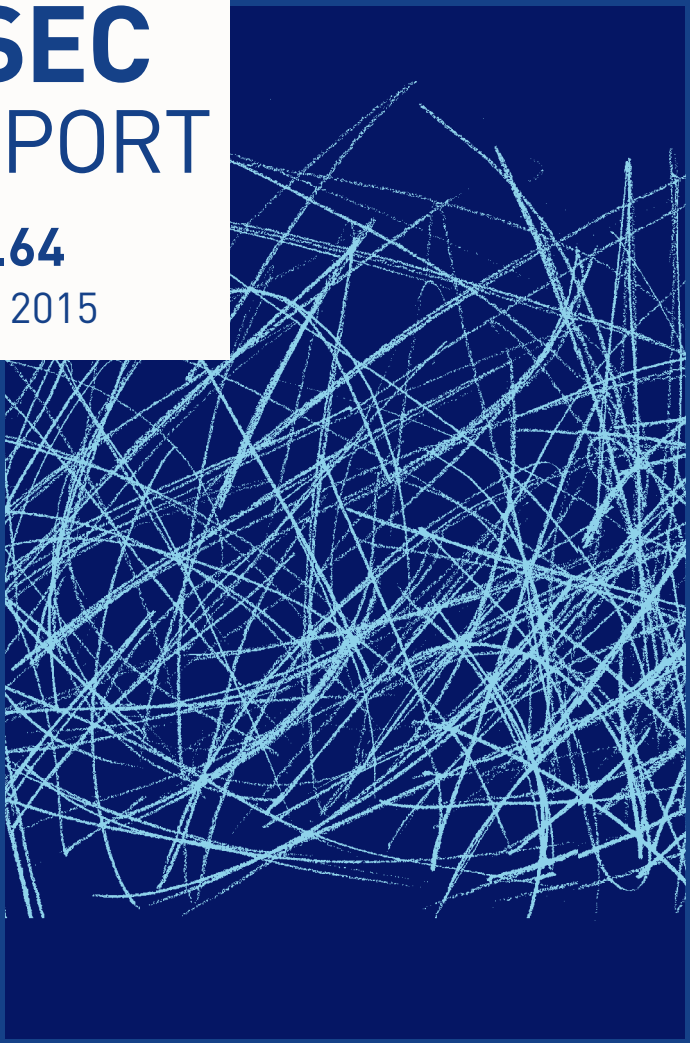
Security Trend

ASEC REPORT

VOL.64

April, 2015



AhnLab

ASEC REPORT

VOL.64 April, 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 APRIL 2015

Table of Contents

1

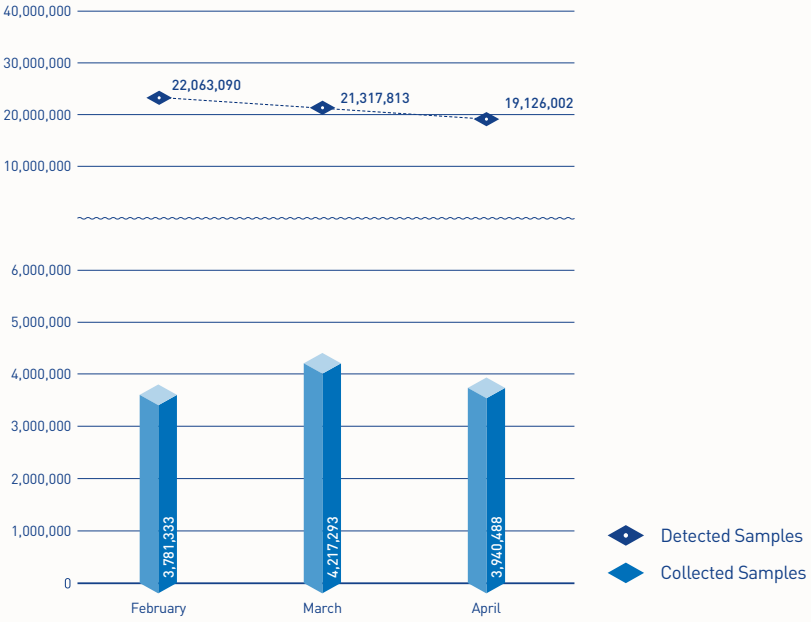
SECURITY STATISTICS

SECURITY STATISTICS

01

Malware Statistics

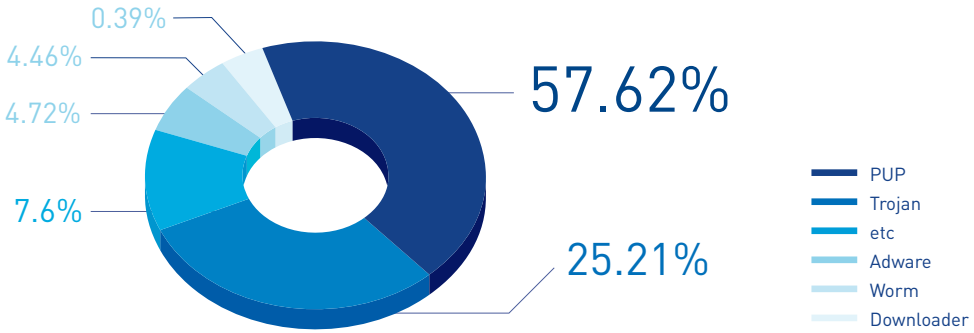
According to the ASEC (AhnLab Security Emergency Response Center), 19,126,002 malware were detected in April 2015. The number of detected malware decreased by 2,191,811 from 21,317,813 detected in the previous month as shown in Figure 1-1. A total of 394,488 malware samples were collected in April.



[Figure 1-1] Malware Trend

In Figure 1-1, "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 April 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 57.62% of the total. It was followed by Trojan (25.21%) and Adware (4.72%).



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

