Deep Dive Into Unfading Sea Haze: A New Threat Actor in the South China Sea

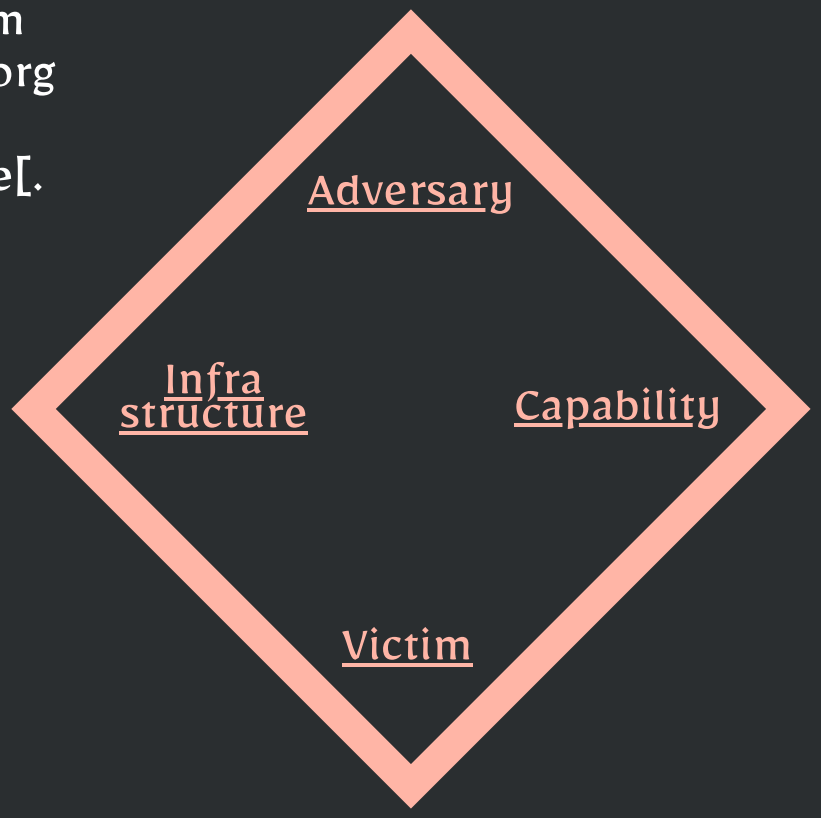
IoC: ✓

MITRE ATT&CK: ✗

Timeline: Since 2018 - 2024

Unfading Sea Haze

- upupdate.ooguy[.]com
- bitdefenderupdate[.]org
- payroll.mywire[.]org
- api.bitdefenderupdate[.]org
- ……
- 167.71.199[.]105
- 188.166.224[.]242
- 159.223.78[.]147
- 128.199.166[.]143
- 164.92.146[.]227
- 192.153.57[.]24
- 209.97.167[.]177
- 112.113.112[.]5
- 193.149.129[.]128
- ……..



Gov. & Mil. org in South China Seas Countries

- GhOst RAT Variations
- SharpJSHandler
- Ps2dllLoader
- DustyExfilTool
- SerialPktdoor (Backdoor)
- SpearPhishing
- Powershell
- Scheduled Task
- Masquerading
- DLL Side-Loading
- Manipulating local Administrator accounts
- Modify Registry
- Web Shell
- Keylogging
- ……..

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Bitdefender
Date: 22 May 2024

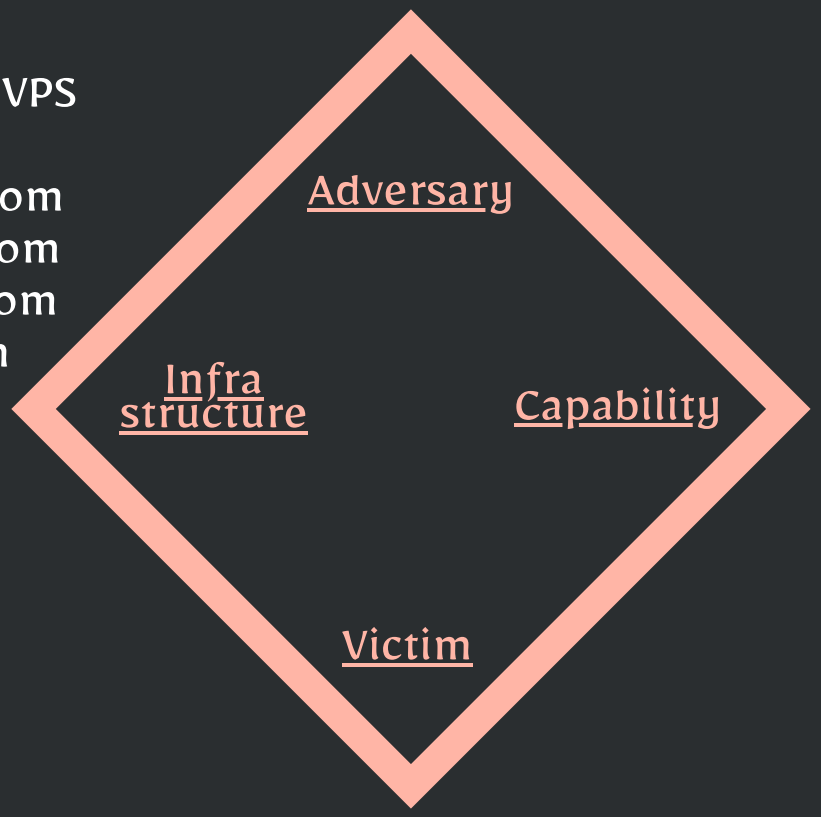
An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set

IoC: ✓

MITRE ATT&CK: ✗

Timeline: since at least late 2022

Operation Diplomatic Specter



- used Chinese VPS providers for C2
- home.microsoft-ns1[.]com
- cloud.microsoft-ns1[.]com
- static.microsoft-ns1[.]com
- api.microsoft-ns1[.]com
- update.microsoft-ns1[.]com
- labour.govu[.]ml
- govm[.]tk
- 103.108.192[.]238
- 103.149.90[.]235
- 192.225.226[.]217
- 194.14.217[.]34
- 103.108.67[.]153
- .....

- TunnelSpecter
- SweetSpecter
- GhOst RAT
- TunnelSpecter
- SweetSpecter
- Agent Racoon
- Ntospy
- PlugX
- GhOst RAT
- China Chopper
- Yasso Penetration Tool Set
- Impacket
- Mimikatz
- Htran
- JuicyPotatoNG
- SharpEfsPotato
- .....

Governmental Entities in the Middle East, Africa and Asia

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Unit 42
Date: 23 May 2024

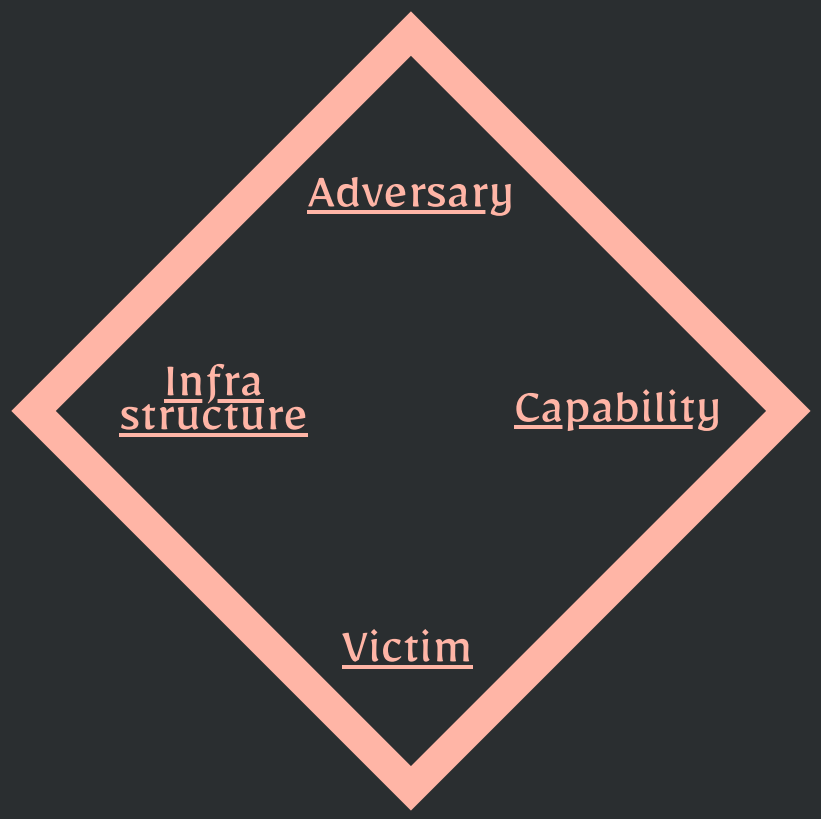
Inside the SharpPanda's Malware Targeting Malaysia

IoC: ✓

MITRE ATT&CK: ✗

Timeline: March - April 2024

SharpPanda



- 185.239.226.91 (located in Hong Kong)

- T1204.002 User Execution: Malicious File
- T1573.001 Encrypted Channel: Symmetric Cryptography
- T1132.001 Data Encoding: Standard Encoding
- T1041 Exfiltration Over C2 Channel
- .....
- Executable file with Microsoft Word Icon(REKOD MINIT KSN KEPADA YAB PM 2023 - 15.exe)

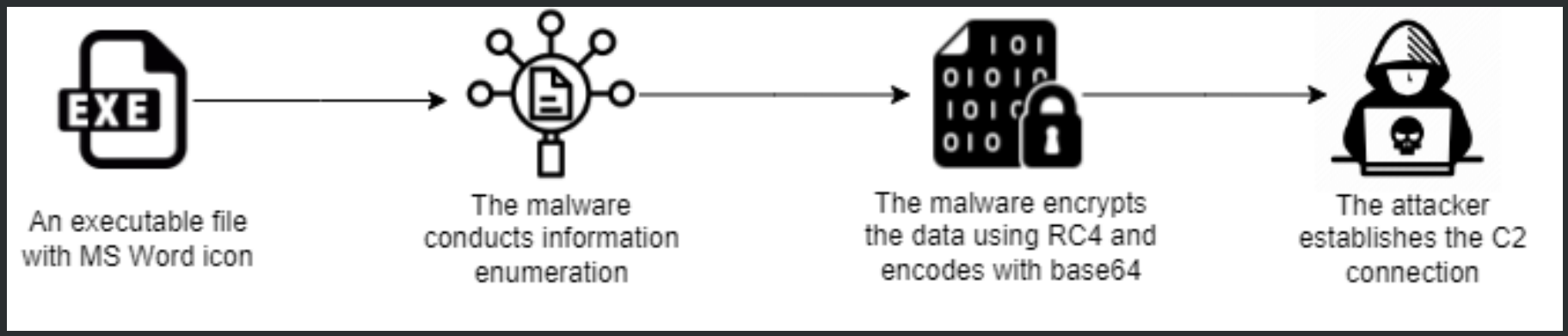
Malaysia

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: NetbyteSEC
Date: 24 May 2024

Inside the SharpPanda's Malware Targeting Malaysia

Execution	Discovery	Command and Control	Exfiltration
Native API	Process Discovery	Data Encoding	Exfiltration Over C2 Channel
User Execution	Software Discovery	Standard Encoding	
Malicious File	System Information Discovery	Encrypted Channel	
	System Network Configuration Discovery	Symmetric Cryptography	
	System Owner/User Discovery		



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: NetbyteSEC
Date: 24 May 2024

Estate Ransomware

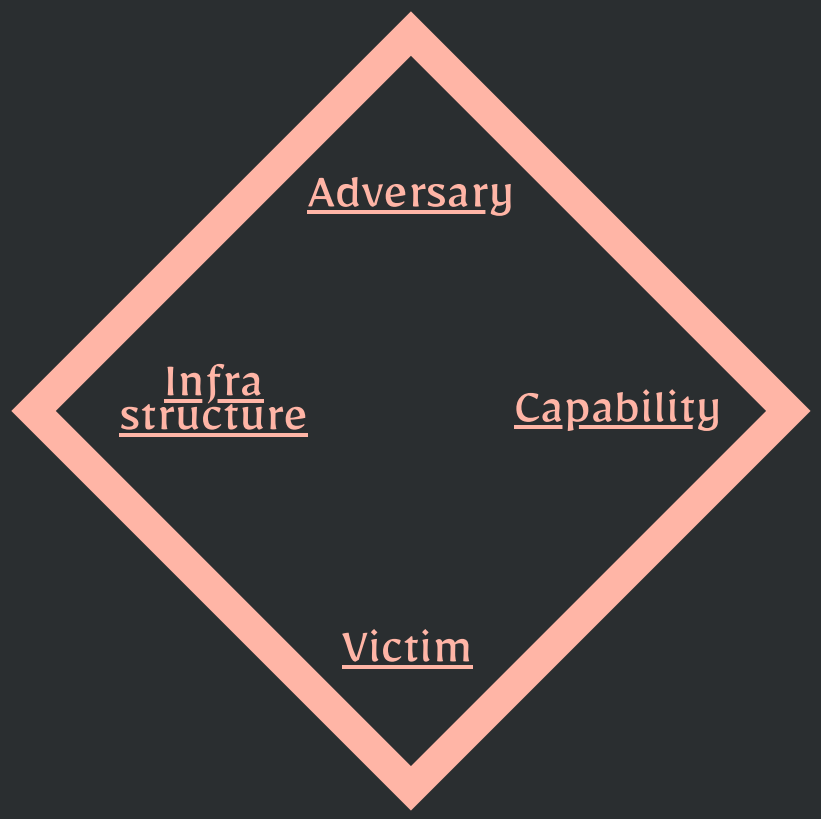
IoC: ☒

MITRE ATT&CK: ☒

Timeline: Unknown

EstateRansomware

- **xindiaz12@cyberfear.com**
- **.6AklzADP4 file extension**



- EstateRansomware
- T1486 : Data Encrypted for Impact
- TA0010 : Exfiltration

Potentially Malaysian Organization (Observed by MyCERT)

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: MyCERT
Date: 28 May 2024

Estate Ransomware

6AkIzADP4.README.txt

```
Your network/system was encrypted by EstateRansomware.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement, your data will be published.
Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.


-- Recovery

Use email: xindiaz12@cyberfear.com (Use a new Protonmail.com account. In the first message, specify the encryption ID!)
```

