Analysis Report 🕕 Q1 2016 Ransomware Trends



www.ahnlab.com © AhnLab, Inc. All rights reserved.

Table of Content

Introduction	3
Highlights 1: Most Rampant Ransomware in 1Q 2016	3
1. Ransom32 written in JavaScript	3
2. CryptoJoker distributed via Phishing email	4
3. LeChiffre that launches remote attacks	4
4. TeslaCrypt 3.0 that changes file extensions	5
5. 7EV3N that disables keyboard keys	5
6. HydraCrypt distributed using the Angler Exploit Kit	6
7. NanoLocker spread via spam mail disguised as a PDF file	6
8. DMA Locker that has a whitelist	7
9. UmbreCrypt that adds an identifier behind the encrypted file extensions	7
10. PadCrypt that comes with live chat feature	8
11. Locky distributed via massive spam campaign	8
12. KeRanger (Mac) that goes after Apple's OS X	9
13. Petya that overwrites the master boot record (MBR)	9
Highlights 2: Changes in Ransomware in 1Q 2016	10
1. Ransomware distribution method	10
2. File format disguises	10
3. Technical changes in ransomware	10
Highlights 3: Ransomware Forecast	11
1. Expansion through alliances	11
2. Possibility of the organized large-scale attack	11
Conclusion: Security Advisory	11

Introduction

Ever since the first ransomware, PC Cyborg Trojan (aka AIDS), was discovered in 1989, ransomware has been making appearances here and there. In the mid-2000s, GPCode ransomware emerged that used an RSA algorithm to encrypt multiple file extensions and demanded ransom for its decryption tool. However, ransomware did not really have a huge impact before the 2010s. Starting off from CryptoLocker, which was discovered in August 2013, to Locky, which has been massively distributed along with spam mail in the beginning of 2016, ransomware has gained world-wide notoriety.

This report explains notable features of ransomware discovered in the first quarter of 2016.

Highlights 1: Most Rampant Ransomware in 1Q 2016

1. Ransom32 written in JavaScript

The so-called Ransom32 is the first ransomware to be written in JavaScript. The JavaScript distributed via spam email campaign is obfuscated, and then downloads and executes ransomware. It uses Tor network, and an AES and RSA encryption algorithm.

Ranse	om32			
ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED				
All your data (photos, documents, databases, etc) have been computer. This menas that you will not be able to access you stored in our servers and the only way to receive y	n encrypted with a private and unique key generated for this ur files anymore until they are decrypted. The private key is rour key to decrypt your files is making a payment.			
The payment has to be done in Bitcoins to a unique address tha make online payments. If you don't know how to get Bitcoins, y the instructions.	It we generated for you. Bitcoins are a virtual currency to rou can click the button "How to buy Bitcoins" below and follow			
You only have 4 days to submit the payment. When the pro aprox.). Also, if you don't pay in 7 days, your unique key will be anymore.	wided time ends, the payment will increase to 1 Bitcoins (\$350 e destroyed and you won't be able to recover your files			
Payment raise	Final destruction			
3 days, 23:59:43	6 days, 23:59:43			
To recover your files and unlock your computer, you n addu	nust send 0.1 Bitcoins (\$35 aprox.) to the next Bitcoin ress:			
Check payment	How to buy Bitcoins			
A If you try to remove this payment platform, your will ne	ver be able to decrypt your files and they will be lost forever ${f \Lambda}$			

[Fig. 1] Screenshot of Ransom32

2. CryptoJoker distributed via Phishing email

CryptoJoker uses an AES 256 encryption algorithm and is distributed via phishing email. It adds ".crjoker" behind the encrypted file extension. A warning message in English and Russian is shown to the user after encryption.



3. LeChiffre that launches remote attacks

LeChiffre is French for "number" or "encryption." Unlike other malware or ransomware, the attacker searches for vulnerable systems and remotely connects to the system to launch its attack. ".LeChiffre" is added to the encrypted file extension, and the file is Base64-encoded.

Attention!
Your important files (photos, videos, documents, archives, databases, backups, etc.) which were crypted with the strongest military cipher RSA1024 and AES. No one can't help you to restore files without our decoder. Photorec, RannohDecryptor, etc repair tools are useless and can destroy your files irreversibly. If you want to restore files - send e-mail to <u>decrypt my files@gmail.com</u> with the file "_secret_code.bt" and 1-2 encrypted files less than 5 MB as *.doc *.xls *.jpg, but not database (*.900 *.001 etc). Please use public mail yahoo or gmail.
You will receive decrypted samples and our conditions how you'll get the decoder. Follow the instructions to send payment.
P.S. Remember, we are not scammers. We don't need your files. If you want, you can get a decryptor for free after 6 month. Just send a request immediately after infection. All data will be restored absolutelly. Your warranty - decrypted samples.
Secret code:

[Fig. 3] Warning dialogue of LeChiffre ransomware

4. TeslaCrypt 3.0 that changes file extensions

TeslaCrypt 3.0 shows a change in both encryption algorithm and file extension when compared to previous ransomware. It adds .xxx, .TTT, .Micro or .mp3 extensions to the end of the file name of the encrypted file.

