Behind LockerGoga – A walk through a ransomware attack worth 40m$

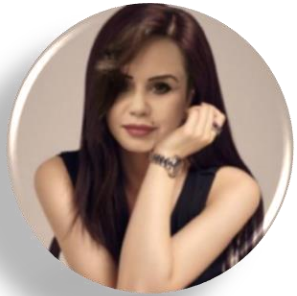
Magda Lilia Chelly, PhD. CISSP

My Career So Far ….

Failing modelling career / Ongoing PhD

IT/Security Consultant & Trainer

Chief Information Security Officer On Demand



CyberFeminist Hacker & Influencer (A lot of photoshop…)

Special Thanks to **Rik Ferguson, VP Security Research at Trend Micro**

And below public contributors to ransomware research:

Contributors	Florian Roth	@cyb3rops
	Bart P	@bartblaze
	Michael Gillespie	@demonslay335
	Marcelo Rivero	@MarceloRivero
	Daniel Gallagher	@DanielGallagher
	Mosh	@nyxbone
	Karsten Hahn	@struppigel
	Anthony Kasza	@anthonykasza
	John Bambenek	@bambenek
	Devon Ackerman	@AboutDFIR
	Fernando Mercês	@MercesFernando
	Jas Chase	@jasc22

Encrypting Ransomware

Incorporated with advanced encryption algorithms, this type of ransomware is designed to block system files and demand payment to provide the affected user with the key that will decrypt the blocked content. For example: Crypto Locker, Wannacry, Locky, CrytpoWall, etc.