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: MyCERT
Date: 28 May 2024

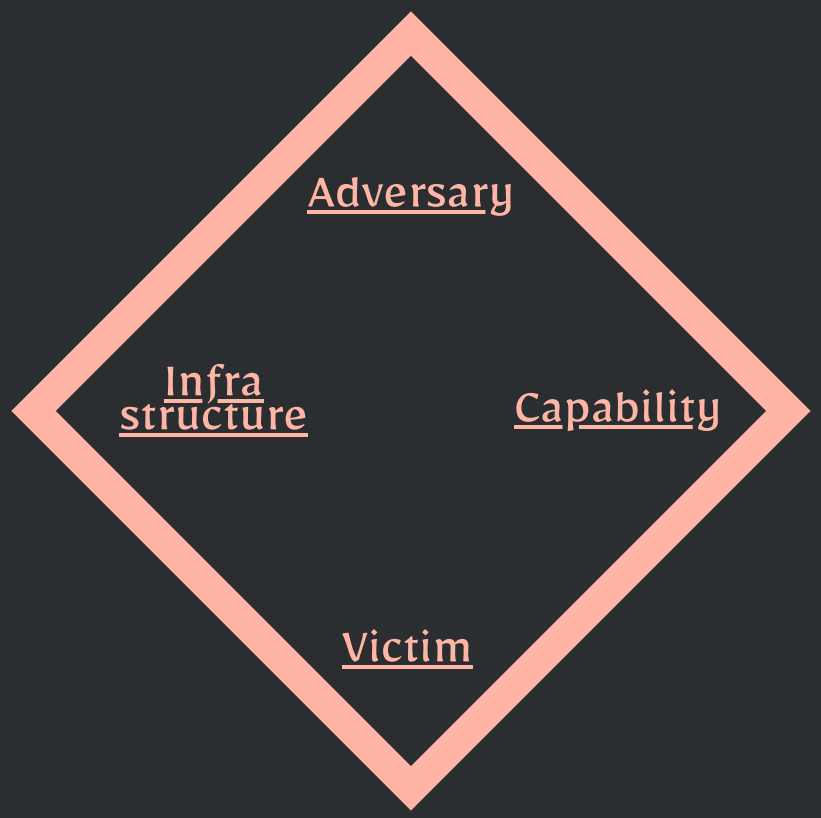
LilacSquid: The stealthy trilogy of PurpleInk, InkBox and InkLoader

IoC: ✓

MITRE ATT&CK: ✗

Timeline: since at least 2021

LilacSquid



- 67.213.221.6
- 192.145.127.190
- 45.9.251.14
- 199.229.250.142

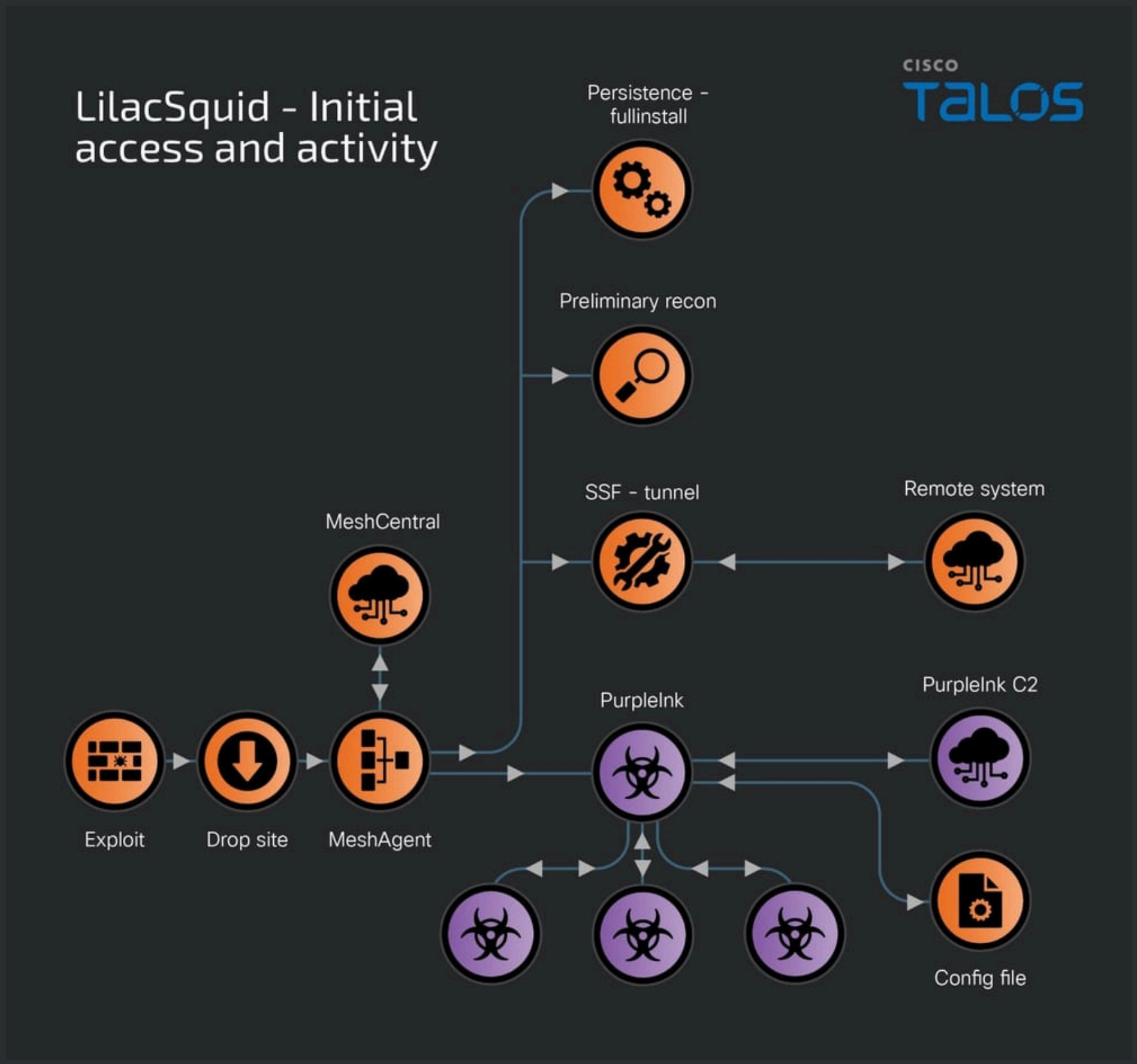
- MeshAgent
- PurpleInk
- InkBox
- InkLoader
- Secure Socket Funneling (SSF)
- T1588.006 Obtain Capabilities: Vulnerabilities
- T1021.001 Remote Services: RDP
- S0190 : BITSAdmin
- T1569.002 System Services: Service Execution
- T1059.003 Command and Scripting Interpreter: Windows Command Shell
- T1041 : Exfiltration Over C2 Channel

- **IT research in US**
- **Energy Sector in Europe**
- **Pharmaceutical in Asia**

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cisco Talos
Date: 30 May 2024

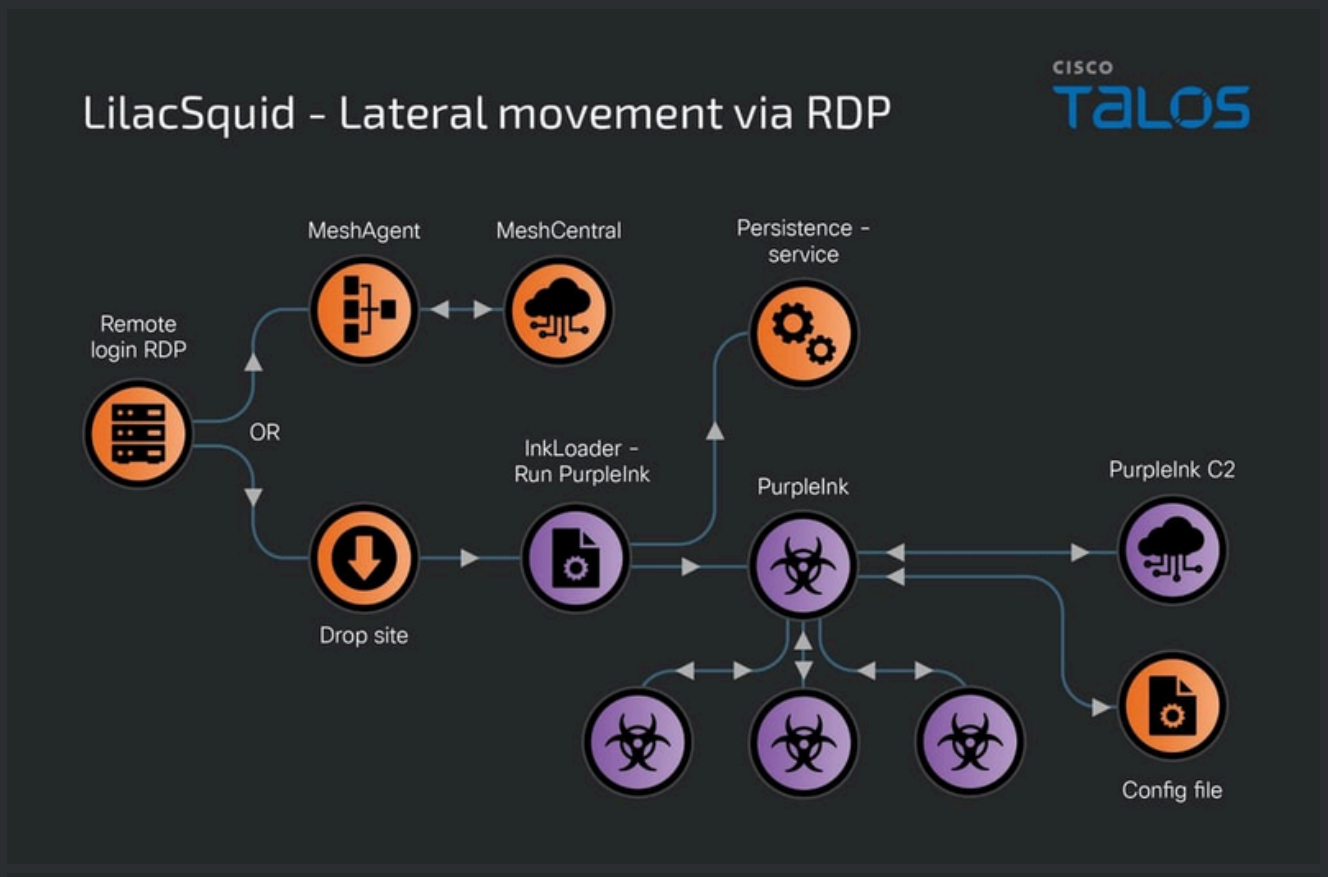
LilacSquid: The stealthy trilogy of PurpleInk, InkBox and InkLoader

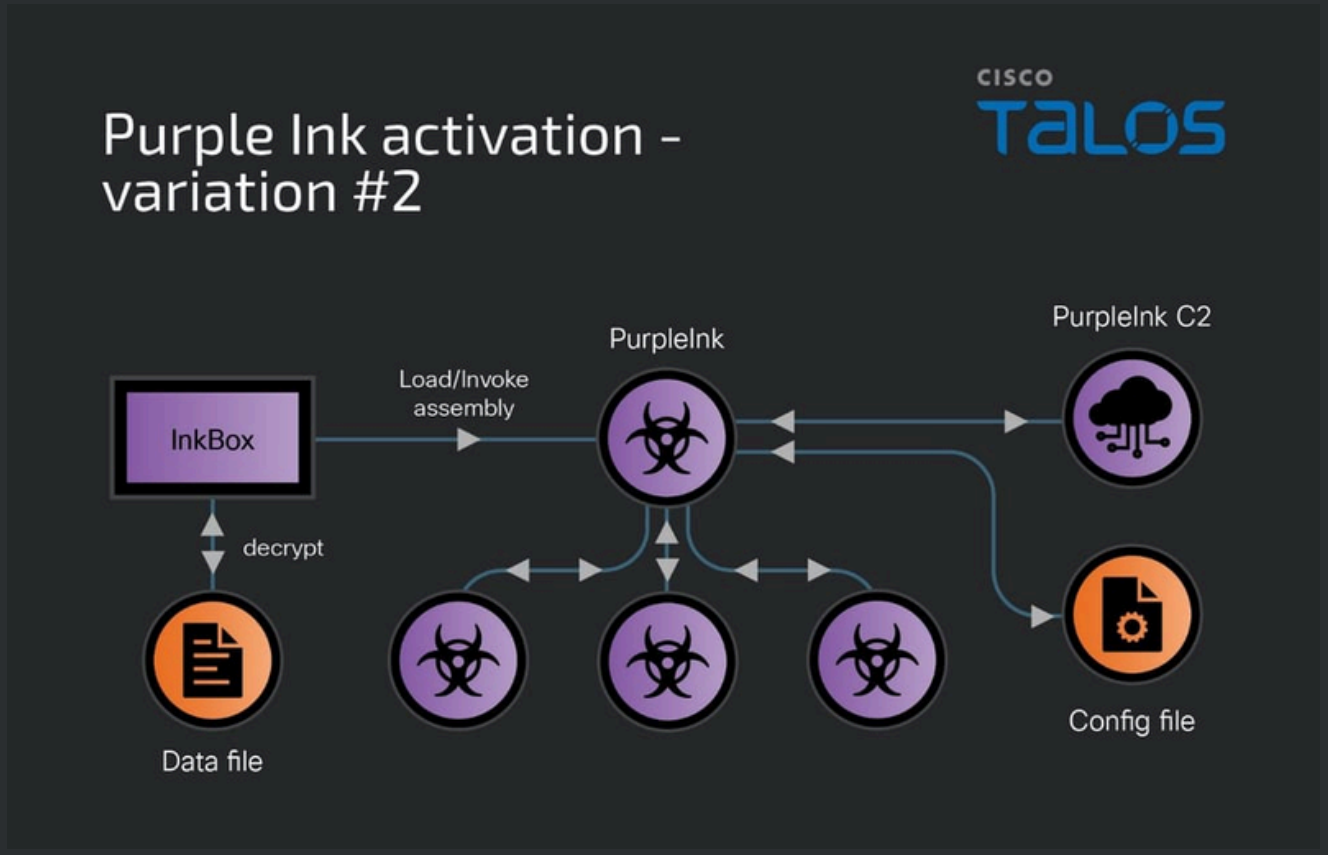


Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cisco Talos
Date: 30 May 2024

LilacSquid: The stealthy trilogy of PurpleInk, InkBox and InkLoader





Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cisco Talos
Date: 30 May 2024