Table 1-1 shows the Top 10 malware threats in April categorized by alias. PUP/Win32.BrowseFox was the most frequently detected malware (1,865,187), followed by PUP/Win32.MywebSearch (1,809,795).

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

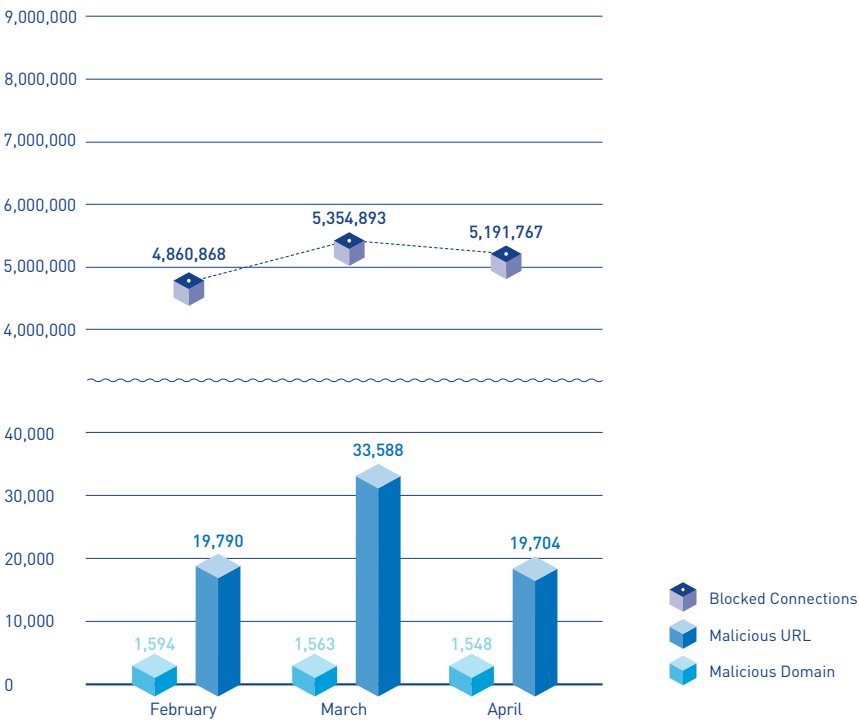
Rank	Alias from AhnLab	No. of detections
1	PUP/Win32.BrowseFox	1,865,187
2	PUP/Win32.MyWebSearch	1,809,795
3	PUP/Win32.MicroLab	1,482,437
4	PUP/Win32.Enumerate	834,002
5	PUP/Win32.Helper	774,611
6	PUP/Win32.CrossRider	435,549
7	PUP/Win32.SubShop	403,861
8	PUP/Win32.InClient	401,272
9	Trojan/Win32.Gen	353,537
10	PUP/Win32.Generic	352,268

SECURITY STATISTICS

02

Web Security Statistics

In April 2015, a total of 1548 domains and 1,9704 URLs were comprised and used to distribute malware. In addition, 5,191,767 malicious domains and URLs were blocked. This figure is the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers. Finding a large number of distributing malware via websites indicates that internet users need to be more cautious when accessing websites.