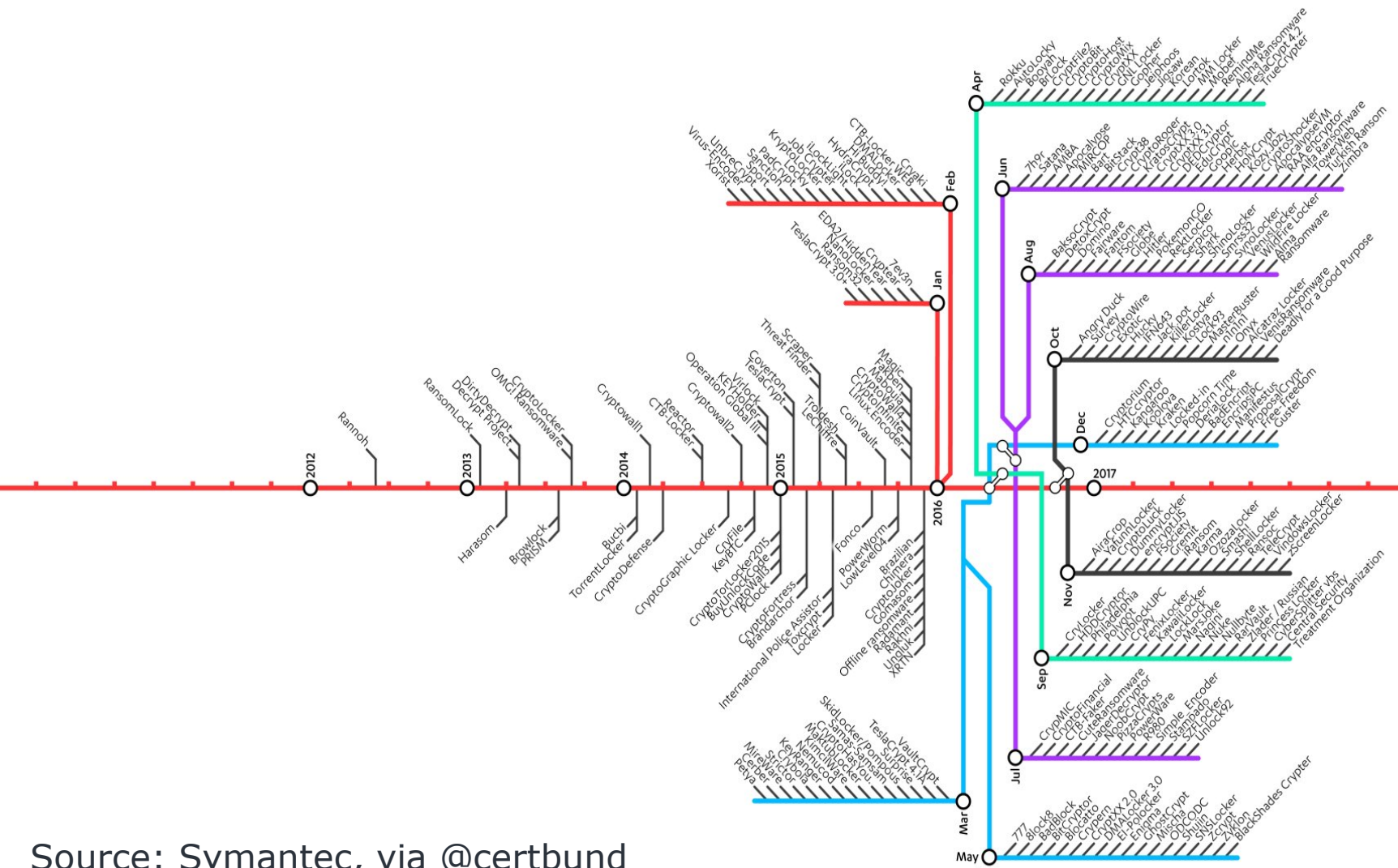
Locker Ransomware

This malware locks the person out of the OS, making it impossible for them to access the data saved on it. Here, the files are not encrypted, but the ransomware still asks for a ransom to unlock the infected device. For example: Police-themed ransomware or Win locker.

MBR Ransomware

Master Boot Record (MBR) ransomware is a type of Locker ransomware. The MBR is a section of a hard drive that enables the Operating System to boot up. However, when the MBR ransomware attacks the drive, the boot process fails to complete and demands the payment of ransom as soon as possible. For example: Satana, Petya, etc.

Source: https://secure.wphackedhelp.com/blog/b0r0nt0k-ransomware/



Source: Symantec, via @certbund

Riviera Beach

US$600,000

May 29

Lake City

US$460,000

June 10

Key Biscayne

No reported payment

June 23

77% ↑

Overall ransomware detections compared to the second half of 2018

55% ↓

New ransomware families compared to the second half of 2018

Ryuk

- Arrives via spam

- Can render infected systems unbootable

LockerGoga

- Arrives via compromised credentials

- Modifies the passwords of infected systems' user accounts, prevents infected systems from being rebooted

RobbinHood

- Arrives via unsecure remote desktops or trojans

- Encrypts each file with a unique key

BitPaymer

- Arrives via compromised accounts and emails containing Dridex

- Abuses PsExec tool

MegaCortex

- Arrives via compromised controllers

- Disables certain processes

Nozelesn

- Arrives via spam

- Its trojan downloader, Nymaim, uses fileless techniques to load the ransomware.

Companies do not patch …

Employees click on phishing links …

Type of Ransomware – What companies do … if they do …

	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)
777	.777	._[timestamp]_$[email]$.777 e.g. ._14-05-2016-11-59-36_$ninja.gaiver@aol.com$.777	read_this_file.txt		XOR
7ev3n	.R4A .R5A		FILES_BACK.txt		
7h9r	.7h9r		README_.TXT		AES
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES(256)
AiraCrop	._AiraCropEncrypted		How to decrypt your files.txt	related to TeamXRat	
Al-Namrood	.unavailable .disappeared		Read_Me.Txt		
Alcatraz Locker	.Alcatraz		ransomed.html		

Norsk Hydro was not an accidental, "WannaCry" style indiscriminate attack, but a deliberate, targeted strike on critical infrastructure.

The Infection

The ransomware was dropped and executed by a renamed **PsExec tool.**

→ It is the same system administration tool abused by various ransomware such as **SOREBRECT and Bad Rabbit.**

The Evasion

Codesigning was used in order to bypass the antivirus → Companies whitelist signed software.

Numerous vendors on the dark web sell such certificates for a relatively cheap price of between **500 and 1700 USD**, so signed ransomware is becoming increasingly common.

Хочу предложить Вам готовые, качественные сертификаты CodeSigning Comodo и CodeSigning EV GlobalSign С расширенной проверкой компании!

Цены на сертификаты следующие:
CodeSigning - $400
CodeSigning EV - $1700
EV SSL - $500

Чистка от AB - $150

telegram:
jabber: f
jabber2:

Сертификаты для подписи кода используются разработчиками для подписи своего программного обеспечения, чтобы доказать, что оно (ПО) не было изменено или скомпрометировано третьей стороной. Несмотря на то, что программное обеспечение, приобретенное в розницу, как правило, считается относительно безопасным, программы, загружаемые из Интернета, часто подвергаются сомнению из-за широкого распространения вирусов и вредоносного ПО. Наличие цифрового сертификата подтверждает целостность (неизменность) программного кода с момента его выпуска. Соответственно, если ваш файл имеет цифровую подпись, пользователи будут относиться к ней с большой уверенностью при загрузке из Интернета или запуске.

Подписанный файл обходит блокировки многих антивирусов, а EV CodeSigning позволяет без набора репутации сертификата обходить SmartScreen!
Учитывая новые правила получения сертификатов, проще купить у нас, чем заморачиваться самим!

Сроки
Code Signing - 2-3 рабочих дней
Code Signing EV- до 10ти рабочих дней.
Гарант.
Сертификаты делаю строго под ключ.

К оплате принимаем: Bitcoin, Ethereum, Monero

The Executable

It is a 32-bit executable compiled by VS2015.