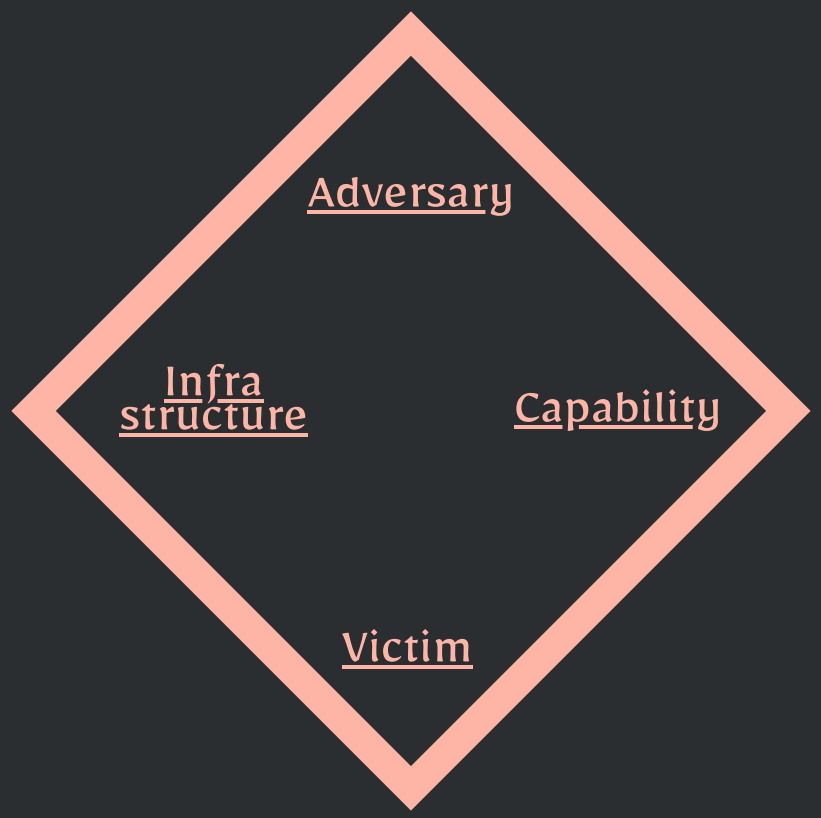
Operation Veles: Decade-Long Espionage Targeting the Global Research and Education Sector

IoC: ☒

MITRE ATT&CK: ☒

Timeline: since at least 2014

UTG-Q-008



- Botnet (inclined to believe that the botnet is of an outsourced or cooperative nature)
- (Botnet): AU, BG, BE, DE, RU, FR, CO, KR, NL, LU, RO, MY, US, ZA, SE, SA, TH, SG, IR, IL, IN, ID, UK, CN

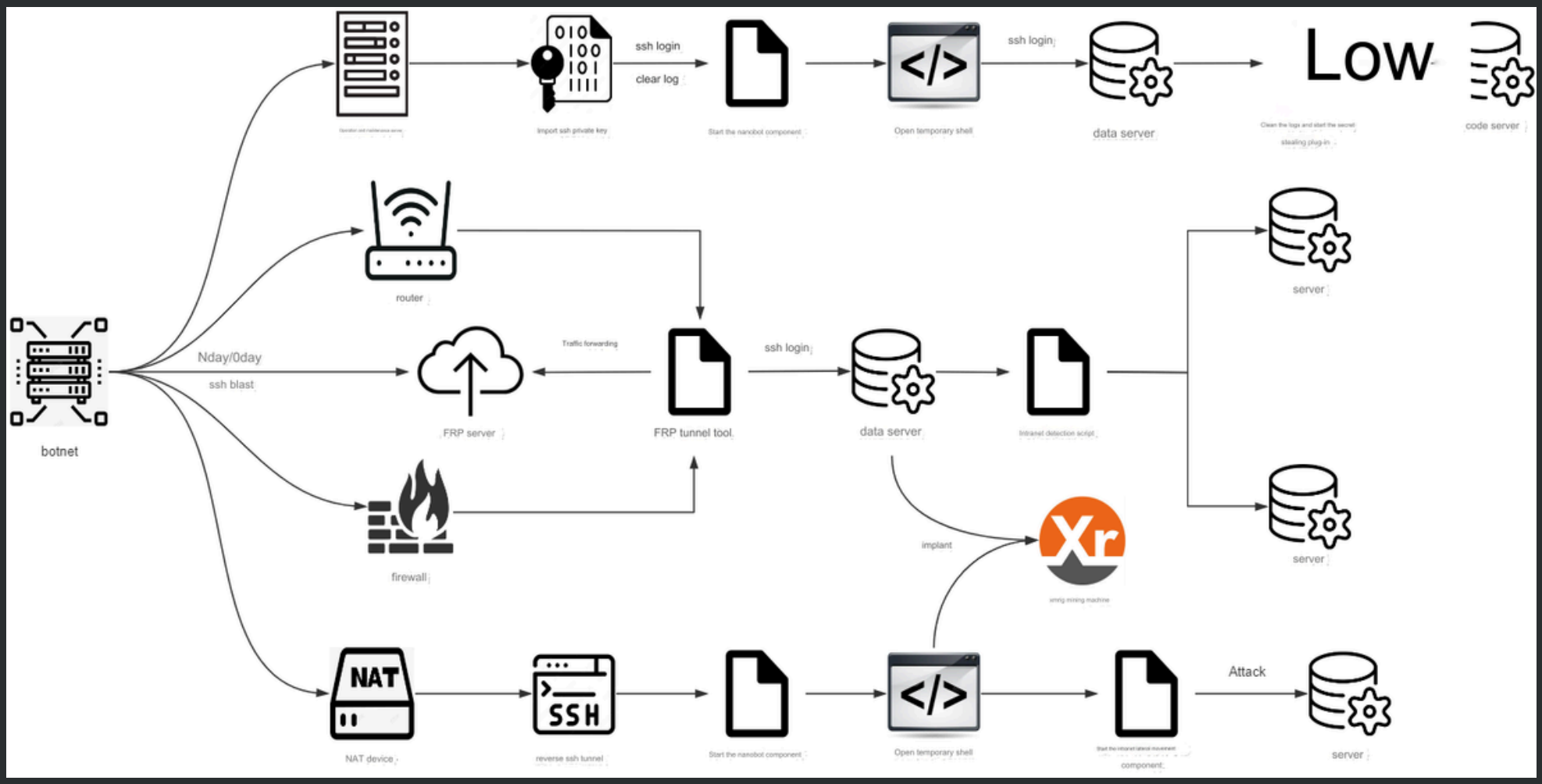
- Nanobot
- T1584.005 Botnet
- T1595 Active Scanning
- T1110 Brute Force
- T1105 Ingress Tool Transfer
- T1059.006 Python
- T1059.004 Unix Shell
- T1046 Network Service Discovery
- T1021.004 SSH
- T1567.001 Exfiltration to Code Repository
- T1090 Proxy
- xmrig
- T1496 Resource Hijacking

Potential Motivation: Espionage
Focus: Linux Systems
Sector: Research & Education
Target: CN, US

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: QiAnXin
Date: 4 June 2024

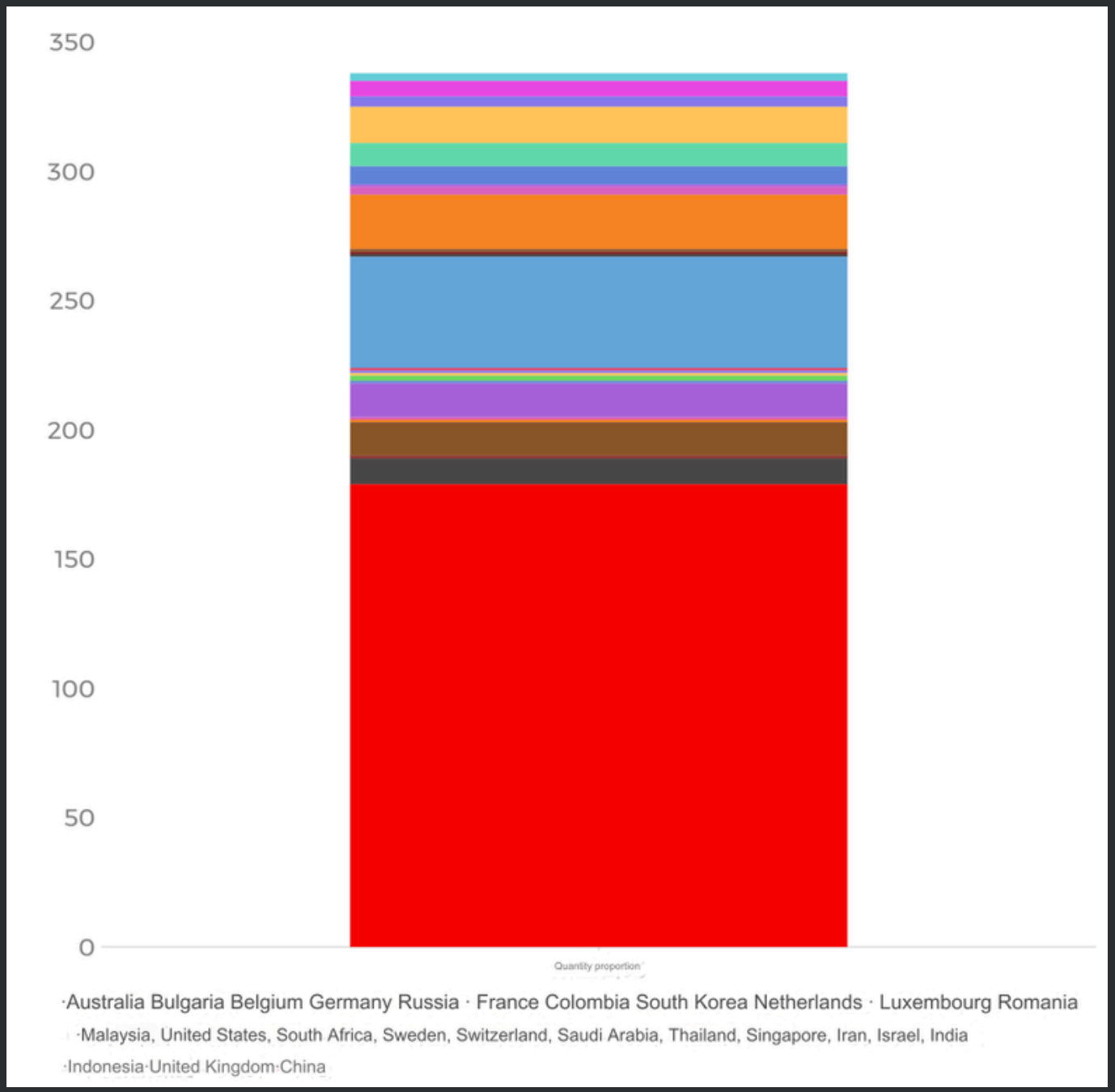
Operation Veles: Decade-Long Espionage Targeting the Global Research and Education Sector



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: QiAnXin
Date: 4 June 2024

Operation Veles: Decade-Long Espionage Targeting the Global Research and Education Sector



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: QiAnXin
Date: 4 June 2024

Operation Crimson Palace: A Technical Deep Dive

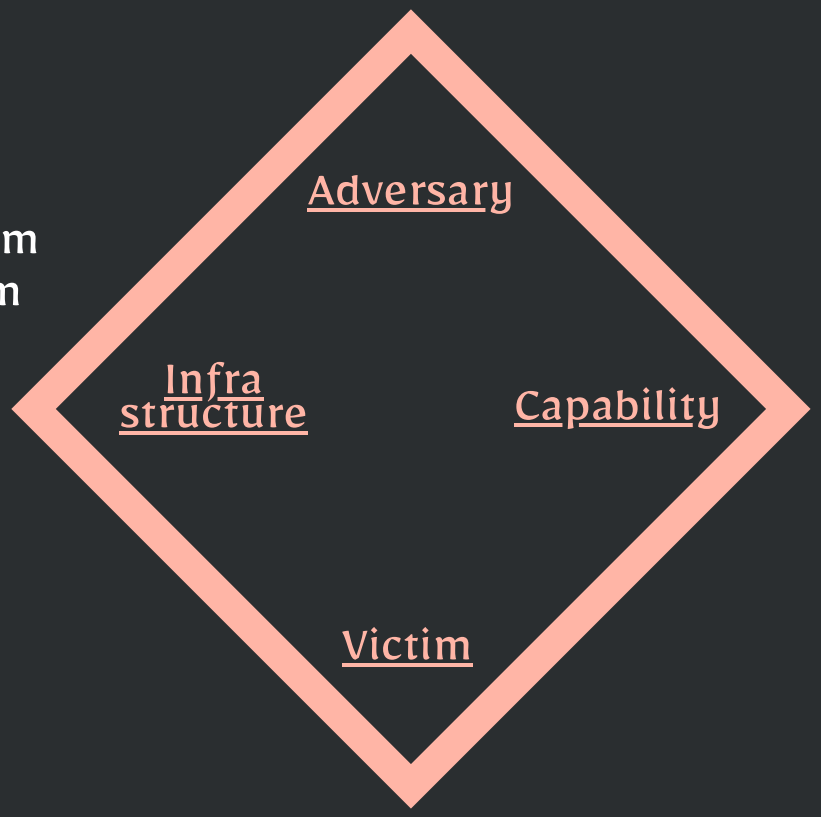
IoC: ✓

MITRE ATT&CK: ✗

Timeline: since at least March 2023

- **Alpha (STAC1248)**
  - **[Overlap - BackdoorDiplomacy]**
- **Bravo (STAC1870)**
  - **[Overlap - Unfading Sea Haze]**
- **Charlie (STAC1305)**
  - **[Overlap - Earth Longzi]**

- cloud.keepasses[.]com
- message.ooguy[.]com
- 198.13.47[.]158
- **64.176.50[.]42**
- **158.247.241[.]188**
- 158.247.241[.]188
- 139.180.217[.]105



- Merlin C2
- RUDEBIRD
- Impersoni-Fake-Ator
- PowHeartBeat
- PHANTOMNET
- EAGERBEE
- CCoreDoor
- PocoProxy
- CobaltStrike
- HUI Loader
- Havoc C2
- T1078 : Valid Accounts
- T1003.001: LSASS Memory
- T1053.005 Scheduled Task