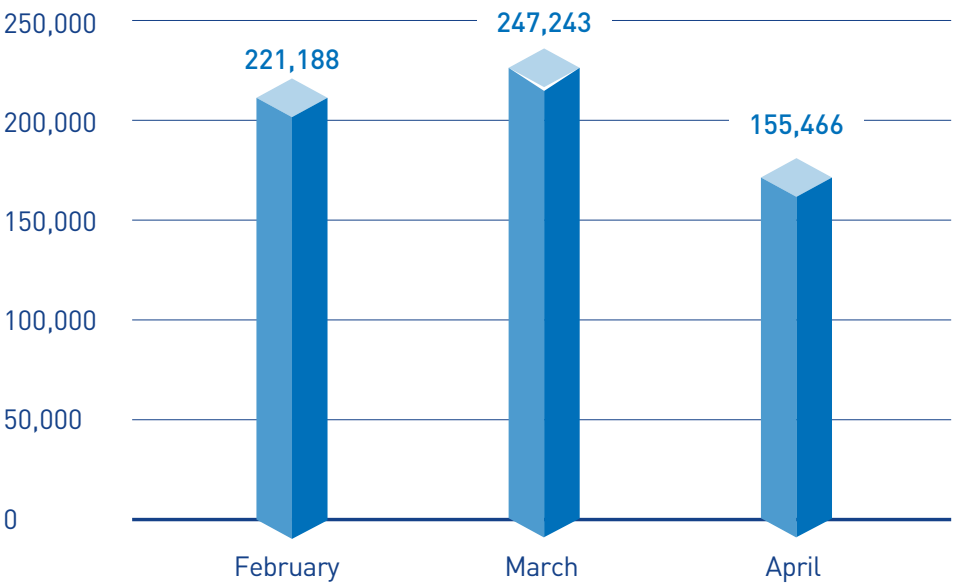
[Figure 1-3] Blocked Malicious Domains/URLs in April 2015

SECURITY STATISTICS

03

Mobile Malware Statistics

155,466 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 April 2015. Android-PUP/SmsReg was the most distributed malware with 66,134 of the total.

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

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SMSReg	66,134
2	Android-PUP/Dowgin	11,303
3	Android-Trojan/FakeInst	10,701
4	Android-PUP/Noico	10,127
5	Android-PUP/Airpush	6,136
6	Android-Trojan/SmsSpy	3,916
7	Android-Trojan/Opfake	3,352
8	Android-Trojan/SmsSend	2,983
9	Android-PUP/Chepa	2,318
10	Android-PUP/Wapsx	2,193

2

SECURITY ISSUE

Email-borne "Upatre" Malware Continues to Rage

SECURITY ISSUE

Email-borne "Upatre" Malware Continues to Rage

Malware infection spread via spammed email messages is becoming a worldwide problem. In a typical malware infection through email, the user is tricked into clicking a link in the email and downloading the malware, or running an attachment disguised as a document file which then infects the user's system. Starting from late 2014, large quantities of these types of spammed messages embedded with variants of the "Upatre" malware are being widely distributed, and users need to remain vigilant.

Different types of Upatre malware have slightly different characteristics depending on the variant, but they have the following processes in common.

- Create a self-replicate when the attachment (initial file) of the spammed email is run.
- Attempt to access a C&C server, download additional malware
- Display a normal PDF file to disguise itself
- Make continuous communication with C&C server, steals information

A sample that was recently received by AhnLab was an Upatre variant bearing the subject "invoice" on the email. The attachment contained the executable file "invoice1212.exe", disguised with a PDF icon.

Figure 2-37 | Email dropper and resultant installed files (invoice121.exe and others shown)

Running the malicious file "invoice1212.exe" attached to the email creates additional files as shown in [Table 2-3], and the file proceeds to attempt a connection with the C&C server and downloads additional malware.