The Infection

%TEMP% directory,

cmd.exe /c move /y tgytutrcXXXX.exe %TEMP%\tgytutrcYYYY.exe

"C:\Windows\system32\wevtutil.exe" cl Microsoft-Windows-WMI-Activity/Trace

→ Ransom note and encryption process.

The Infection

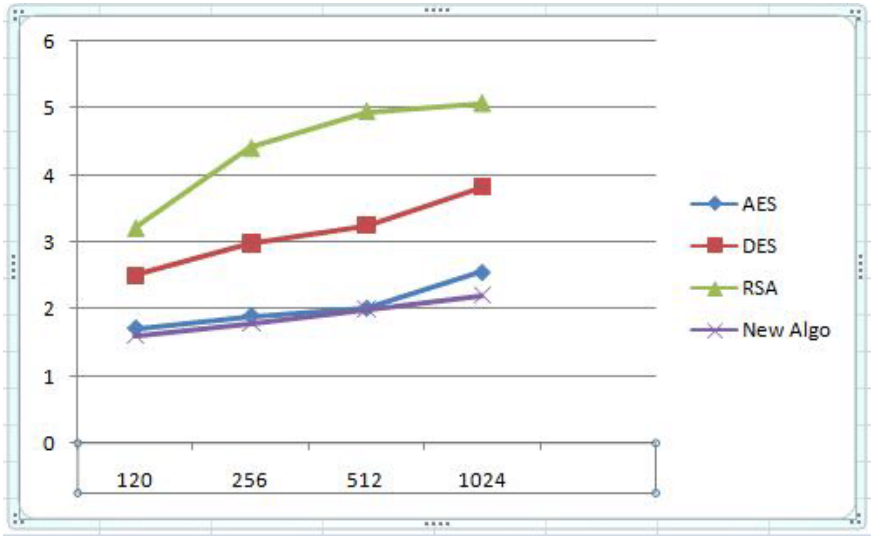
- **The process with -m** as the parameter is mainly for scheduling (System-wide lock- Mutex).
- **“-iSM-zzbdrimp –s” c**reate more child processes.
- The parent process detects the number of child processes. The number of child processes is the same as the number of CPU cores.
- The child process obtains the path of the file from the parent process, and the path name needs to be decoded by Base64.

The Encryption; AES & RSA

AES key to encrypt the file using the AES algorithm.

Hard-coded RSA public key in the decoding program:

The Encryption; AES & RSA



The Ransom

Manual process of email, using numerous **Protonmail**, mail.com and o2.pl email accounts

Summary

LockerGoga encrypts various types of files, including executable files, system directories, and files in the startup directory.

It is very destructive…

It traverses files in the parent process, then encrypt files in multiple child processes, and leverage multiple cores of the CPU.

The Detection

6 known samples of LockerGoga in the wild:

1.7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26

2.C3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a

3.88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f

4.c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15

5.eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0

6.ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f

The Prevention

Measure
Backup and Restore Process
Block Macros
Disable WSH
Filter Attachments Level 1

Filter Attachments Level 2
Email Marking
Restrict program execution
Show File Extensions

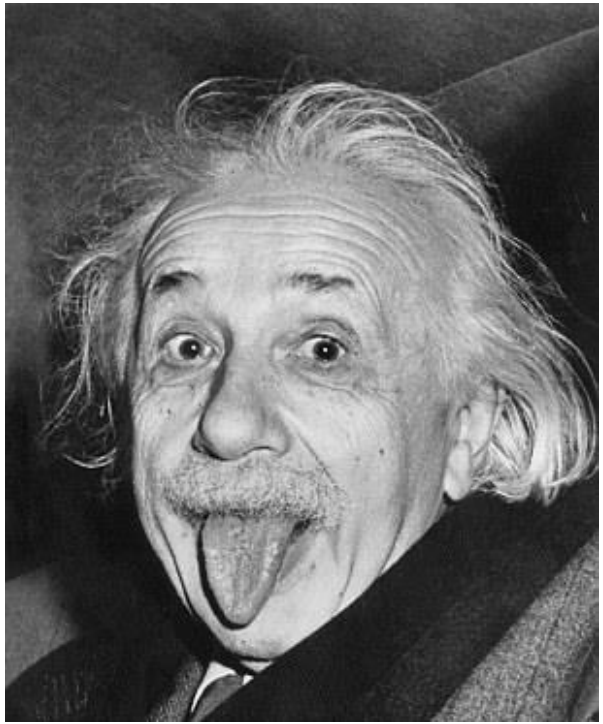
Measure
Enforce UAC Prompt
Remove Admin Privileges
Restrict Workstation Communication
Sandboxing Email Input
Execution Prevention
Change Default "Open With" to Notepad
File Screening
Restrict program execution #2
EMET
Sysmon

Wrong Assumptions

Backup will ALWAYS save you !

If the ransomware encrypts the files, then it will encrypt the backup as well overwriting the good one…

Who’s in the game, yet ?



Thank You

Magda Chelly
mchelly@responsible-cyber.com