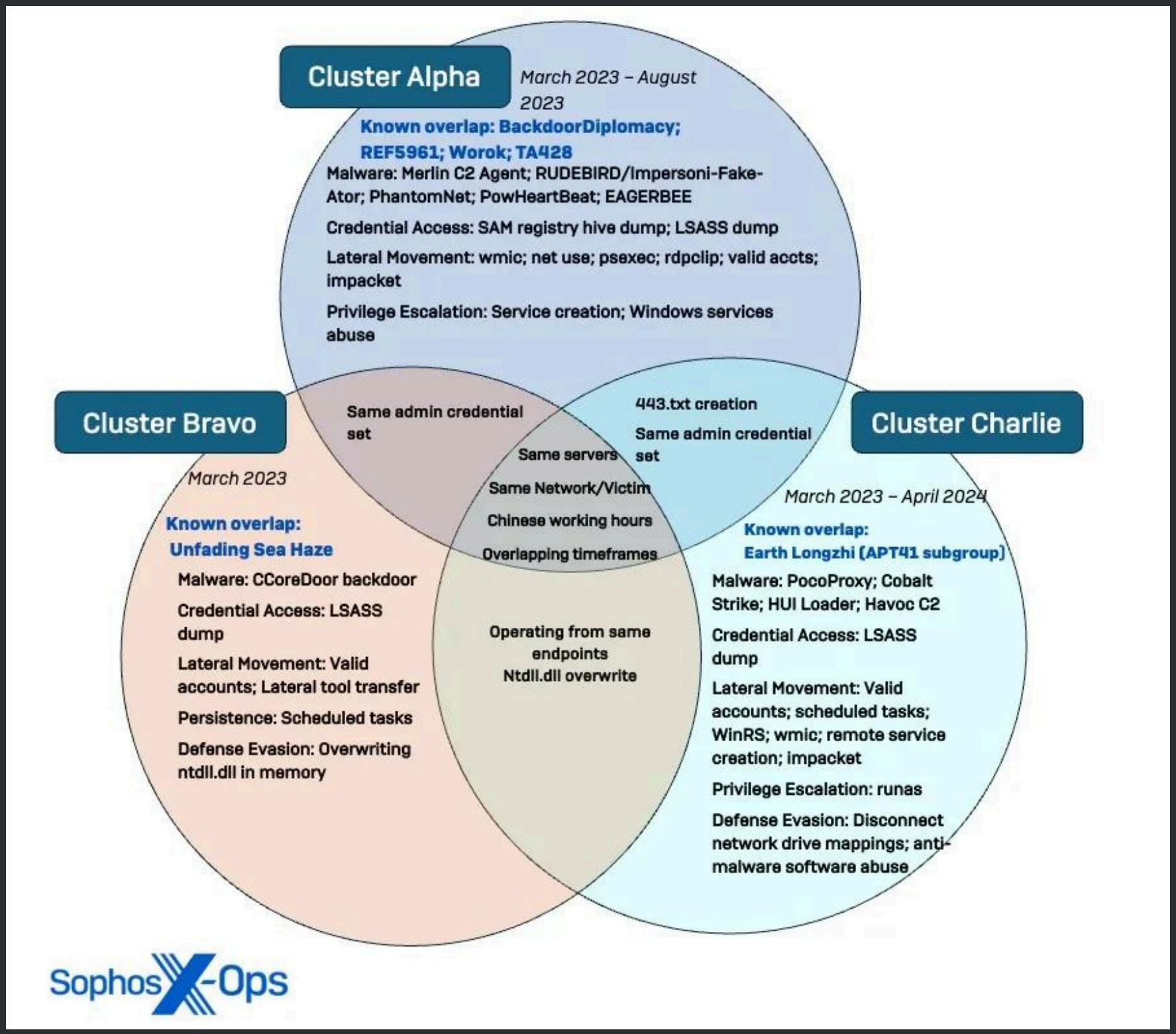
Target: High-profile government organization in Southeast Asia

Potential Motivation: Cyberespionage

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Sophos
Date: 5 June 2024

Operation Crimson Palace: A Technical Deep Dive



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Sophos
Date: 5 June 2024

One By One: Gentleman

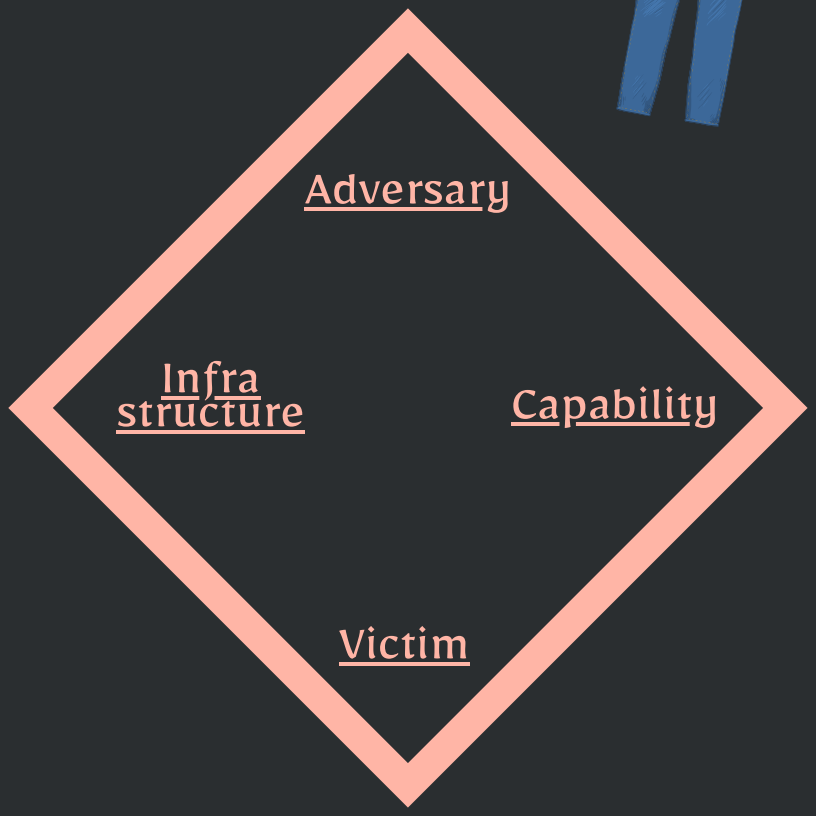
IoC: ☒

MITRE ATT&CK: ☒

Timeline: June 2024

Perspective A

Anne



ATTACK FROM BEHIND

Apek

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: X
Date: 6 June 2024

One By One: Gentleman

IoC: ☒

MITRE ATT&CK: ☒

Timeline: June 2024

Perspective B

Apek

Adversary

Infra structure

Capability

Victim

ONE BY ONE GENTLEMAN OKAY MARI!

Anne

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: X
Date: 6 June 2024

Motif dan Modus Operandi DragonForce Malaysia

IoC: ☒

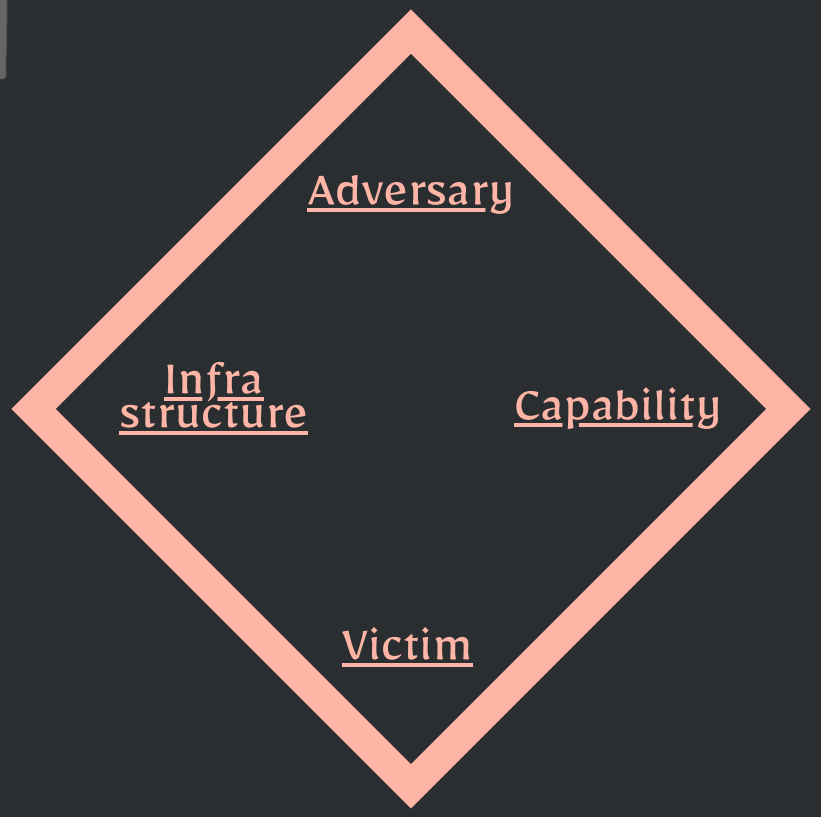
MITRE ATT&CK: ☒

Timeline: since at least 2012

Special note:
DFM stated that they are **not affiliated** with the DragonForce Ransomware or any ransomware activities

DragonForce Malaysia

- **ENIGMA**
- **URSA**
- **PROP**



- dragonforce[.]io

- T1585.001 Establish Accounts: Social Media Accounts
- T1498 : Network Denial of Service
- T1491 : Defacement
- T1588.006 Obtain Capabilities: Vulnerabilities

Targets:

- **Entities affiliated with Israel**
- **Entities against Malaysia**

Motivation: Hacktivism

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: DragonForce Malaysia
Date: 9 June 2024

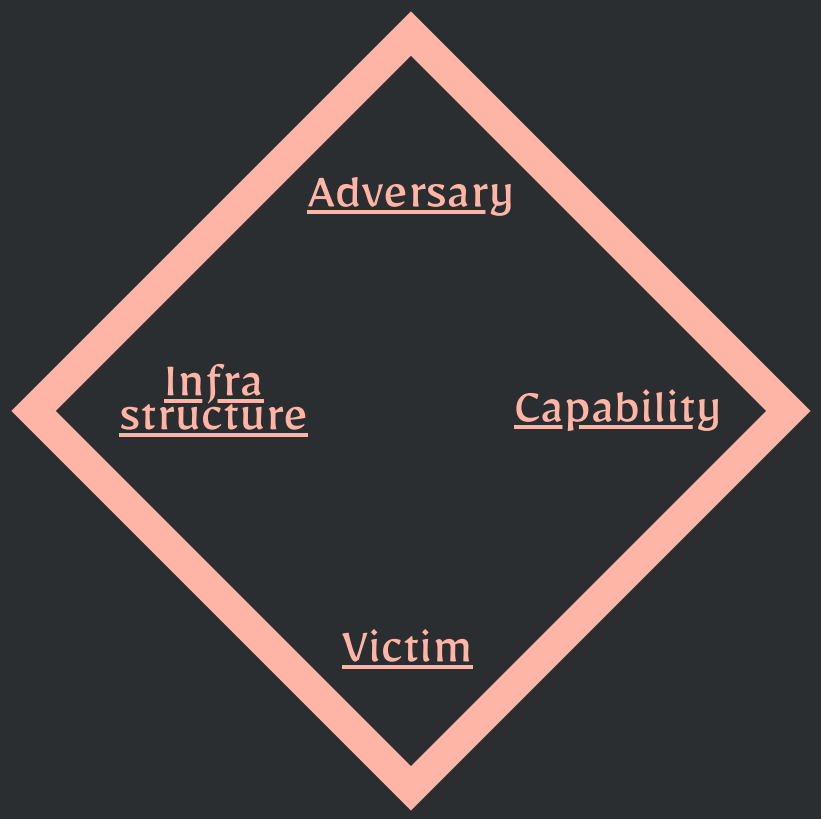
CVE-2024-4577 in PHP Actively Exploited by TellYouThePass Ransomware

IoC: ✓

MITRE ATT&CK: ✗

Timeline: as early as June 8, 2024

- **TellYouThePass**
- **service@cyberkiller.xyz**
- **BTC address: bc1qnuxx83nd4keeegrum tnu8kup8g02yzgff6z53l**



- **hxxp://88.218.76[.]13/dd3.hta**
- **C2 IP: 88.218.76[.]13**

- **Critical PHP vulnerability: CVE-2024-4577**
- **TellYouThePass Ransomware**
- T1190 : Exploit Public-Facing Application
- T1218.005: Mshta
- T1059.005: Visual Basic

Target:
Businesses and individuals

1 victim from Malaysia identified in Censys Dashboard

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: SOCRadar, Imperva & Censys
Date: 10, 11 June 2024

CVE-2024-4577 in PHP Actively Exploited by TellYouThePass Ransomware

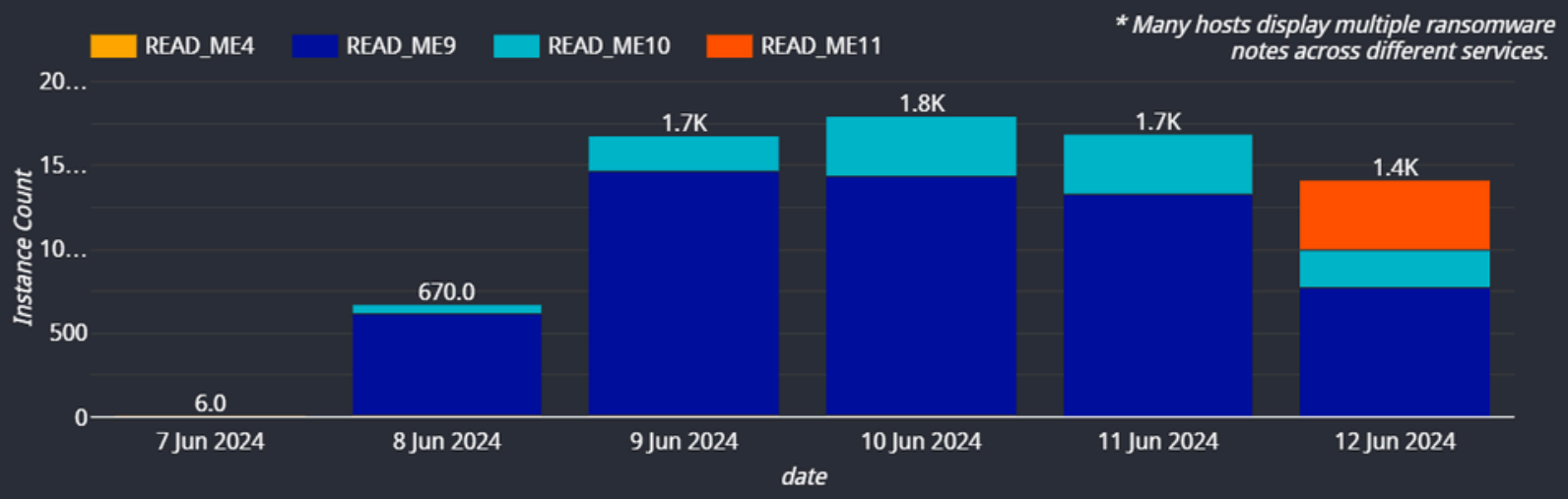
Infection Trends and Observed Ransom Notes

Total Distinct Infected Hosts Online

1,321

Change in # Infected Hosts Online Since Yesterday

-351



Autonomous System	Hosts
TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	329
HINET Data Communication Business Group	222
ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd.	140
ERX-TANET-ASN1 Taiwan Academic Network TANet Information Center	90
CHINANET-BACKBONE No.31,Jin-rong Street	64
HWCSNET Huawei Cloud Service data center	40
CHINA169-BACKBONE CHINA UNICOM China169	27