Table 2-3 | List of created files
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩cwutokat.exe (duplicate)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temporary Internet Files₩Content.IE5₩BR95JRB5₩doc101.pdf (encoded file)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩temp25.pdf (normal PDF)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩bhihxxs96.exe (decoder)

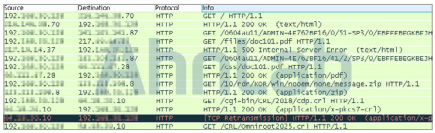


Figure 2-38 | C&C Server connection information

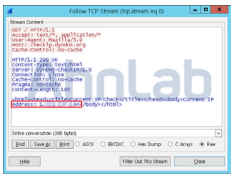


Figure 2-39 | IP address check

Following the infection and packet information check, the malware accesses the IP address check site "checkup.dyndns.org" to determine the infected system's IP address.

Next, the malware attempts to download the encoded file "doc101.pdf" from the download path shown in [Table 2-4].

Table 2-4 | Download path
Electro*****.ro/*****/doc101.pdf (21*.**.**.37:80) electro********.com.**/***/doc101.pdf (66.***.**.28:80)

Figure 2-40 | Normal PDF file displayed

After attempting the download, a normal PDF is displayed to hide the malware infection from the user.

Precise information on the attack that follows the attempted access of the C&C server has not been verified, but generally the malware acts as an "infostealer" that hijacks financial information. This type of spammed message uses terms such as "doc", "document", "invoice", "ticket", "photo" etc. to deceive the user into clicking the message, and users should exercise extra caution when encountering such a message.

New variants of Upatre malware are being constantly discovered. Most enterprises employ a spam blocker solution to protect the system from being harmed by email spam with hidden malware.

The Ahnlab range of V3 products detects the following malware aliases:

<Aliases Detected by V3 Products>

Trojan/Win32.Upatre (2015.04.08.01)

Win-Trojan/Agent.516096.EG (2015.04.07.03)

BinImage/Encdata (2015.04.07.05)

3

IN-DEPTH ANALYSIS

Six Notorious Ransomware

SECURITY ISSUE

Six Notorious Ransomware

Ransomware, a type of malware that began appearing several years ago, is becoming increasingly infamous around the world. CryptoLocker, a type of ransomware, has even been written and distributed in multiple languages other than English, raising concerns about the evolution of targeted and localized ransomware.

This report classifies several recent and high-profile ransomware, examining their characteristics and attack patterns. The classification and ranking is based on the amount of attention generated in Korea and abroad as well as the number of diagnosis made by AhnLab, covering the period between October 2014 and March 2015.

1. Classification of major recent ransomware

Six ransomware that are recently being diagnosed in increasing numbers by V3, AhnLab's anti-virus software suite, as well as receiving increasing attention and discussion by the media and user groups are listed as below in [Table 3-1]. These can be grouped into "Nabucur" ransomware, and other variants. Nabucur alters normal files by inserting malicious code into encoded original files; V3 can restore these files into their original states. However, the other types of ransomware uses encryption methods such as RSA and AES, and requires the decryption key in order to restore the original files. A closer look at their operational methods reveal considerable similarities between the two types.

Table 3-1 | Classification of major ransomware

	Types of Ransomware	Data
1	NsbLocker / Nabucur	4DDE0233CD956FAA19FF21B3FB73FBBD ED42954A5824A5DD1E579168480191B2 770D3BC32F7ACA8F94DD22209532A352 19840868F8D20089BA4CE289F48A6A09 DC5BAD327EF50D2594F423A1DF7A6C03 FF6CAFE7597BD6FF1521A1A1F817D9BF

2	CtbLocker / Critroni	DEFB9614AFA1DA0D0057C80AACBCA7F0 D0C3CE7B8B99D4B4278CE3E3CECE33E9 E89F09FDDED777CEBA6412D55CE9D3BC F420BDEB156FDB2F874A1E5D51E9D65F FEC68D340ED13292701404E438059FB7 14C0558C757C93465ECCBBD77D58BBF3
3	CryptoLocker	0204332754DA5975B6947294B2D64C92 6FE47DC2BDB86B0FC28017FC6A67B1F9 0E1543914E129FF069D1079695115FE9 0DF492989EEA14562EE2E8C880EEDDB6 419ECEC2051479609ADED0C173619DF8 04FB36199787F2E3E2135611A38321EB
4	CryptoWall / CryptoDefense	31C2D25D7D0D0A175D4E59D0B3B2EC94 0650C9045814C652C2889D291F85C3AE B6C7943C056ACE5911B95D36FF06E0E4 A9927372ADB1BBAB4D9FEDA4973B99BB 73A9AB2EA9EC4EAF45BCE88AFC7EE87E
5	TorrentLocker	7D1D5E27C1C0CB4ABCC56FA5A4A16744 253491AD824E156971C957CD15254844 4A96F22E4FFDBCF271FF4EB70B1320ED 86296FB3DDD46431DDFE8A48D6FB165C 6694617DAB8CD78630AA0A3E002E5197 71C066D831A5749685747B33CB9588A8
6	TeslaCrypt	01ADE9C90D49AF3204C55D201B466C1B

