2016. 04. 06

Analysis Report

Q1 2016 Ransomware Trends

AhnLab

www.ahnlab.com

Table of Content

Introduction

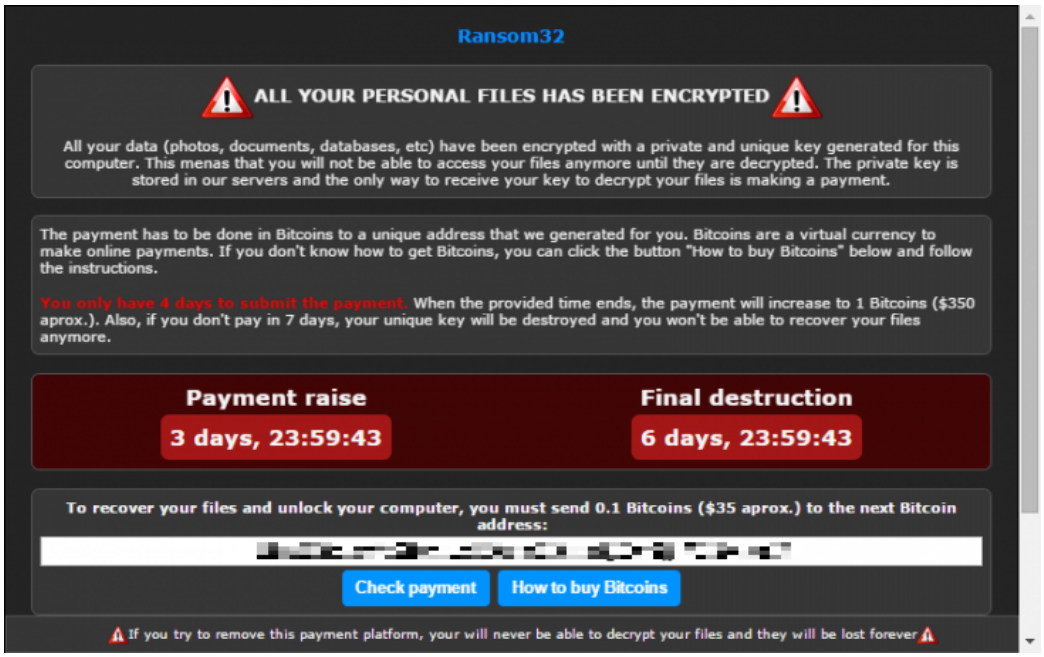
Ever since the first ransomware, PC Cyborg Trojan (aka AIDS), was discovered in 1989, ransomware has been making appearances here and there. In the mid-2000s, GPCode ransomware emerged that used an RSA algorithm to encrypt multiple file extensions and demanded ransom for its decryption tool. However, 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