1 - 50 / 139

Country	Hosts
United States	15
Singapore	4
Thailand	1
Vietnam	1
Finland	1
Philippines	1
Germany	1
Malaysia	1

1 - 12 / 12

Detected PHP Ver...	Hosts
null	1,321
1.1.1	725
1.0.2	266
3.1.3	151
2.4.58	151
2.4.54	137
8.2.12	114
2.4.56	101

1 - 100 / 253

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: SOCRadar, Imperva & Censys
Date: 10, 11 June 2024

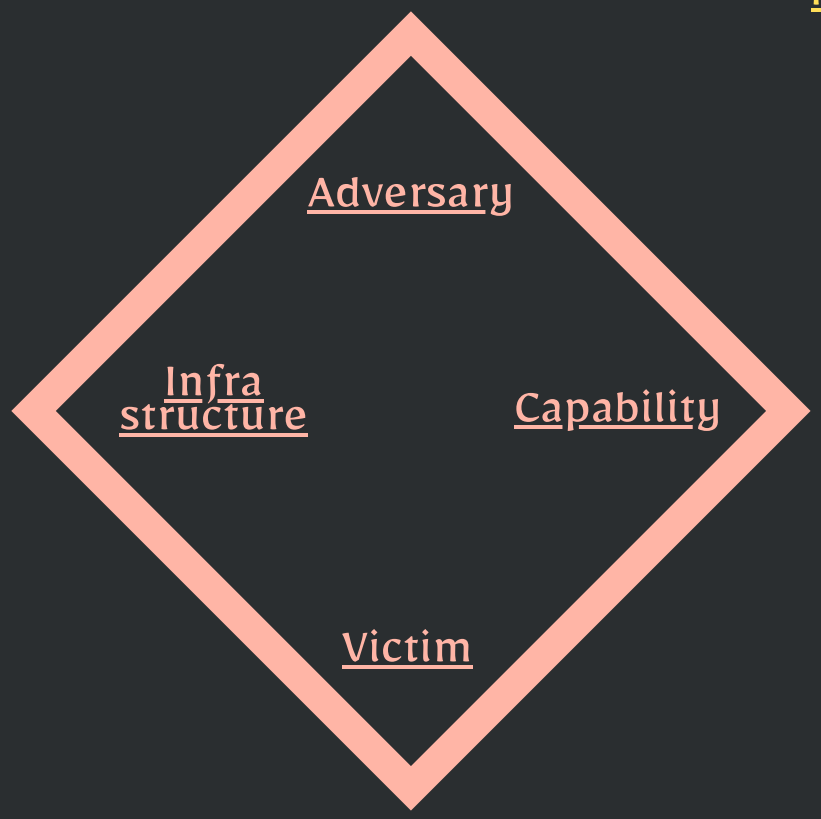
Noodle RAT: Reviewing the New Backdoor Used by Chinese-Speaking Groups

IoC: ☒

MITRE ATT&CK: ☒

Timeline: since at least March 2018

- **Chinese-speaking groups**
- **Iron Tiger**
- **Calypso APT**
- **unknown cluster**



Potential Motivation:
Cyberespionage and cybercrime

Target:
Thailand (2020)
India (2020)
Japan (2022)
Malaysia (2023)
Taiwan (2023)

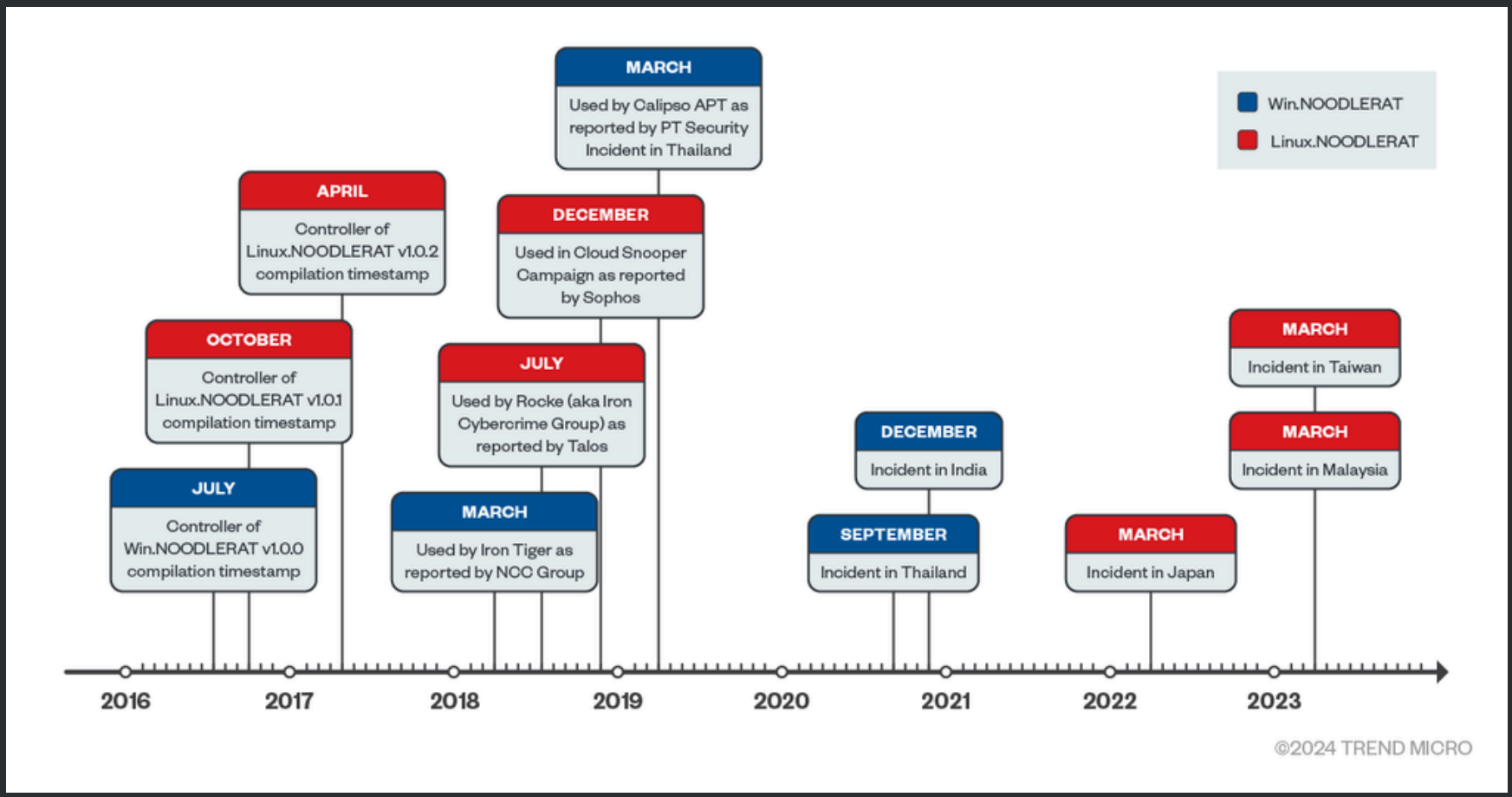
Noodle RAT

- **Win.NOODLERAT**
  - **Download and upload files**
  - **Run additional in-memory modules**
  - **Work as TCP proxy**
- **Linux.NOODLERAT**
  - **Reverse shell**
  - **Download & Upload files**
  - **Scheduling execution**
  - **SOCKS tunneling**

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 11 June 2024

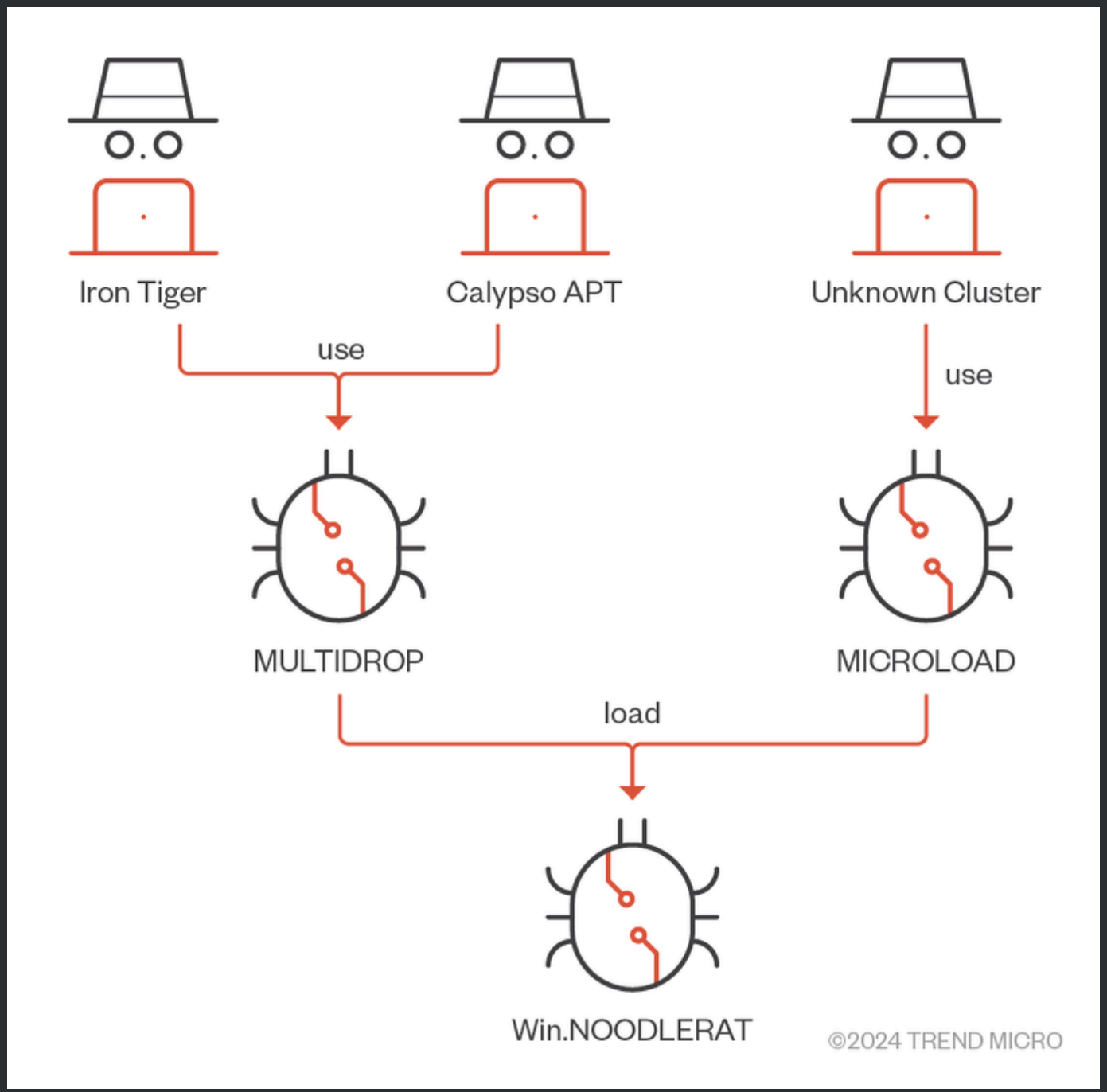
Noodle RAT: Reviewing the New Backdoor Used by Chinese-Speaking Groups



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 11 June 2024

Noodle RAT: Reviewing the New Backdoor Used by Chinese-Speaking Groups



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 11 June 2024

Profile: Lizard Squad

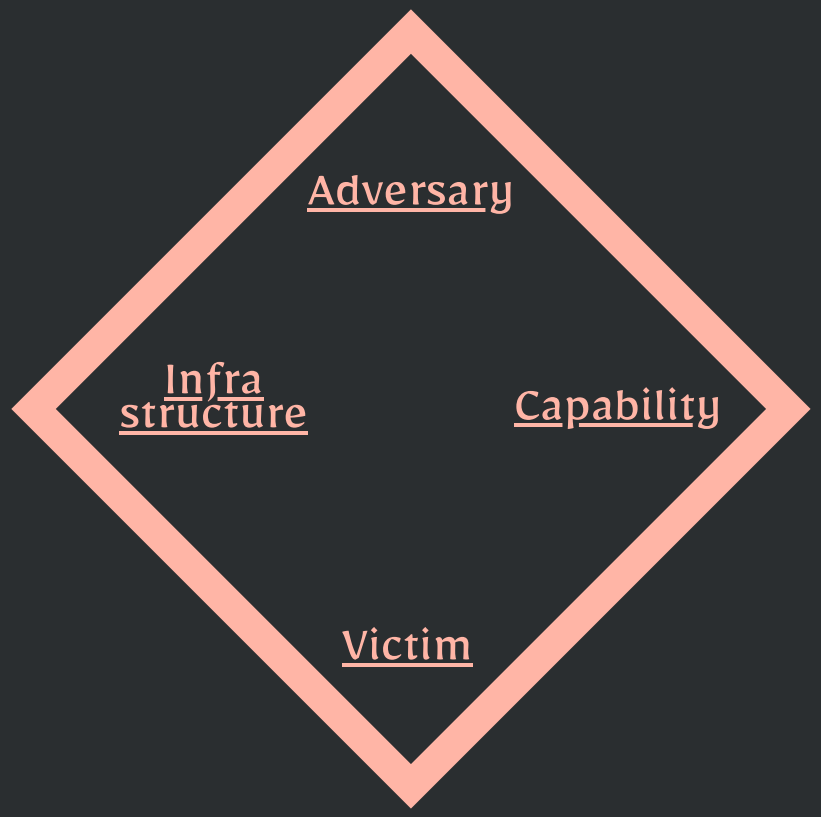
IoC: ☒

MITRE ATT&CK: ☒

Timeline: 2014 - 2015

Lizard Squad

- **Julius “zeekill” Kivimäki: A Finnish teenager who was convicted of multiple cybercrimes.**
- **Vinnie Omari: A British teenager arrested in connection with the 2014 attacks.**



- T1498 : Network Denial of Service
- T1585.001 Establish Accounts: Social Media Accounts

- **Sony PlayStation Network and Xbox Live Attacks (2014)**
- **Malaysia Airlines Website Defacement (2015)**
- **Twitch Attack (2014)**

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: @threatscapechronicles
Date: 15 June 2024