Each ransomware's characteristics can be tabulated as show in [Table 3-2]. The biggest feature, as noted earlier, is that Nabucur does not use encryption and its targets include ".exe" files. A feature they share is that all ransomware directs the user to make a payment using Bitcoins.

Table 3-2 | Overview of major ransomware

	Data	Protocol	Encryption Method	Main Target Files	Execution	Payment Method	Ransom Amount Demanded
1	NsbLocker / Nabucur	TCP	Polymorphic	Doc/EXE/image files /media files	Polymorphic	Bitcoin	250 USD
2	CtbLocker / Critroni	HTTPS/ TOR	AES, ECDH	Doc / image files	OpenSSL	Bitcoin	0.5 USD
3	CtbLocker	HTTP	AES, RSA	Doc / image files	MS Crypto API	Bitcoin	300 USD
4	CryptoWall / Crypto Defense	HTTP/ TOR	RSA	Doc / image files	MS Crypto API	Bitcoin	500~1000 USD
5	Torrent Locker	HTTPS	AES	Doc / image files	OpenSSL	Bitcoin	0.8 BTC
6	TeslaCrypt	HTTPS/ TOR	AES, ECC	Games/ Doc/image files	OpenSSL	Bitcoin, Paypal	500~1000 USD

A timeline of the appearance of these ransomware can be presented as below in [Figure 3-1]. The recently-discovered "TesaCrypt" is notable for including in its targets not just documents or image files but game-related files. Outbreaks of email-distributed "CtbLocker" variants have also been on the rise recently.

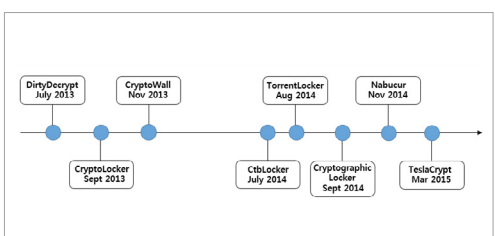


Figure 3-1 | Timeline of major ransomware outbreaks

2. Analysis of How Major Ransomware Work

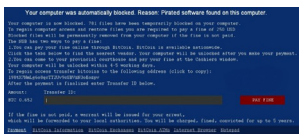
1) NsbLocker / Nabucur

An overview of Nabucur has been previously presented in the February 11th, 2015 AhnLab blog posting (asec.ahnlab.com/1025) under "NSB: National Security Bureau". An infection by this malware places under attack images files (*.bmp, *.gif, *.jpg, *.png), document files (*.doc, *.ppt, *.xls), media files (*.mp3, *.wma) and even executable files (*.exe) and compressed files (*.rar, *.zip). The original files are encoded and backed up, and then transformed into executable files. These original files are not altered using "AES", "RSA" or other similar encryption methods and thus can be restored by a vaccine program. The altered executables contain not only the backed-up original file but the Nabucur malware code as well, essentially making it another copy of Nabucur malicious code that can further infect other files.

Running a file infected by Nabucur will create two additional executable files in the '%User%' and '%ALLUser% subfolders, which then run as threads and attempt to connect to the C&C server and infect files in the system with particular extensions. Finally, a message demanding monetary payment is displayed on the infected system.