NOT YOUR LANGUAGE? USE Google Translate
hat happened to your files?
l of your files were protected by a strong encryption with RSA
ore information about the encryption RSA can be found here: <u>https://en.wikipedia.org/wiki/RSA_(cryptosystem)</u>
hat does this mean?
is means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read em or see them, it is the same thing as losing them forever, but with our help, you can restore them.
ow did this happen?
specially for you, on our SERVER was generated the secret keypair RSA - public and private.
your files were encrypted with the public key, which has been transferred to your computer via the Internet.
crypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!
hat do I do?
as, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be ranged
you really need your data, then we suggest you do not waste valuable time searching for other solutions becausen they do not ist.
or more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page elow:
http://p57gest54celltraf743knjf.mottesapo.com/
.http://k4restportgonst34d23r.oftpony.at/Caracterian
.http://rr7mdgibihbefykhbashrg.ginnypecht.com/

[Fig. 4] Screenshot of TeslaCrypt 3.0 ransomware

5. 7EV3N that disables keyboard keys

7EV3N was distributed via spam mail disguised as information for a Valentine's Day promotional offer. The corrupted link installs the ransomware which then disables keyboard keys on the Windows system.



[Fig. 5] Screenshot of 7EV3N ransomware

6. HydraCrypt distributed using the Angler Exploit Kit

HydraCrypt is distributed using the Angler Exploit Kit. It encrypts files and adds ".hydracrypt_ID_[8 random characters]" to the file name of the encrypted file.



[Fig. 6] Screenshot of HydraCrypt ransomware

7. NanoLocker spread via spam mail disguised as a PDF file

NanoLocker infects systems by inducing victims to open a fake PDF file attached to a spam mail.



[Fig. 7] Screenshot of NanoLocker ransomware

8. DMA Locker that has a whitelist

DMA Locker adopts a whitelist method that does not encrypt some folders and file extensions designated by the attacker.



[Fig. 8] Screenshot of DMA Locker ransomware

9. UmbreCrypt that adds an identifier behind the encrypted file extensions

UmbreCrypt is distributed as an email attachment and adds "umbrecrypt_ID_[infected PC_id]" to the encrypted file. It has a whitelist of folders and file extensions that it does not target for encryption.



10. PadCrypt that comes with live chat feature

PadCrypt becomes installed and then infects systems when the victim executes the double-extension file (.pdf.scr) in the zip file attached to a spam mail. It also comes with a live chat feature in a separate window that opens when the victim clicks "Live Chat" on the bottom-left of the notification message.

	Your files and documents have been	encrypted!	
	What happened to my files? Your photos, documents, and videos on this computer haw AES-256. To get your files back you will need to purchase y within the set date, failing to pay will result in the destruction How do I obtain my key?	e been encrypted with your encryption key n of your key.	
Price will multiply on 01/01/1970	The key produced for your computer is stored on our server. To obtain the unique key for your computer, which will decrypt and recover your encrypted files, you will need to pay a fee in Bitcoin/UKash/PSC piror to the key destroy date. After that your key will be destroyed and nobody will ever be able to recover your files. Payment Method		
Time Left 00 : 00 : 00 : 00	Bitcoin (Cheapest Option) ~	0.8 BTC	
Live Chat Decrypt Help Encrypted Files		Next	

[Fig. 10] Screenshot of PadCrypt ransomware

11. Locky distributed via massive spam campaign

Locky is executed when a victim opens the document or JavaScript file attached to a spam mail. The number of attacks is increasing as it is distributed via a massive spam campaign with the notorious Dyre malware and Dridex group.



[Fig. 11] Screenshot of Locky ransomware

12. KeRanger (Mac) that goes after Apple's OS X

KeRanger runs on Apple's OS X. It adds ".encrypted" to the encrypted file. This ransomware is distributed along with Transmission, an open source Torrent client program.



13. Petya that overwrites the master boot record (MBR)

Petya is distributed as an email attachment. It overwrites the master boot record (MBR), leaving the PC in an unbootable state.



[Fig. 13] Screenshot of Petya ransomware

Highlights 2: Changes in Ransomware in 1Q 2016

1. Ransomware distribution method

CryptoLocker is distributed as an email attachment disguised as a document file and chat message on Instant Messenger. Attackers also compromise downloaded files on various web services, or exploit the vulnerabilities found in OS, applications and web servers to launch ransomware attacks. They also use malvertising that involves injecting malicious advertisements into legitimate online advertising networks or into a Torrent service that is used to share and download files.