Cloaked and Covert: Uncovering UNC3886 Espionage Operations

IoC: ✓

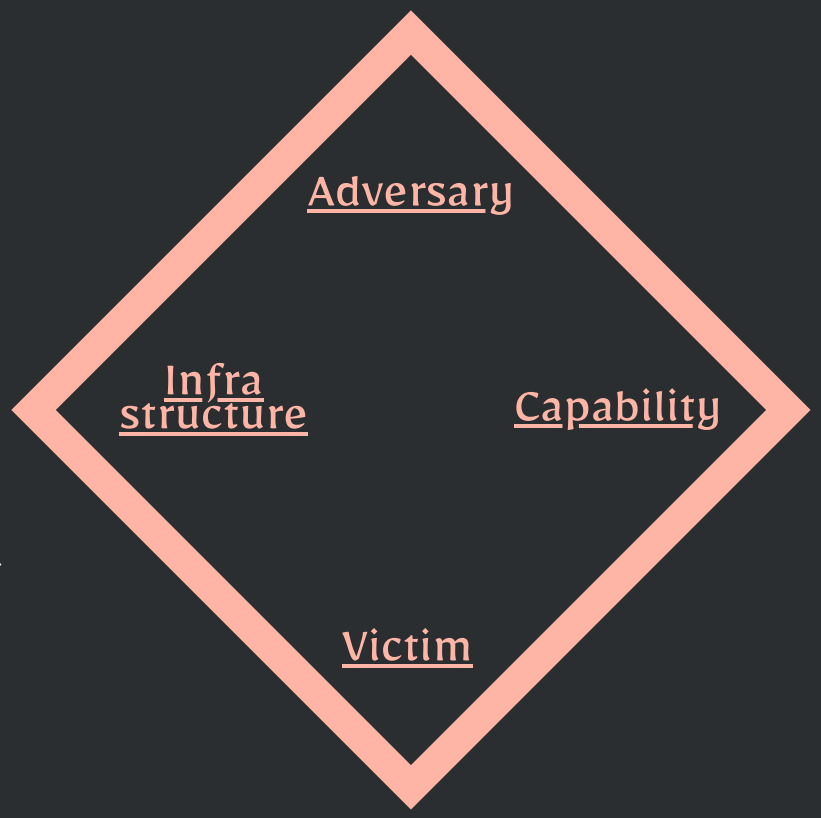
MITRE ATT&CK: ✗

Timeline:
Campaign 23-022: Since March 23
Active: since at least late 2021

UNC3886:

- **a suspected China-nexus cyber espionage actor**

- Trusted Third Parties as C2 Channel (GitHub, Google Drive)
- Netblocks:
  - Alibaba
  - Choopa, LLC
  - Gigabit Hosting Sdn Bhd
  - HKBN Enterprise Solutions Limited
  - Ucloud Information Technology Hk Limited



- Zero-Day Exploitation
- CVE-2023-34048
- CVE-2022-41328
- CVE-2022-22948
- CVE-2023-20867
- T1190 : Exploit Public-Facing Application
- T1078 : Valid Accounts
- T1584.006 Web Services
- THINCRUST backdoor
- CASTLETAP backdoor
- DRIEDMOAT
- REPTILE rootkit
- LOOKOVER sniffer
- MOPSLED backdoor
- RIFLESPINE backdoor
- VIRTUALPITA backdoor
- VIRTUALPIE backdoor

Identified Targets:

- North America, Southeast Asia, Oceania regions.

Additional Victims:

- Europe, Africa, and other parts of Asia.

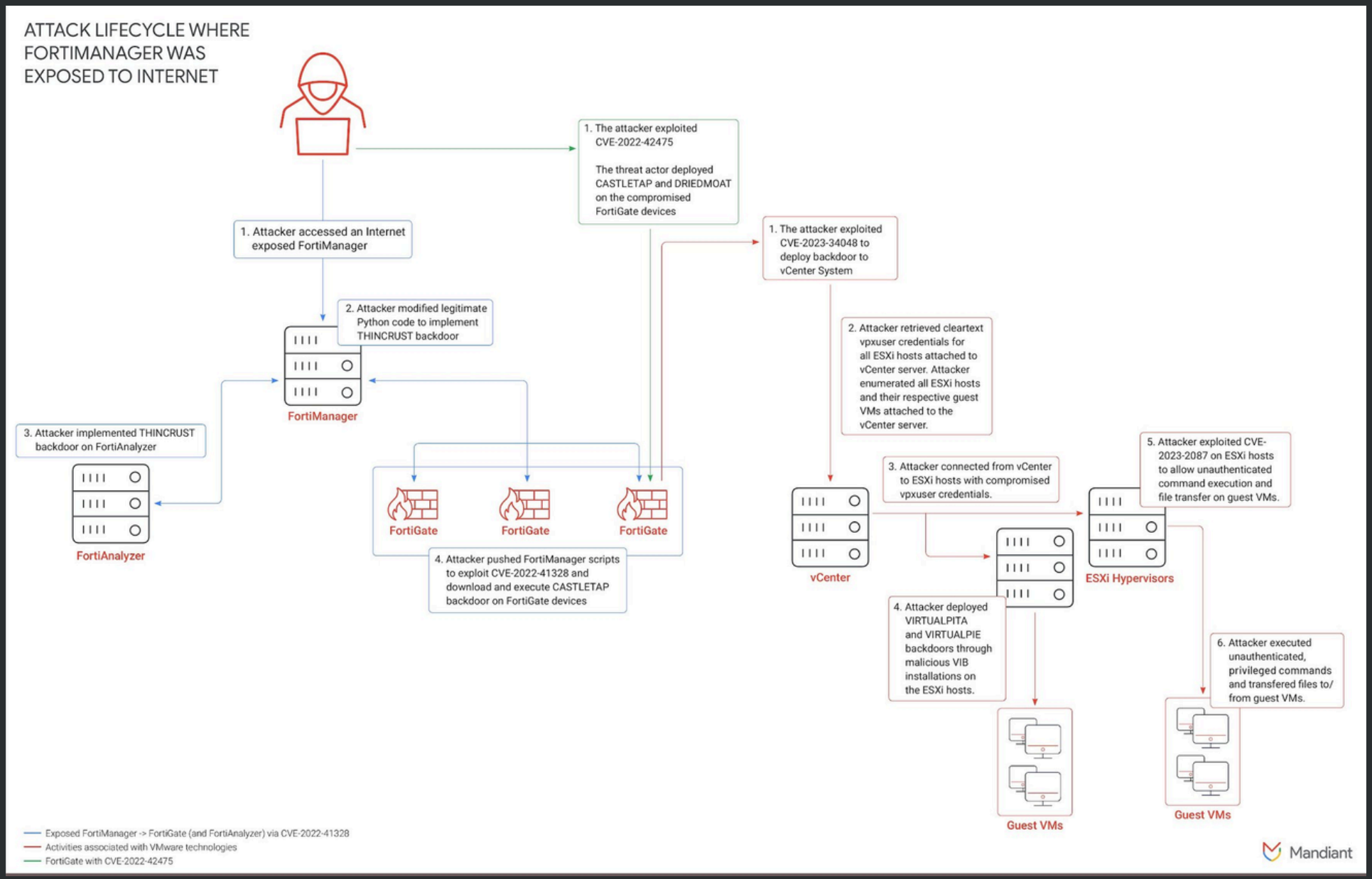
Sectors:

Governments, telecommunications, technology, aerospace and defense, and energy and utility sectors

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Mandiant (Google)
Date: 19 June 2024

Cloaked and Covert: Uncovering UNC3886 Espionage Operations



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Mandiant (Google)
Date: 19 June 2024

Sustained Campaign Using Chinese Espionage Tools Targets Telcos

IoC: ✓

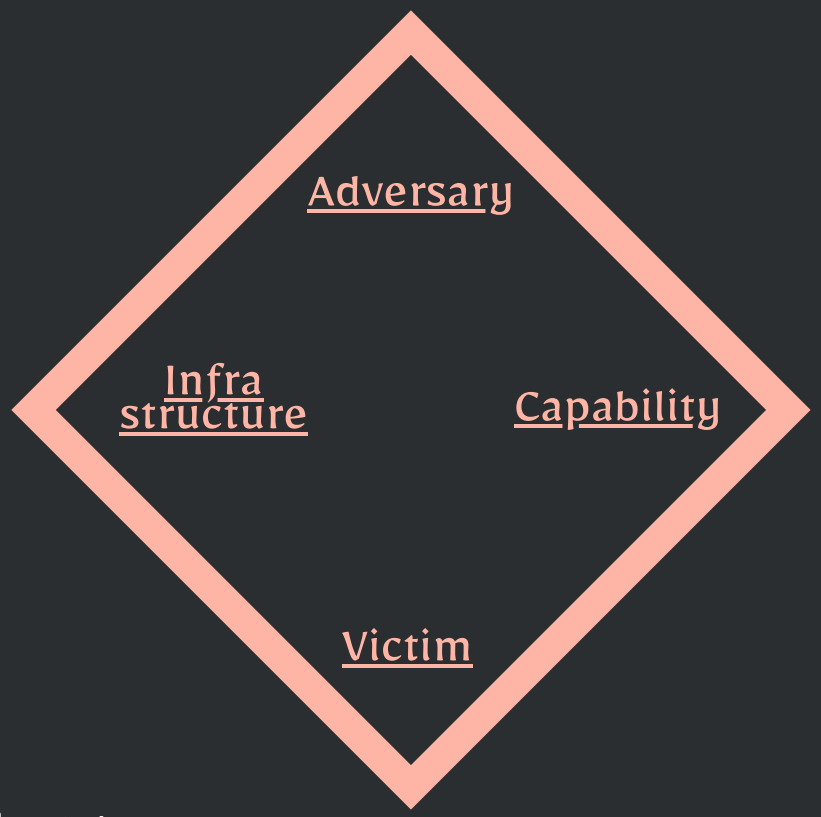
MITRE ATT&CK: ✗

Timeline: since at least 2021

Possible attribution:

- **Attacks by multiple actors, acting independently of one another.**
- **A single actor using tools and/or personnel acquired from or shared by other groups.**
- **Multiple actors collaborating in a single campaign.**

- swiftandfast[.]net
- 39.84.163[.]162
- 14.161.4[.]152
- 142.93.223[.]200
- 146.190.18[.]167
- 143.110.250[.]11
- 143.110.244[.]132
- 159.65.158[.]28
- 159.89.170[.]164
- 157.245.107[.]16
- 65.20.66[.]128
- 49.204.77[.]162
- ....



- Tools associated with Chinese espionage groups
- Coolclient backdoor
- Quickheal backdoor
- Rainyday backdoor
- Keylogging malware, possibly custom-developed
- Port scanning: At least three distinct port-scanning tools were deployed
- Credential theft through the dumping of registry hives
- Responder
- Enabling RDP

Targets:

- **Multiple telecom operators in a single Asian country**
- **1 services company that serves the telecoms sector and a university in another Asian country**

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Symantec
Date: 20 June 2024

Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation

IoC: ☑

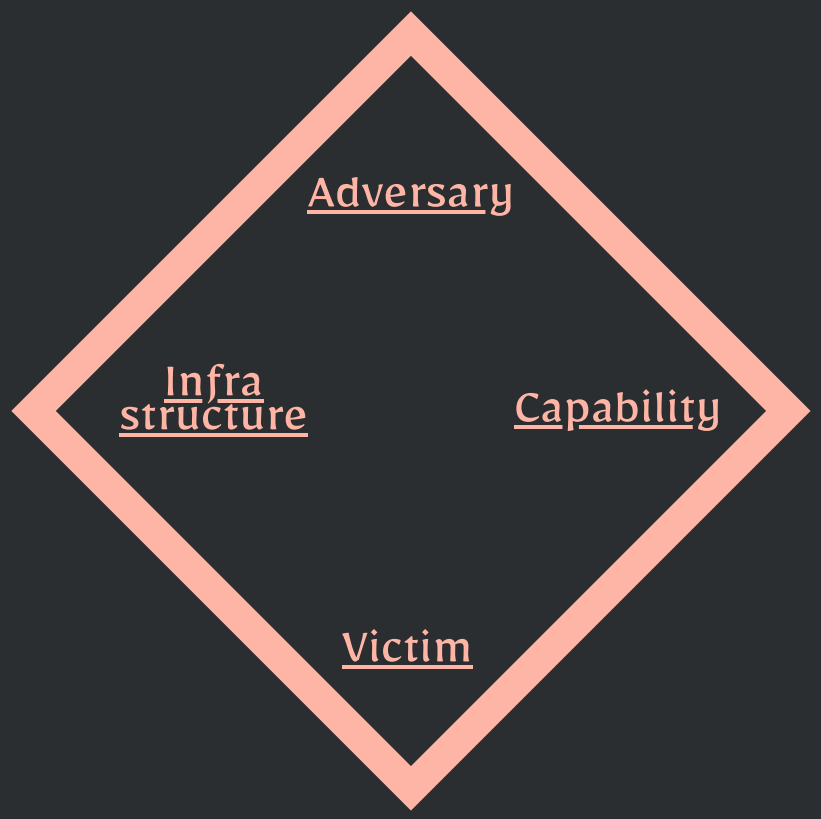
MITRE ATT&CK: ☑

Timeline:
Main: Nov 23 - Apr 24
Active: since at least mid 2021

RedJuliett:

- **likely Chinese state-sponsored group**

- cktime.ooguy[.]com
- www.sofeter[.]ml
- www.dns361[.]tk
- 38.147.190[.]192
- 61.238.103[.]155
- 122.10.89[.]230
- 137.220.36[.]87
- 140.120.98[.]115
- 154.197.98[.]3
- 154.197.99[.]202
- 176.119.150[.]92
- TA controlled VPS
- Compromised infra
- ....