Table 3-3 | How NsbLocker / Nabucur works

Process	Log
Create files	**%User%₩<random folder name1>₩<random file name1>.exe** **%ALLUser%₩<random folder name2>₩<random file name2>.exe** ⇒ The file that acts as the actual ransomware **%TEMP%₩< random file name 3>.bat** ⇒ 4-byte key needed to decode the original file; deleted after creating the original file **%TEMP%₩<original file name>.exe** ⇒ decoded original file
Add to registry	**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩< random file name 1>.exe** → %User%₩< random folder name 1>₩< random file name 1>.exe **HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩< random file name 2>.exe** → %ALLUser%₩< random folder name 2>₩< random file name 2>.exe ⇒ Add to autorun **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Advanced\Hidden** → "0x2" **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Advanced₩HideFileExt** → "0x1" ⇒ Change folder and extension view options **HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩policies₩system₩EnableLUA** → "0x0" ⇒ Change Windows user account settings
Connect to network	200.87.164.69:9999(or port 666) 200.119.204.12:9999(or port 666) 190.186.45.170:9999(or port 666)

Target files	.bmp, .cer, .crt, .doc, .exe, .gif, .jpg, .mdb, .mp3, .mpg, .p12, .p7b, .pdf, .pem, .pfx, .png, .ppt, .psd, .rar, .wma, .xls, .zip
File status	".exe" is tacked onto the end of the original file extension. However, no additional extension is added to executable (.exe.) files. Examples: test.jpg.exe, compress.zip.exe, etc
Display output	
Notes	A <random 4-letter name.ico> is created using the icon information of the infection target file. Then, a <random 4-letter name.exe> file is created that contains the "original file's icon + encoded original file + malicious code". This file is copied as "original file name +.exe.", after which the original file is deleted.

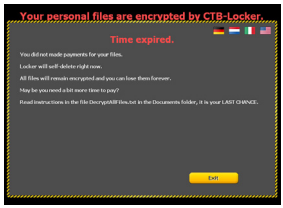
2) CtbLocker / Critrioni

First spotted around July 2014, CtbLocker is also known by the name "Critrioni" and is created and executed by a downloader attached to spammed email. The downloader, which rides on the message as an attachment, is compressed as a ".zip" or "cab" file and distributed. The decompressed file has a ".scr" extension. When run, the file creates and opens a normal ".rtf" file in the "%TEMP%" folder, camouflaging itself as a document file yet downloading malicious files in the background with the user's knowledge.

The downloaded file is the malicious ransomware that targets not only Office document files but images, source files and a variety of other file types for encryption; when this process is completed, a message about CtbLocker and a demand for a payment in Bitcoins is displayed on the screen.

Table 3-4 | How CtLocker / Critrioni works

Process	Log
Create files	**%temp%₩temp_cab_<random number>.cab** **%temp%₩<downloader>.rtf** ⇒ A normal document file for deceiving the user **%temp%₩<random name>.exe** ⇒ Runs as actual ransomware
Add to registry	None
Connect to network	https://breteau-photographe.com/tmp/pack.tar.gz https://voigt-its.de/fit/pack.tar.gz https://maisondessources.com/assets/pack.tar.gz https://jbmsystem.fr/jb/pack.tar.gz https://pleiade.asso.fr/pivigotest/pack.tar.gz https://scolapedia.org/histoiredesarts/pack.tar.gz ⇒ File download URLs
Target files	.pwm, .kwm, .txt, .cer, .crt, .der, .pem, .doc, .cpp, .c, .php, .js, .cs, .pas, .bas, .pl, .py, .docx, .rtf, .docm, .xls, .xlsx, .safe, .groups, .xlk, .xlsb, .xlsm, .mdb, .mdf, .dbf, .sql, .md, .dd, .dds, .jpe, .jpg, .jpeg, .cr2, .raw, .rw2, .rwl, .dwg, .dxf, .dxg, .psd, .3fr, .accdb, .ai, .arw, .bay, .blend, .cdr, .crw, .dcr, .dng, .eps, .erf, .indd, .kdc, .mef, .mrw, .nef, .nrw, .odb, .odm, .odp, .ods, .odt, .orf, .p12, .p7b, .p7c, .pdd, .pdf, .pef, .pfx, .ppt, .pptm, .pptx, .pst, .ptx, .r3d, .raf, .srf, .srw, .wb2, .vsd, .wpd, .wps, .7z, .zip, .rar, .dbx, .gdb, .bsdr, .bsdu, .bdcr, .bdcu, .bpdr, .bpdu, .ims, .bds, .bdd, .bdp, .gsf, .gsd, .iss, .arp, .rik, .gdb, .fdb, .abu, .config, .rgx

File status	A random string of seven letters is attached to the extension of the encrypted files, as shown below. Examples: test.jpg.[7 random letters], compress.zip.[7 random letters], etc.
Display output	
Notes	A ransom note is displayed threatening to prevent data recovery unless payment is made within 96 hours. If the ransom period expires or if the computer clock is manually adjusted, the following "Time expired" message is displayed. 

