Manamecrypt – a ransomware that takes a different route

gdatasoftware.com/blog/2016/04/28234-manamecrypt-a-ransomware-that-takes-a-different-route

Hardly a week passes these days without a new family of ransomware making the headlines. This week our analysts are taking apart Manamecrypt, also referred to as CryptoHost. Basically, Manamecrypt is a ransomware Trojan horse, but it differs from other ransomware families in a number of aspects. For instance, it not only encrypts files, but also prevents certain applications from running which have a specific pattern in their process name. Also, it uses an unconventional way of spreading which so far was not considered typical of ransomware. The good news for victims is: the encryption of its current iteration can be cracked!

Infection vector: the classic Trojan horse

The main aspect in which Manamecrypt is fundamentally different from other file-encrypting types of malware we heard of in the past weeks is: the analyzed sample does not spread vial email attachment or via an exploit kit. Instead, it bundles with legitimate software and can therefore be classified as a classic Trojan horse. The bundle consists of the genuine, working and properly signed µTorrent client with the malware component bundled “on top”.

- Bundle: c71c26bf894feb5dbedb2cf2477258f3edf3133a3c22c68ab378ba65ecf251d3
  G DATA detection: Gen:Variant.MSIL.Lynx.13

- Dropped µTorrent Client:
  b7579ad8dfa57512a56e6ff62ae001560c00a4ebb9faa55086a67d30fbb1eea6
  G DATA detection: Win32.Application.OpenCandy.G

- Dropped Ransomware:
  4486a1aaa49d8671826ff4d0d5c543892e1a3f0019e7f041032531ff69839bc9
  G DATA detection: Trojan.GenericKD.3048538

Interesting fact: due to a coding error the µTorrent Client is saved as uTorrent.exeuTorrent.exe instead of its original name, uTorrent.exe. The client is also detected by G DATA’s solutions as Win32.Application.OpenCandy.G.

Win32.Application.OpenCandy.G is a Potentially Unwanted Program (PUP). It is installed alongside legitimate freeware such as PDF readers, archive programs, media players and other applications which are bundled with the software. The software which is detected as Win32.Application.OpenCandy.G is developed by SweetLabs, a company based out of San Diego, CA, USA. This PUP changes the browser’s behavior by modifying its home page as

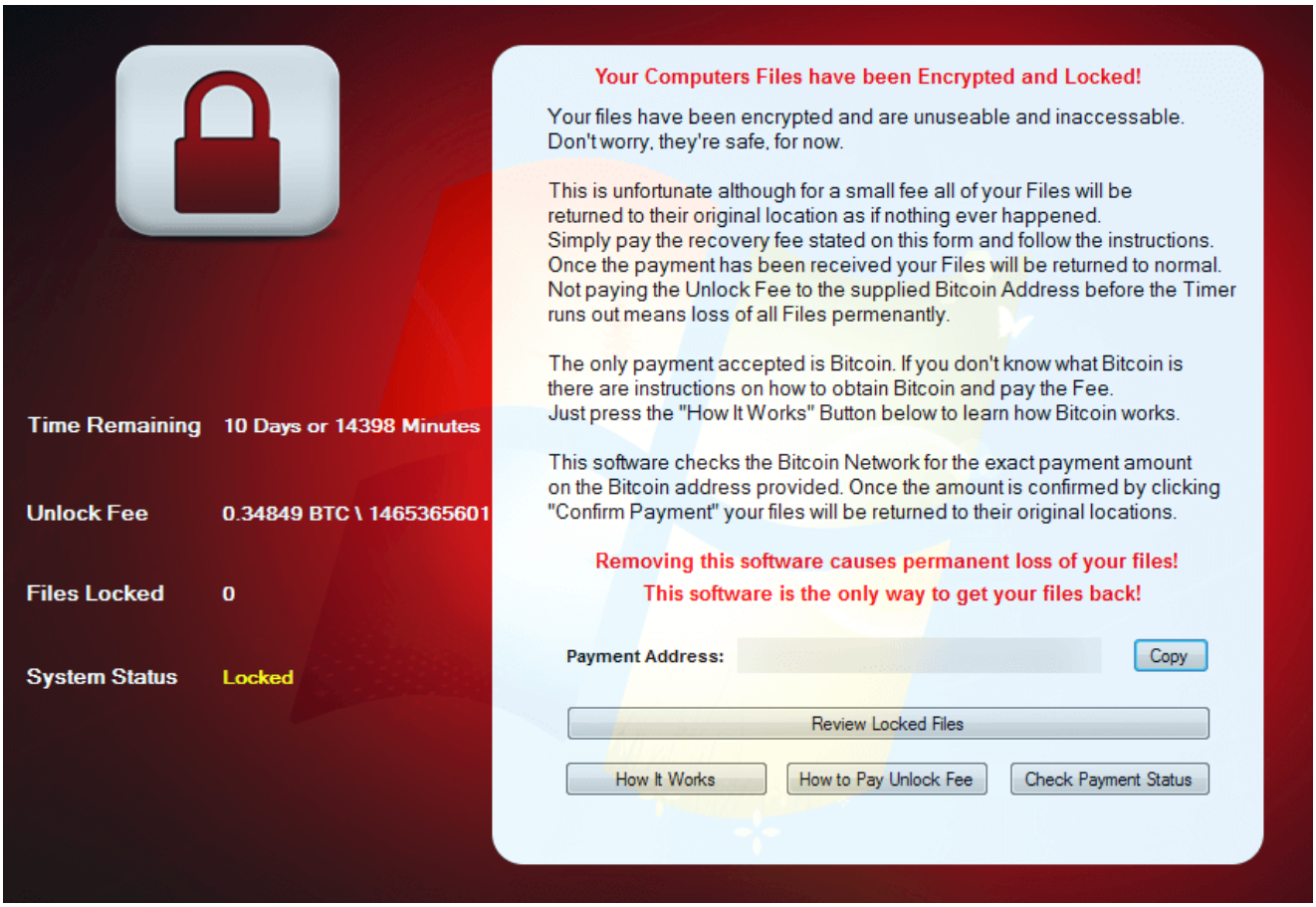
well as search engine settings. Users are then redirected to potentially unwanted websites and it displays pop-up notifications. The reason for those changes is the generation of profit through displaying advertisements.