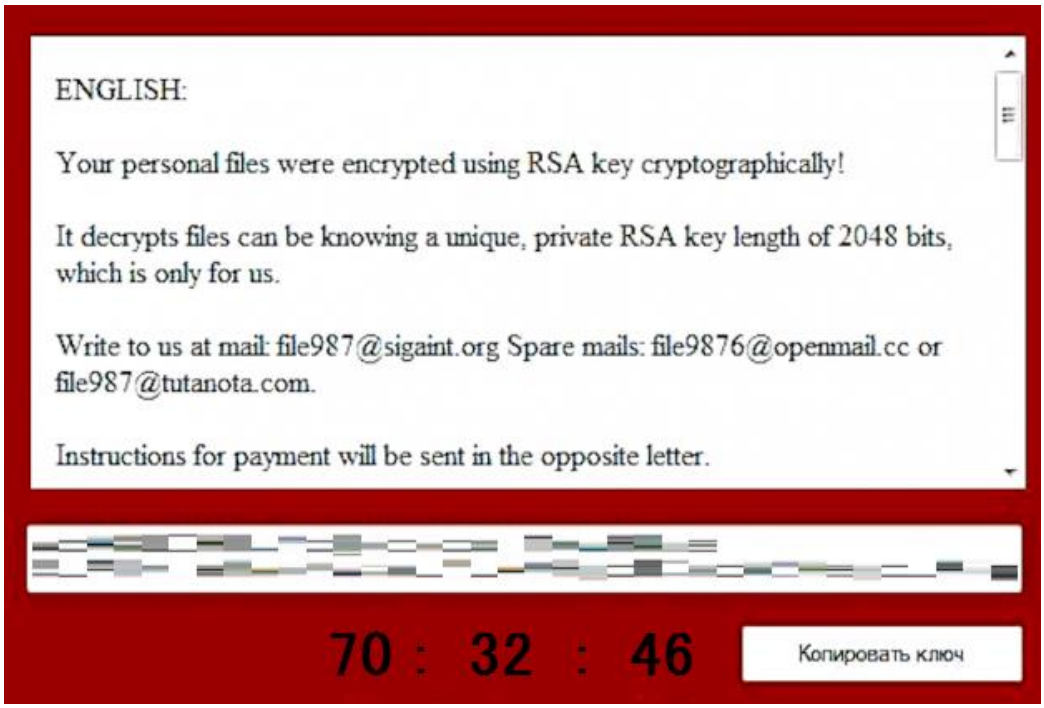
The so-called Ransom32 is the first ransomware to be written in JavaScript. The JavaScript distributed via spam email campaign is obfuscated, and then downloads and executes ransomware. It uses Tor network, and an AES and RSA encryption algorithm.



[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.



[Fig. 2] Screenshot of CryptoJoker ransomware

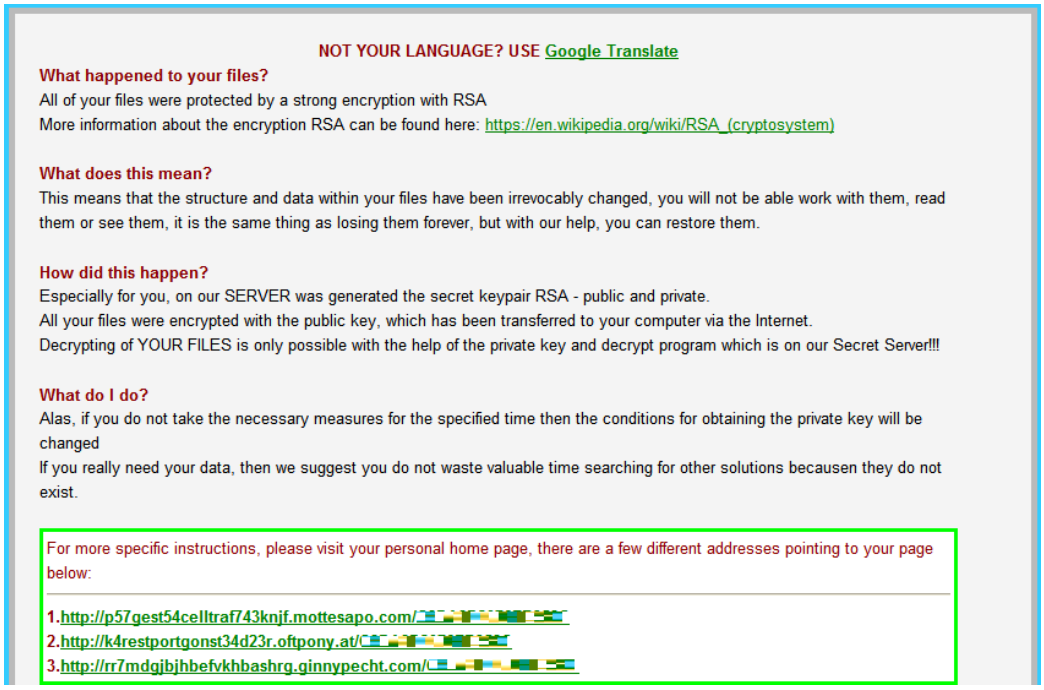
3. LeChiffre that launches remote attacks

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.