- T1583.003 Virtual Private Server
- T154 Compromise Infrastructure: Server
- T595.002 Vulnerability Scanning
- T1190 Exploit Public-Facing Application
- T1133 External Remote Services
- T1505.003 Web Shell
- T1068 Exploitation for Privilege Escalation
- devilzShell
- AntSword
- DirtyCow (CVE-2016-5195)

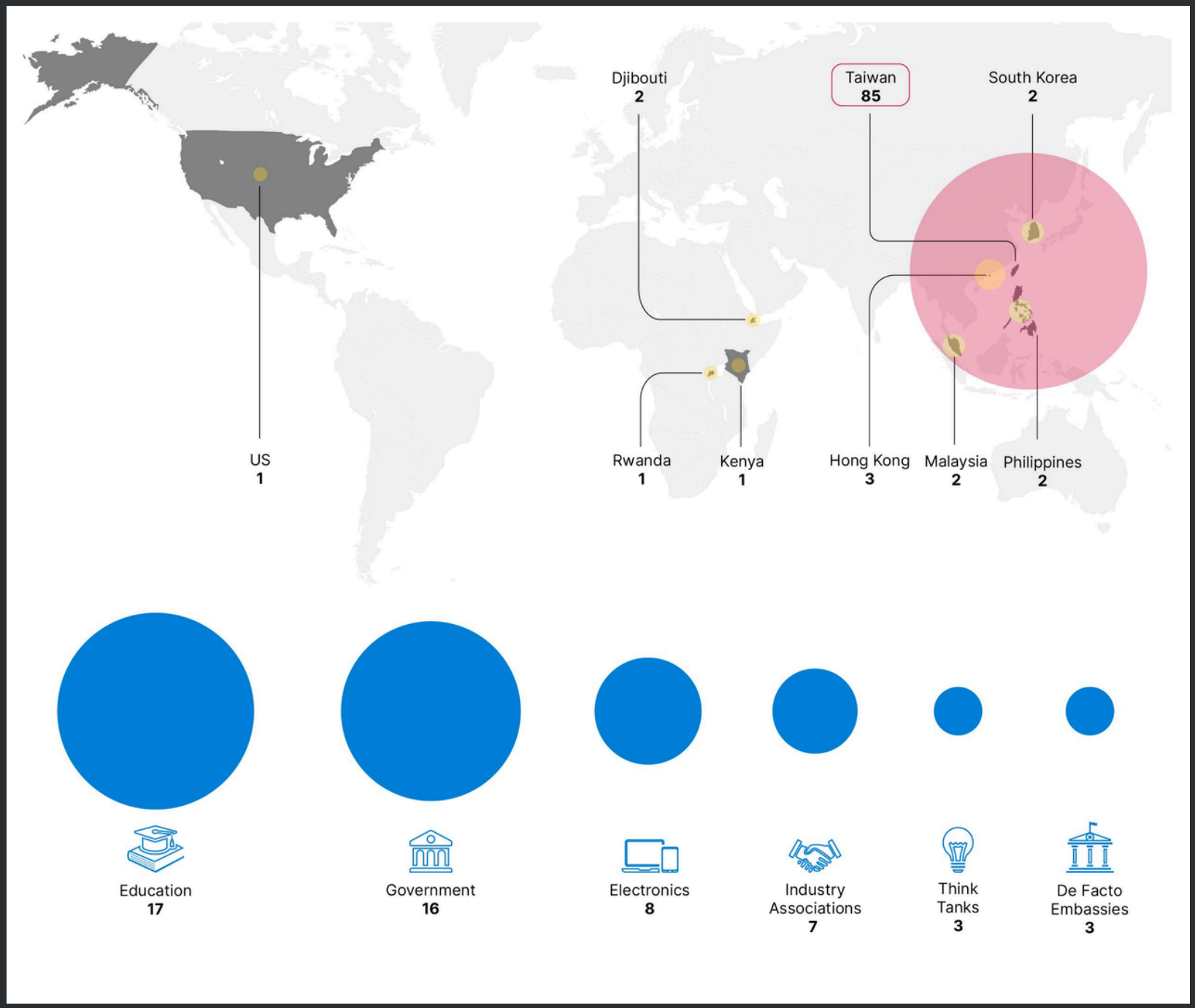
Targets/Victims:

- Taiwan(85 - predominantly: Gov, Academic, Tech, Diplomatic)
- Hong Kong(3), Malaysia(1 Airline, 1 ???), South Korea(2), Djibouti(2), Philippines(2), Kenya (1), Rwanda(1), US(1), Laos(1),

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Recorded Future
Date: 24 June 2024

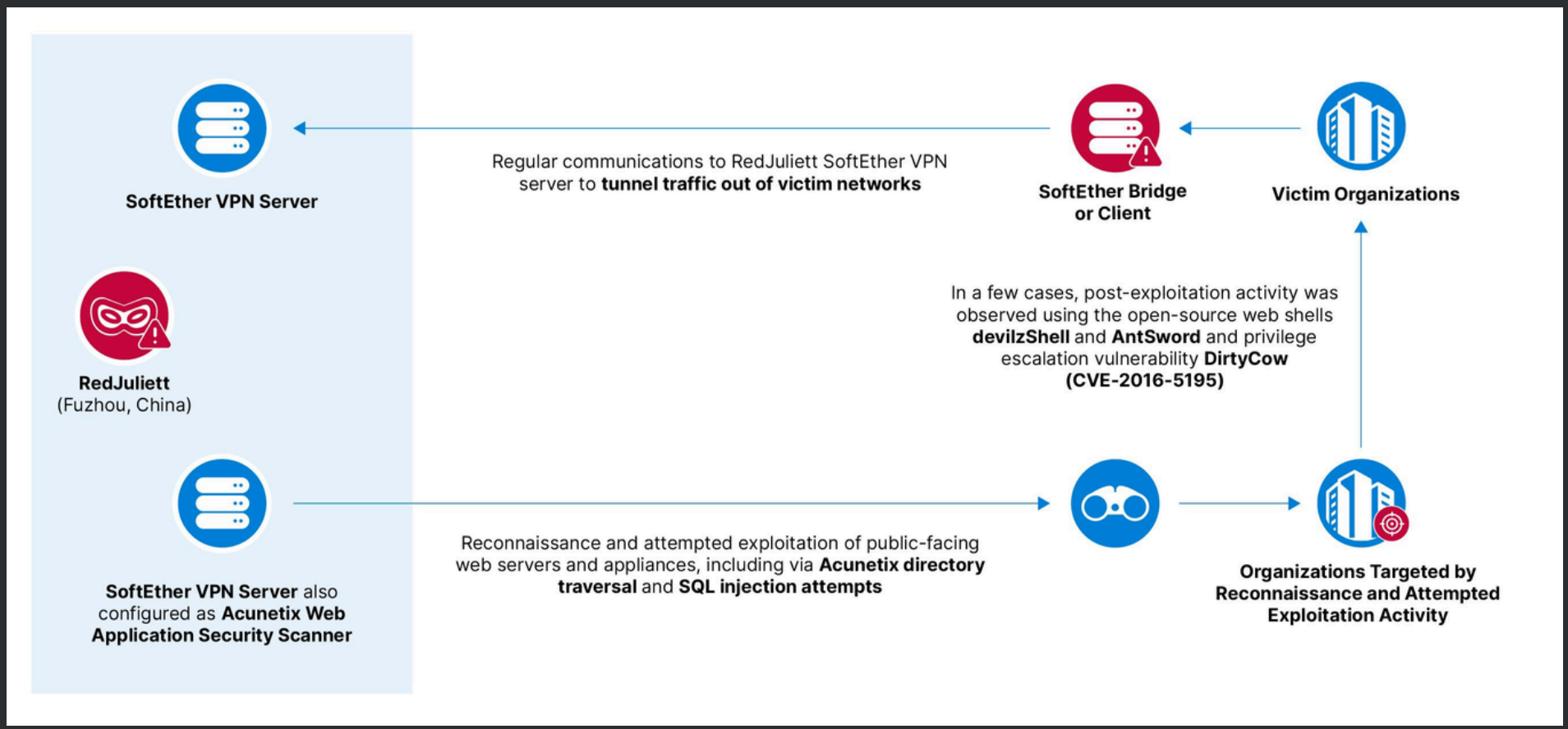
Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Recorded Future
Date: 24 June 2024

Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Recorded Future
Date: 24 June 2024

APT PROFILE – FANCY BEAR

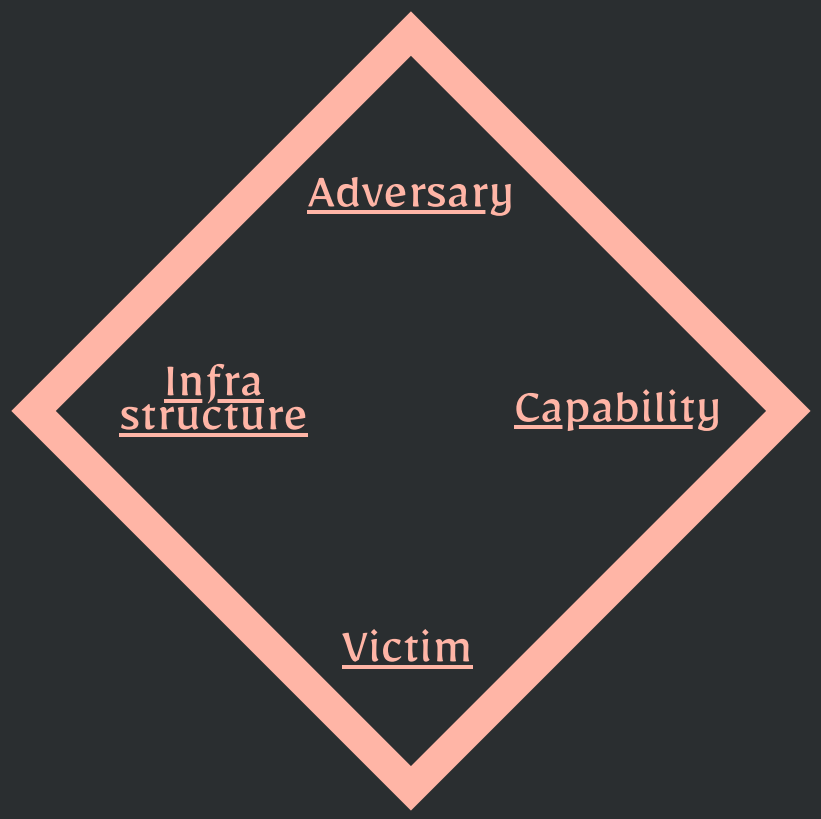
IoC: ☒

MITRE ATT&CK: ☑

Timeline:
Active: since 2007

FANCY BEAR:

- **a notorious Russian cyberespionage group**



- CVE-2024-21412
- CVE-2023-32315
- CVE-2023-38831
- CVE-2023-36025
- CVE-2023-23397
- CVE-2023-27351
- Zebrocy, Sofacy, X-Agent, CHOPSTICK, CORESHELL, JHUHUGIT, ADVSTORESHELL, Drovorub, Skinnyboy
- Utilized Print Spooler vulnerability delivers malware named 'GooseEgg'
- Widespread Password-Spraying
- "search-ms" URI handler to deliver phishing payloads

Targeted countries:
Afghanistan, Brazil, Cambodia, France, Georgia, Germany, India, Indonesia, Kazakhstan, Malaysia, Moldova, Pakistan, Romania, Russia, South Africa, Syria, Thailand, Turkey, Ukraine, United States, Vietnam, and Australia.

Motivation:
Financial Gains, Reputational Damage, Espionage, Political Agenda

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cyfirma
Date: 26 June 2024

APT PROFILE – FANCY BEAR

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cyfirma
Date: 26 June 2024

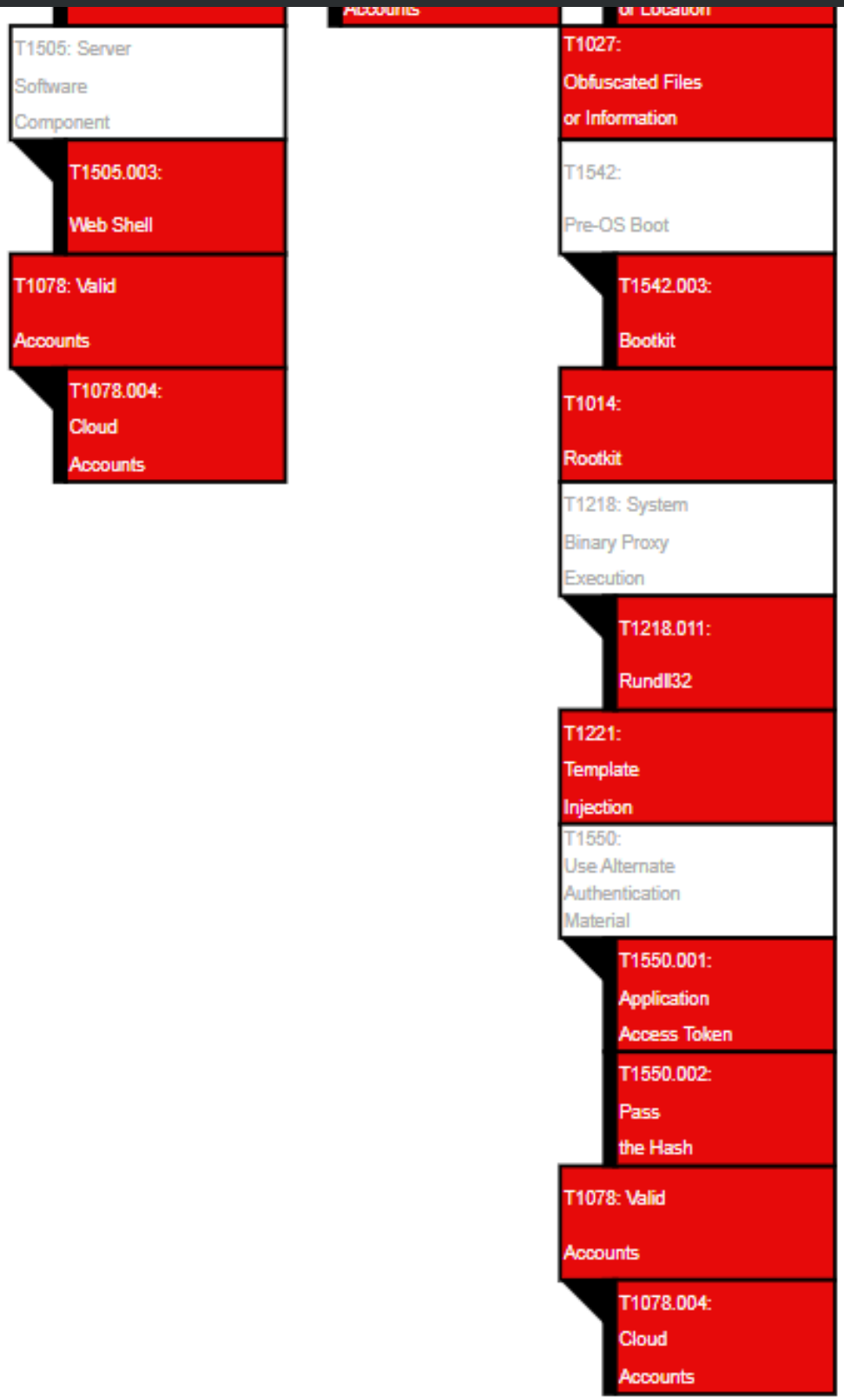
APT PROFILE – FANCY BEAR

T1595: Active Scanning	T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1134: Access Token Manipulation	T1134: Access Token Manipulation
T1595.002: Vulnerability Scanning	T1583.001: Domains	T1190: Exploit Public-Facing Application	T1059.001: PowerShell	T1098.002: Additional Email Delegate Permissions	T1134.001: Token Impersonation/Theft	T1134.001: Token Impersonation/Theft
T1589: Gather Victim Identity Information	T1583.006: Web Services	T1133: External Remote Services	T1059.003: Windows Command Shell	T1547: Boot or Logon Autostart Execution	T1098: Account Manipulation	T1140: Deobfuscate/Decode Files or Information
T1589.001: Credentials	T1588: Compromise Accounts	T1566: Phishing	T1203: Exploitation for Client Execution	T1547.001: Registry Run Keys / Startup Folder	T1098.002: Additional Email Delegate Permissions	T1211: Exploitation for Defense Evasion
T1598: Phishing for Information	T1586.002: Email Accounts	T1566.001: Spearphishing Attachment	T1559: Inter-Process Communication	T1037: Boot or Logon Initialization Scripts	T1547: Boot or Logon Autostart Execution	T1564: Hide Artifacts
T1598.003: Spearphishing Link	T1588: Obtain Capabilities	T1566.002: Spearphishing Link	T1559.002: Dynamic Data Exchange	T1037.001: Logon Script (Windows)	T1547.001: Registry Run Keys / Startup Folder	T1564.001: Hidden Files and Directories
	T1588.002: Tool	T1091: Replication Through Removable Media	T1204: User Execution	T1546: Event Triggered Execution	T1037: Boot or Logon Initialization Scripts	T1564.003: Hidden Window
		T1199: Trusted Relationship	T1204.002: Malicious File	T1546.015: Component Object Model Hijacking	T1037.001: Logon Script (Windows)	T1070: Indicator Removal
		T1078: Valid Accounts	T1204.001: Malicious Link	T1133: External Remote Services	T1546: Event Triggered Execution	T1070.001: Clear Windows Event Logs
		T1078.004: Cloud Accounts		T1137: Office Application Startup	T1546.015: Component Object Model Hijacking	T1070.004: File Deletion
				T1137.002: Office Test	T1068: Exploitation for Privilege Escalation	T1070.006: Timestomp
				T1542: Pre-OS Boot	T1078: Valid Accounts	T1036: Masquerading
				T1542.003: Bootkit	T1078.004: Cloud Accounts	T1036.005: Match Legitimate Name or Location