2. File format disguises

■ .DOC and .PDF extensions and icons

Malicious files disguised as .DOC or .PDF files are still widely used today. Most computer users usually open MS Word files or .PDF files without any suspicion.

Fake screensaver file

Screen saver files are often used to distribute malware because an .scr file is executed with a mouse click, just like an .exe file.

Macros in document file

A more sophisticated way of installing malware other than disguising it as a document file is to use a normal file that contains malicious macros. When the user opens the attached document file, it will be full of unreadable characters to deceive the victim into enabling macros. The macros in documents are in obfuscated JavaScript. The JavaScript is used for external communication to download, install and execute malware.

JavaScript (.js) extension

There has been an increase in distributing compressed obfuscated JavaScript files along with document files containing malicious macros as email attachments. The attached file name contains words such as *payment*, *invoice* and *contract* to deceive users into opening the file. When the .js script is executed, it communicates externally to download, install and execute malware.

3. Technical changes in ransomware

Whitelist method

Among the latest ransomware, there have been some ransomware that have a whitelist of folders and file extensions not to encrypt. That is, the attacker whitelists paths or files not to encrypt. There is even a ransomware that uses a whitelist of Russian language computers that it will not encrypt.

Live Chat

One of the latest ransomware attacks provides a live chat function along with a menu that describes its service. It is assumed that the attackers use the live chat to threaten the victims more aggressively and to increase the psychological and financial damage. Live chats can also be used to commit more crimes. However, the live chat feature was not able to connect when security researchers at AhnLab analyzed the relevant ransomware.

Elaborate designs

Some ransomware suspiciously display irregular designs, whereas many ransomware and variants poorly mimic the existing ransomware's design with shoddy features. Ransomware are usually in the form of a simple icon or text, but recently, there have been ransomware with elaborate designs, giving the appearance of a highly reliable service. For example, Maktub ransomware redirects victims to a carefully designed webpage that uses sophisticated terms and expressions. Most victims will mistake the web page for a legitimate web service, unaware that they are being attacked.

Ransomware as a Service (RaaS)

Today, some attackers no longer directly create and distribute malware by themselves. Ransomware creators have started Ransomware as a Service (RaaS), which is a service that creates ransomware on demand for illegal customers. They also provide information on the distribution and infection status of the ransomware ordered by customers

Highlights 3: Ransomware Forecast

1. Expansion through alliances

Spammers who worked in collusion with Dyre malware creators, which ranked high amongst malware distributors from the summer of 2014 to last year, started collaborating with other ransomware creators to distribute ransomware via massive spam campaigns. In addition, ransomware creators are pursuing alliances with other groups, highlighting their file downloads and C&C server infrastructure, as well as profits made through the extortion payments of victims.

2. Possibility of the organized large-scale attack

Until recently, ransomware that first emerged in 2013 typically demanded anywhere from \$200 to \$400 USD as a ransom. Recently, however, a ransomware that attacked a hospital in the US demanded 9,000 bitcoins (worth roughly \$3.6 million USD). The hospital ultimately paid 40 bitcoins (\$17,000 USD) to decrypt their encrypted data.

There are two points to note here. First, attackers may re-attack victims who have already paid up. The victims will surely be aware of the possibility and reinforce their security to prevent further attacks. However, the cyber criminals will be ready to beat the reinforced security.

Second, attackers will not stop at demanding ransoms at the previous amount of \$400 USD. There has been a successful case in which much more money has been made, so it is plausible that attackers will strive for higher ransom amounts. They may also use malware to gain private and corporate information to classify victims according to the amount of money available. Also, the distribution of ransomware for financial gain from a specific organization may become a new type of Advanced Persistent Threats (APTs).

Conclusion: Security Advisory

As examined above, attackers continue to distribute ransomware variants heavily armed with various features to bypass security solutions. Thus, it is not easy to respond to attacks using only traditional security solutions. Ransomware use encryption algorithms to encrypt files, so it is in fact almost impossible to restore the encrypted files. To prevent ransomware attacks, users need to exercise caution: immediately delete suspicious emails or emails from unknown senders, and always back up important data.

With its line of V3 antivirus products and AhnLab MDS (Malware Defense System), an APT (Advanced Persistent Threats) protection solution, AhnLab has garnered much notice for having detected and responded to the variety of ransomware that have been discovered up to this date. In order to reduce the damages caused by ransomware, users should install the latest updates for V3 engine currently in use. Also, by activating the Execution Holding function for customers who use AhnLab MDS, ransomware can be blocked.