3) CryptoLocker

Initially discovered in September 2013, CryptoLocker is distributed as an attachment on a spammed email similar to CtbLocker, or through "Gameover Zeus" P2P botnet malware, to encrypt documents and image files. The malware demands a MoneyPak payment or Bitcoins to restore the files.

This ransomware adds itself to the registry to autorun; note that the registry entry is labeled as "CryptoLocker". The downloader connects to its C&C server and downloads a public key, then encrypts the system's files. The C&C servers are currently offline, preventing the ransomware from functioning.

On August 2014, global security experts launched "Operation Tovar" that brought down the C&C server of the developer of this malware and extracted a number of decryption keys that were stored on the server. Currently a large portion of encrypted files can be restored to their previous states. Approximately 500,000 systems around the world are estimated to have been infected by CryptoLocker leading up to the abovementioned date.

Table 3-5 | How CryptoLocker works

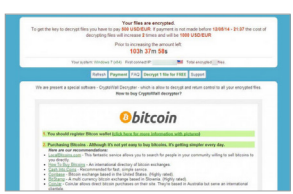
Process	Log
Files created	**%AppData%₩<random file name>.exe** ⇒ [Windows XP] **%AppData%₩Loca\<random file name>.exe** ⇒ [Windows 7] ⇒ self-copy
Add to registry	**HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩CryptoLocker** → %AppData%₩<random file name>.exe **HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce₩*CryptoLocker** → %AppData%₩<random file name>.exe ⇒ Add to autorun

Connect to network	http://iryymjeallxat.net http://cvlagtrfprixtf.com http://ppsryujrxvap.ru http://vtnwqvqdlunbk.biz http://odnhaentyltc.info http://iubeloxoublp.co.uk http://alegqseessuop.org ⇒ C&C server URLs
Target files	.odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlsb, .xlk, .ppt, .pptx, .pptm, .mdb, .accdb, .pst, .dwg, .dxf, .dxg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .eps, .indd, .cdr, .jpg, .dng, .3fr, .arw, .srf, .sr2, .bay, .crw, .cr2, .dcr, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf, .raf, .raw, .rwl, .rw2, .r3d, .ptx, .pef, .srw, .x3f, .der, .cer, .crt, .pem, .pfx,.p12, .p7b, .p7c
File status	Activates after successfully communicating with C&C server
Display output	
Notes	Once successfully connected to the C&C server, the malware sends using POST data that includes information on the executable file and the affected system to the /home/ directory of the server. 

4) CryptoWall / CryptoDefense

CryptoWall's process flow is similar to that of CryptoLocker outlined above. Both work by creating subprocesses and injecting PE images, activating the ransomware component by receiving the public key from the C&C server.

Table 3-6 | How CryptoWall works

Process	Log
Files created	**C:₩<random name>₩<random name>.exe** **%AppData%₩<random name>.exe** **%Startup%₩<random name>.exe** ⇒ self-copy
Add to registry	**HKCU₩Software₩Microsoft₩Windows₩ CurrentVersion₩Run₩ <random name-1>** → C:₩<random name>₩<random name>.exe **HKCU₩Software₩Microsoft₩Windows₩ CurrentVersion₩RunOnce₩*<random name-1>** → C:₩<random name>₩<random name>.exe **HKCU₩Software₩Microsoft₩Windows₩ CurrentVersion₩Run₩ <random name>** → %AppData%₩<random name>.exe **HKCU₩Software₩Microsoft₩Windows₩ CurrentVersion₩RunOnce₩*CryptoLocker** → %AppData%₩<random name>.exe ⇒ Add to autorun <random name-1> is the 7-letter file name minus a single character, making a six-letter file name ⇒ random file name
Connect to network	http://likeyoudominicana.com http://maskaradshowdominicana.com http://dominikanabestplace.com http://nofbiatdominicana.com http://dominicanajoker.com ⇒ C&C server URLs
Target files	Document files including *.doc, *.ppt, *.rtf; image files
File status	Activates after successfully communicating with C&C server
Display output	

Notes	When CryptoWall infects the system after receiving the key values from the C&C server, the following three files are installed in each folder that contains instructions for file recovery. DECRYPT_INSTRUCTION.HTML DECRYPT_INSTRUCTION.TXT DECRYPT_INSTRUCTION.URL

5) TorrentLocker

TorrentLocker also works in a similar fashion as CryptoLocker and CrytoWall examined above, and the code execution process is quite similar as well. The nomenclature "TorrentLocker" comes from the fact that it writes a list of encrypted files to the registry "HKCU\Software\Bit Torrent Application\ configuration".