[Fig. 3] Warning dialogue of LeChiffre ransomware

4. TeslaCrypt 3.0 that changes file extensions

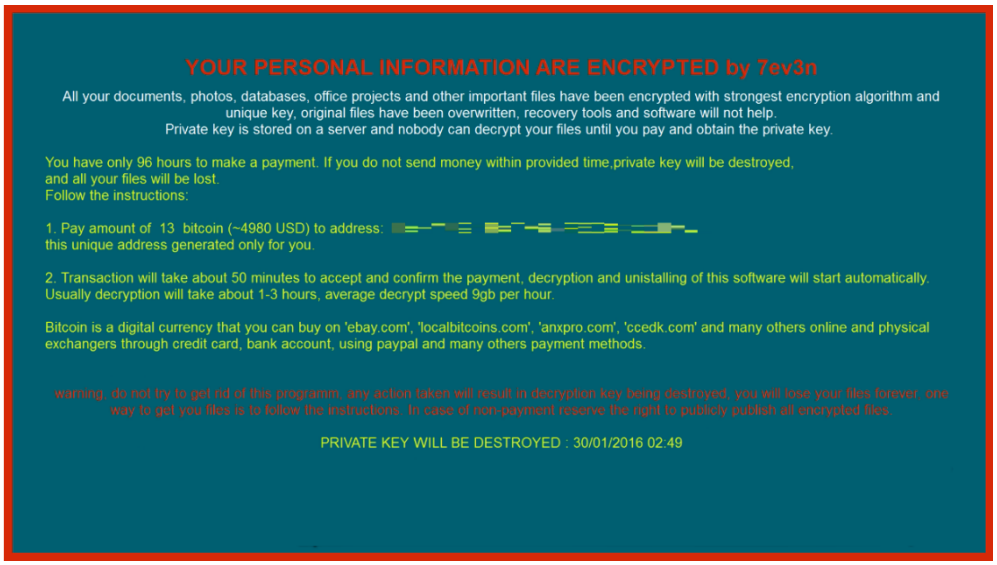
TeslaCrypt 3.0 shows a change in both encryption algorithm and file extension when compared to previous ransomware. It adds .xxx, .TTT, .Micro or .mp3 extensions to the end of the file name of the encrypted file.



[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

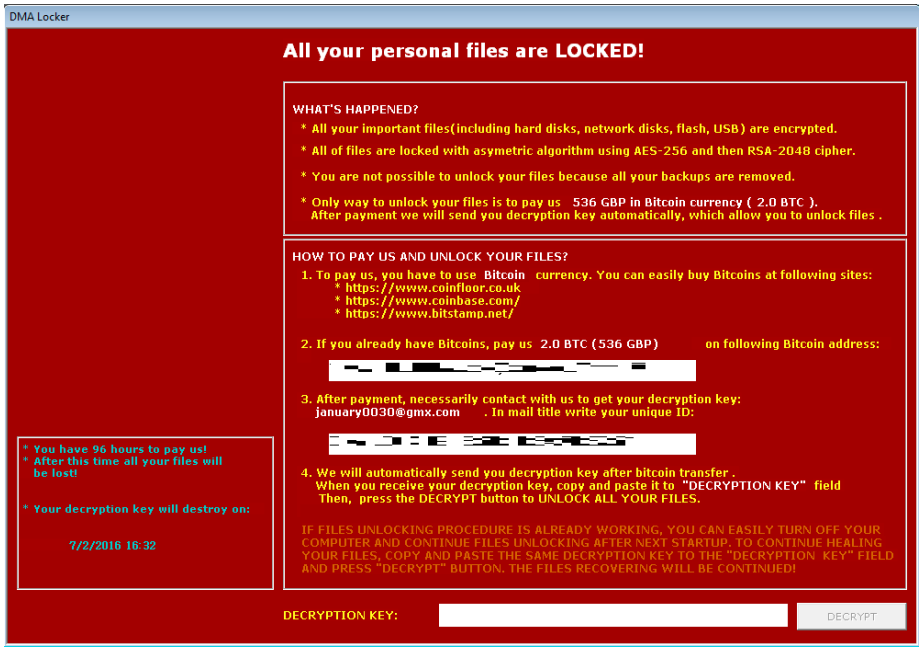
7. NanoLocker spread via spam mail disguised as a PDF file