What Manamecrypt does on an infected PC

The malware has several functions: it encrypts the user's files and it blocks certain programs on the PC. This type of behavior has been unheard of so far.

The encryption is also fundamentally different from the likes of Locky, Petya or Teslacrypt which made the rounds for the past few weeks. Manamecrypt takes the data it wants to encrypt and copies it to a .RAR file (a type of archive file, similar to .ZIP), and encrypts this archive with a password. The original files are then deleted. The following file types are encrypted:

```
*.3g2 *.3gp *.7z *.asf *.avi *.doc *.docx *.flv *.gif *.jpeg *.jpg *.m4v *.mov *.mp4
*.mpeg *.mpg *.pdf
*.png *.ppd *.pps *.ppt *.pptx *.psd *.qt *.rm *.tiff *.txt *.wmv *.wpd *.wps *.xlr
*.xls *.xlsl *.zip
```



Manamecrypt shows its demands

Besides encrypting the files, Manamecrypt prevents certain applications from running if they have certain strings in their process name. For instance, a frequently used analysis tool was shut down very quickly by the malware:

The word "monitor" in the process name triggers the malware's action

If the ransomware comes across a window which contains the following strings, it terminates the corresponding process immediately:

ad-aware	facebook	registry editor
amazon	game	rune
anti virus	instagram	shop
anti-virus	internet security	sophos
antivirus	kaspersky	steam
avg	lol	system configuration
avira	mcafee	system restore
bitdefender	meetme	task manager
bullguard	monitor	trend micro
comodo	netflix	tumblr
debugger	norton	twitter
dr.web	obfuscator	vimeo
ebay	origin	vipre
f-secure	registry	

Technical details

When executed, a new entry called „software“ is added to the registry at HKCU\Software\Microsoft\Windows\CurrentVersion\Run. This enables the malware to run at boot-up.

Furthermore, the following files are created:

%APPDATA%\cryptohost.exe (The actual ransomware binary, a copy of the sample)
%APPDATA%\processor.exe (WinRAR command line tools)
%APPDATA%\files (a list of file names with encrypted files)
%APPDATA%\[Encrpted_RAR_with_generic_name]

In addition, the following key is written to the registry: „HKCU\Software\VB and VBA Program Settings\software\setting\“ - The amout of Bitcoin to be paid as well as the remaining time are stored in here.

To decrypt, processor.exe is called as follows: „processor X -o+ -pEncryptedRarArchiveNameUserName EnryptedRarArchiveName.rar C:\Users\UserName\Desktop“.

It is possible to get your data back!

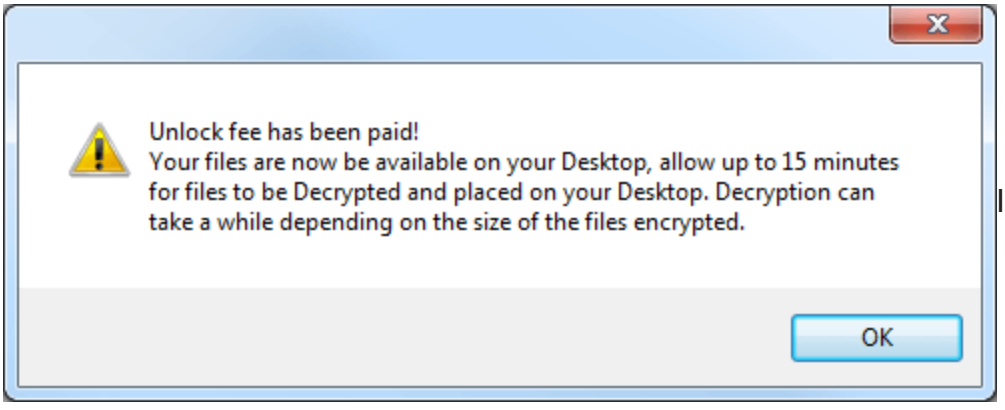
In its current implementation, the ransomware is actually susceptible to attacks. Victims can restore their data. The password for the RAR file consists of the following components:

SHA1Hash(Win32_processor.processorID + VolumeSerialNumber_Volume_C + Win32_BaseBoard.SerialNumber) + username

Researcher at PCRisk.com reported that the password for RAR files created by their sample of Manamecrypt consists of “the name of the .RAR file + computer name.” According to our results, it is a combination of the .RAR file’s name and the user name instead of the computer name.

The SHA1 is the name of the .RAR file. The user name can be determined as follows: press the Windows key + R; then enter cmd and press Enter. In the newly opened command line window, enter echo %username% and press Enter again. The displayed string is the user name.

Example: The .RAR file is called 123456789ABCDE and the Username is JDoe. The password therefore is 123456789ABCDEJDoe



In case the password is entered correctly, Manamecrypt releases the date

Summary

Ransomware remains one of the most obvious threats within the past weeks. Manamecrypt/Cryptohost differs on some aspects from malware which was observed before. The mode of propagation, encryption method and blocking of programs are the most prominent differences. Also, experts were able to provide a way of decrypting files in a very short time. Still, prevention is the method of choice in the battle against file-encrypting malware. The following tips are a good foundation for an effective defense.

How to protect yourself – prevention is the key

Infection with such an encryption Trojan is fatal for the afflicted users and companies and, in many cases, decrypting the data without the appropriate key is extremely resource-intensive, even impossible. Looking at Manamecrypt/CryptoHost, it is possible to decrypt the files of the current attacks.

Paying the ransom is no guarantee that the data will be decrypted again by the attackers. An extortioner can suddenly demand more money to release the data, or encrypt the data once again at a later date via a backdoor in the system and demand money again – even when it at first appears that he has kept his promise and released the data.
In the investigations to date, Manamecrypt is not conspicuously using such a backdoor, as other malware families do.

The payment demanded is generally made via e-Payment systems that provide anonymised accounts and payment methods - in the current case: Bitcoin. Hence, if the extortioner fails to do anything about the decryption despite the payment being made, the money cannot be reclaimed or tracked. So making a payment implies risk in all sorts of ways.

Consequently it is particularly important that preventive steps are taken against this type of malware, and that a comprehensive security concept is in place.

Use a comprehensive security solution

Get a comprehensive solution that includes not just a virus scanner but also proactive technologies for fending off previously unknown threats. Obviously the protective software should also monitor the email inbox. Always keep the security solution installed on the computer fully up-to-date.

Download software from the producer's website

In this current case, the ransomware component was bundled with a legitimate program - a classic Trojan horse. Our advice: download needed/wanted software from the producer's website only or from trusted download portals. Where possible, do not download it from third-party-sites.

Create backups

Regular backups ensure that you are less dependent on the data on the computer. This is not only advantageous in the event of a malware infection, but also if the system suffers a technical failure. Store the backups offline, i.e. separate from the computer being used. Some ransomware tracks down and encrypts data stored on network drives, attached USB sticks, connected external hard drives and in the Cloud.

Carry out updates

Software programs contain both small and major bugs that are found and removed over time. Once the developers have improved ("patched") the program, they expect end users to update the product. Malware – including ransomware – can be smuggled onto computers via unclosed vulnerabilities.

End users should regularly look out for updates or patches and, where available, install them immediately. Software and operating systems frequently offer automated availability checks for updates, making it easier for the user to stay up to date. In the business world, one refers to Patch Management. The list of software to be updated includes both installed programs and the operating system and, above all, the browser and all available plug-ins used in conjunction with the browser.

Check email attachments before opening them

As is seen with e.g. Locky or Teslacrypt, emails act as a gateway for this type of malware. Therefore attachments from unknown sources should never be opened without thinking – especially not if they are executable files. These days, many email services will block the sending and receipt of executable files; therefore the attackers use indirect means, by making the addressees click on a link or by packing the files into archives, as in this case.

By all accounts resist the urge to satisfy your curiosity, even if you appear to have received an overdue notice or indeed a copy of the salary scale. Regard attachments from internal staff with a critical eye as well. Senders' names can be faked.

If you know the sender or at least have contact details for him/her, use a second channel (e.g. telephone) to ask if the email has actually come from that person before opening the attachment.

Disable the automatic execution of macros

The execution of macros is disabled by default in modern Microsoft Office products, for security reasons. Check the current settings for the product you are using and adjust them in case necessary. Microsoft also advises to disable macros.