ● FEADME.txt 22KB 목스트 문서 2016-05-19 오건 ■ TesiaBecoder.exe 7XB 용을 프로그램 2016-05-19 오건 ■ TesiaRefactor.exe 17XB 용를 프로그램 2016-05-19 오건 | | | | |
| TeslaDecoder.exe 72KB 응용 프로그램 2016-05-19 오전 ■ TeslaRefactor,exe 17KB 응용 프로그램 2016-03-17 오후 | | | | |
| TeslaRefactor,exe 17KB 응용 프로그램 2016-03-17 오후 | | | | |
| TestaViewer,exe 23KB 응용 프로그램 2016-03-30 오걘 | | | | |
| | TeslaViewer, exe | 23KB 응용 프로그램 | 2016-03-30 오겐 | |
| | | | | |
| | | | | |
| | | | | |
| - igure 3-1 Uncompressing TeslaDecoder | igure 3-1 Uncompr | essing TeslaDec | oder | |

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>.



| | Set custom key for decryption | |
|---|--|-----------------------------|
| Trying to load Tes ERROR - Registry Trying to load Tes ERROR - Data file **** You can load **** You can load **** You can set c **** For more info | The king on the new of the following laws used by TeslaCryst D. 4.1a and older: - Phonetarty relation (Teslar Syntame Juny) - Phonetarty relation (Teslar Syntame Juny) - TeslaDecoder will automatically check the key and compute related keys if necesary. Relationships (Teslar Syntame Juny) Relationships (Teslar Syntame Juny) Relationship | re data file ode request |
| | Extension: ecceccc eccecc eccecc eccecc eccecc eccecc ecc. | Close |

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.

| MU2LU # | * |
|--|--|
| P20130519_192207487_02B548ED-5C68+4AEE-8896-CE4ED196DEEE,JPG | 1,566KB JPEG 0[D[X] 2016-05- |
| P20130519_192537429_3AB6AA75-8C08-4F2A-8692-6BCDA305811D, JPG | 1,591KB JPEG 01D1X1 2016-05- 1,576KB JPEG 01D1X1 2016-05- |
| P20130519_193221403_CA921DBF-67EE-4364-B6DB-48A1AA1D463B,JPG P20130519_194232626_6866F81C-FCC1-460A-98E8-A2C183AA73EL.JPG | 2 319KB JPEG 0101X1 2016-05- |
| MG_3923.JPG. TeslaBackup | 1.957KB TESLABACKUP 2016-05- |
| MG_3924,JPG, TeslaBackup | 2,008KB TESLABACKUP 2016-05- |
| MG_3926, JPG, TeslaBackup | 2,082KB TESLABACKUP 2016-05- |
| MG_3928, JPG, TeslaBackup | 2,297KB TESLABACKUP 2016-05- |

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.



ASEC REPORT VOL.77 May, 2016

Contributors Editor

Design

ASEC Researchers Content Creatives Team Design Team

Publisher Website Email

AhnLab, Inc. www.ahnlab.com global.info@ahnlab.com

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.