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

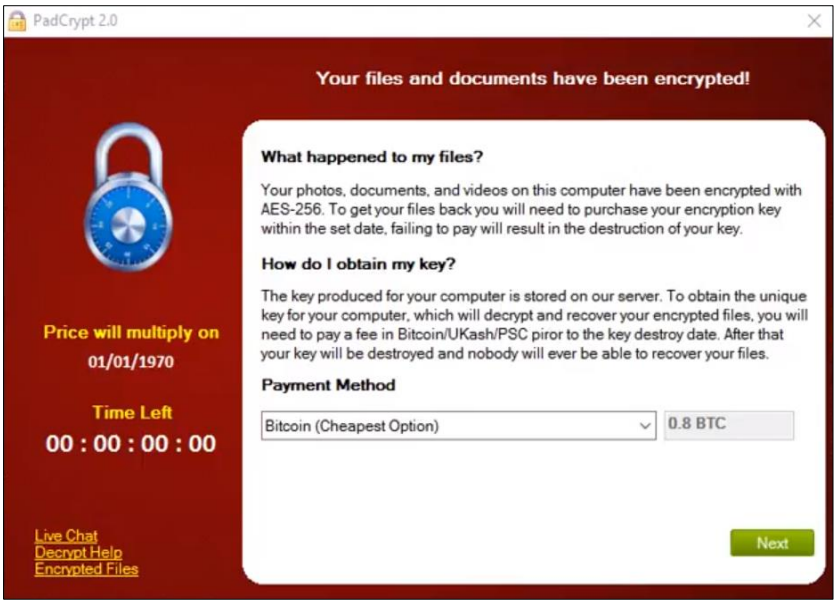
9. UmbreCrypt that adds an identifier behind the encrypted file extensions

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.

[Fig. 9] Screenshot of UmbreCrypt ransomware

10. PadCrypt that comes with live chat feature

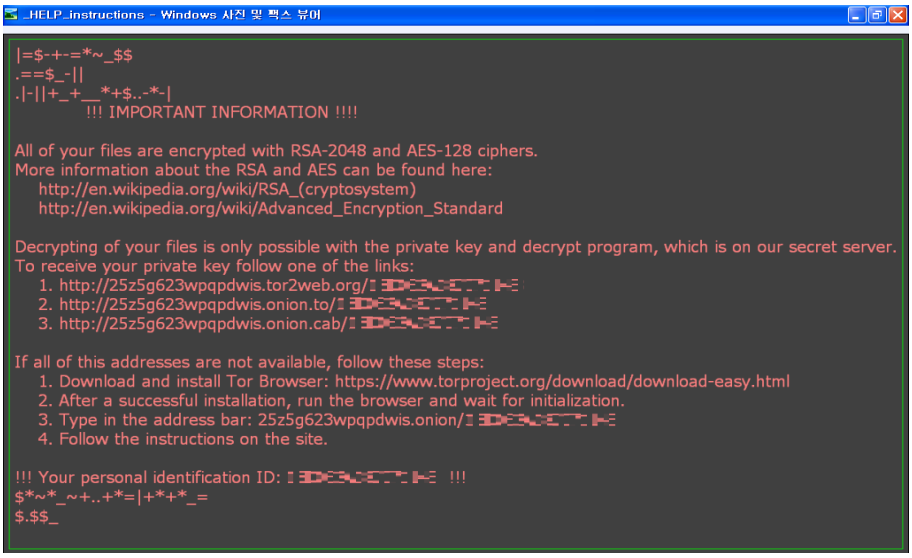
PadCrypt becomes installed and then infects systems when the victim executes the double-extension file (.pdf.scr) in the zip file attached to a spam mail. It also comes with a live chat feature in a separate window that opens when the victim clicks “Live Chat” on the bottom-left of the notification message.



[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.

[Fig. 12] KeRanger ransomware distributed with Transmission

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.