Table 3-7 | How TorrentLocker works

Process	Log
Create files	**%WINDOWS%₩<random name>.exe** ⇒ self-copy
Add to registry	**HKCU₩Software₩Microsoft₩Windows₩ CurrentVersion₩Run₩ <random name>** → %WINDOWS%₩<random name>.exe ⇒ Add to autorun
Connect to network	http://octoberpics.ru/topic.php http://it-newsblog.ru/topic.php http://tweeterplanet.ru/topic.php http://deadwalk32.ru/topic.php ⇒ C&C server URL
Target files	Document files including *.doc, *.ppt, *.rtf; image files
File status	Activates after successfully communicating with C&C server

Display output	
Notes	Once the ransomware function is activated after receiving the key from the C&C server, target files are encrypted and stored in a folder named "%AppData%\<16 random lower-case letter name".

6) TeslaCrypt

TeslaCrypt is a ransomware variant that attacks game functions and save data, installed onto the PCs of regular users by exploiting weaknesses in flash players that use tags instead of iFrame. The structure itself is similar to CryptoLocker, the difference being that TeslaCrypt attacks not only document files but game-related files (profiles, save files, data, maps, mods, etc.).

Unlike CryptoLocker, TeslaCrypt makes a network connection to transmit the Bitcoin address of the user's PC. A "log.html" file that contains the list of encrypted files and "key.dat" that is used for decoding are stored in the %AppData% folder. A "HELP_RESTORE_FILES.txt" file is created on the desktop containing instructions on making a Bitcoin payment in order to decrypt the affected files.

Table 3-8 | How TeslaCrypt Works

Process	Log
Create files	**%AppData%₩Roaming₩<random name>.exe** ⇒ self-copy **%AppData%₩Roaming₩log.html** ⇒ encrypted file list **%AppData%₩Roaming₩key.dat** ⇒ decoding key **%Desktop%₩CryptoLocker.lnk** ⇒ shortcut file **% Desktop%₩HELP_RESTORE_FILES.txt** ⇒ instructions on how to pay the ransom to have the system restored
Add to registry	**HKCU₩Software₩Microsoft₩Windows₩ CurrentVersion₩Run₩ <random name>** → %AppData%₩Roaming₩<random name>.exe ⇒ Add to autorun
Connect to network	https://7tno4hib47vlep5o.tor2web.fi https://7tno4hib47vlep5o.tor2web.blutmagie.de
Target files	.d3dbsp, .icxs, .menu, .mpqge, .wotreplay, .pptx, .sc2save, .hvpl, .layout, .DayZProfile, .desc, .xlsb, .ibank, .hplg, .blob, .rofl, .jpeg, .xlsm, .pkpass, .hkdb, .dazip, .litemod, .mrwref, .xlsx,.sidn, .mdbackup, .arch00, .asset, .indd, .docm, .sidd, .syncdb, .vpp_pc, .forge, .dbfv, .docx, .mddata, .mcgame, .mcmeta, .rgss3a, .accdb, .itdb, .ztmp, .vfs0, .unity3d, .pptm
File status	The extra extension ".ecc" is added to the file extensions, and a "HELP_RESTORE_FILES.txt" file is created in every folder. Examples: test.jpg.ecc, compress.zip.ecc, etc
Display output	
Notes	Once the ransomware function is activated after receiving the key from the C&C server, target files are encrypted and stored in a folder named "%AppData%\<16 random lower-case letter name".

3. Conclusion

Users inevitably panic when their PC becomes disabled by a ransomware infection. If there are important files stored on the system, the user has no other choice but to pay the ransom. The problem is that there is no guarantee that the system will be restored even if the ransom is handed over. Prevention, then, is the best way to protect a system from ransomware. Suspicious files attached to emails sent from unknown or unfamiliar senders should never be clicked. Keeping a system's virus vaccine up-to-date with the latest release and making sure that the OS and all applications are kept up-to-date are important as well. We also strongly recommend backing up important files.

AhnLab

ASEC REPORT

VOL.64
April, 2015

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

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