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cyfirma
Date: 26 June 2024

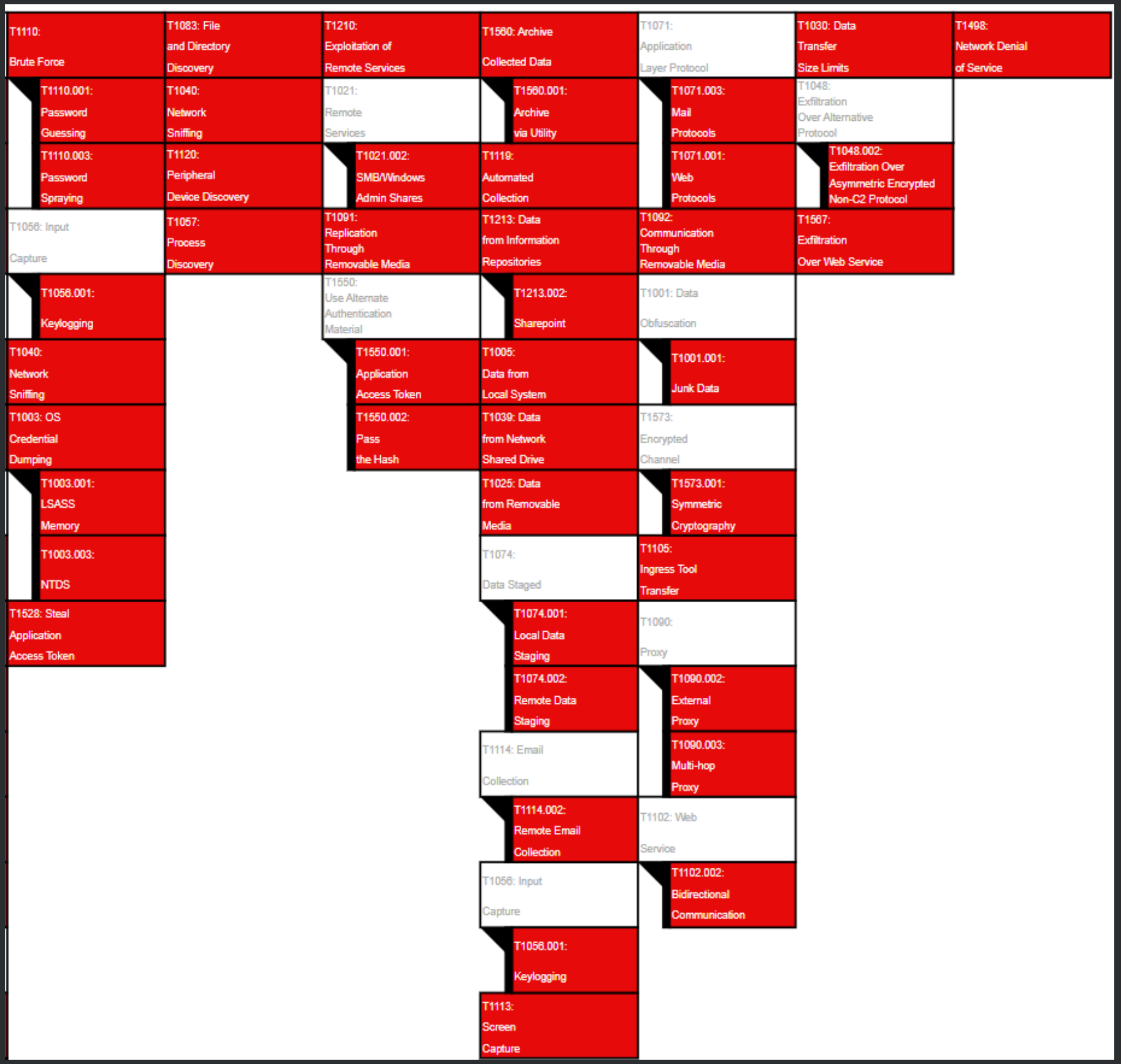
APT PROFILE – FANCY BEAR



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cyfirma
Date: 26 June 2024

APT PROFILE – FANCY BEAR



Twitter/X: @_rectifyq
Tiktok: @rectifyq

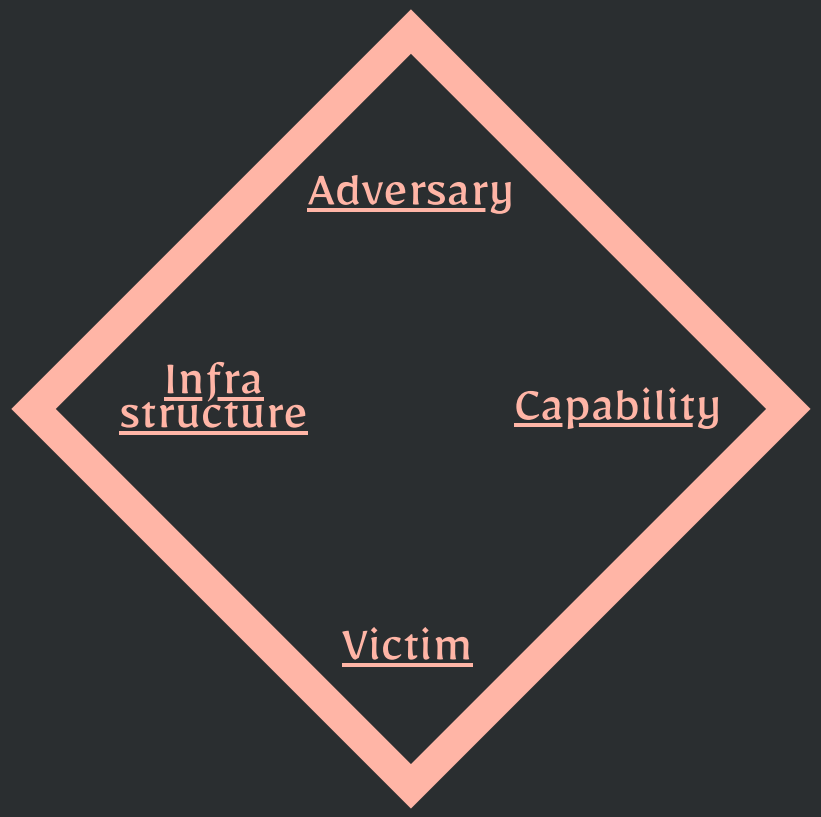
Source: Cyfirma
Date: 26 June 2024

Beware of Snowblind: A new Android malware

IoC: ☒

MITRE ATT&CK: ☒

Timeline:
Early 2024



- Linux kernel feature seccomp

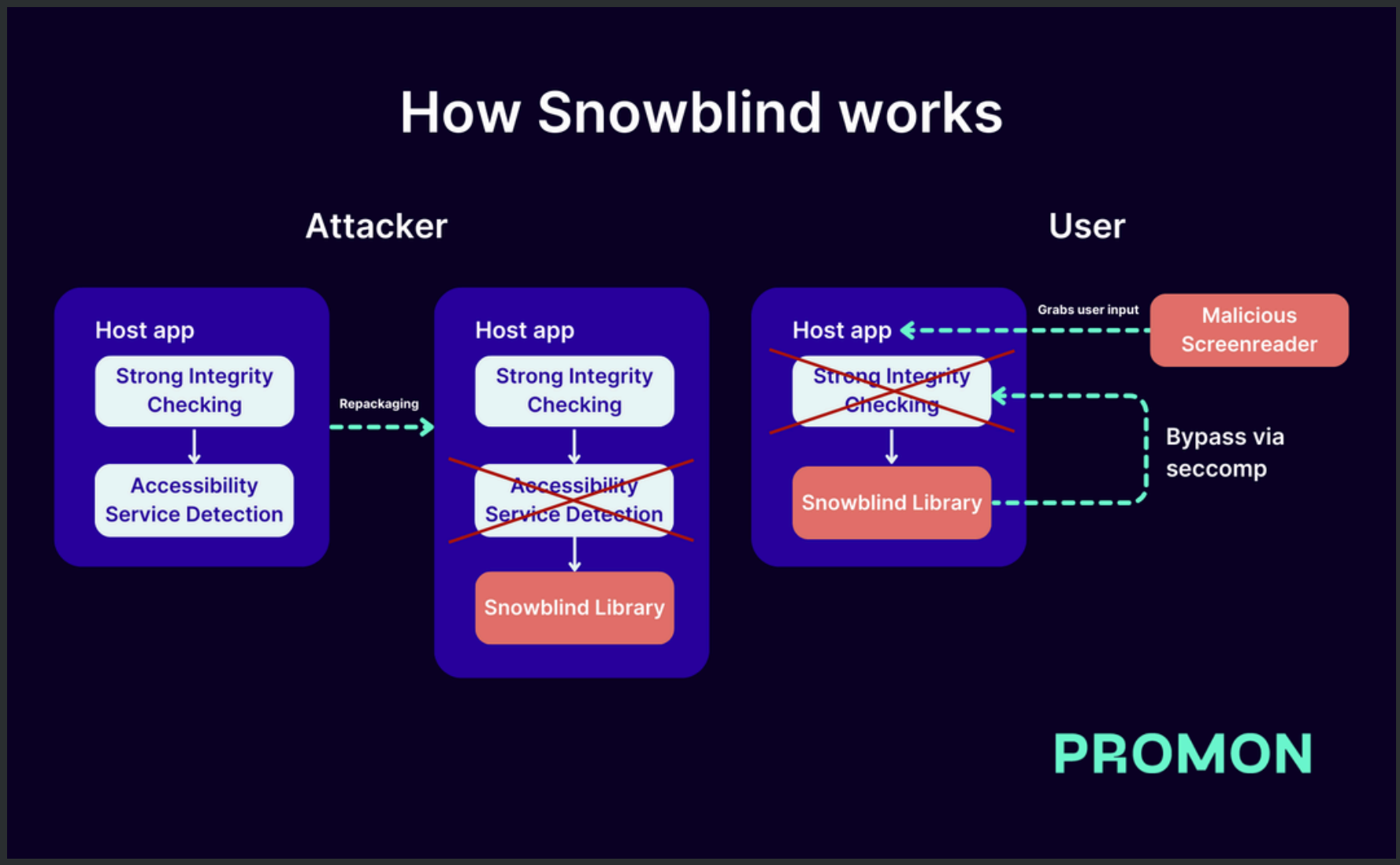
- Android banking trojan: Snowblind
- Attack Android apps based on the Linux kernel feature seccomp
- Bypass strong anti-tampering mechanisms like repackage detection

Targeting banks in Southeast Asia

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Promon
Date: 26 June 2024

Beware of Snowblind: A new Android malware



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Promon
Date: 26 June 2024

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action

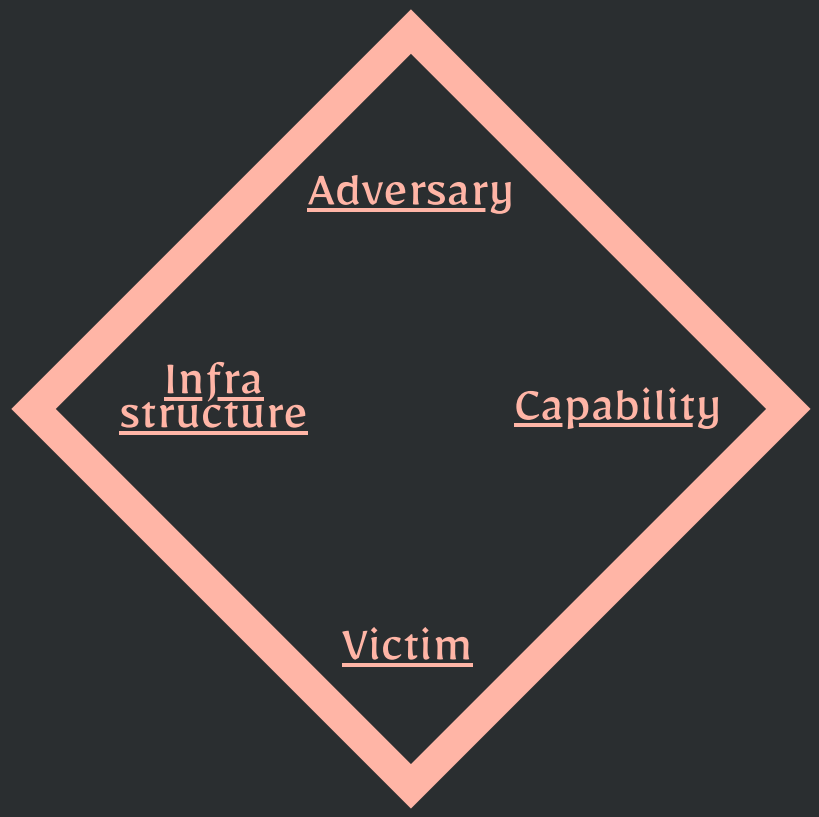
IoC: ✓

MITRE ATT&CK: ✓

Timeline:
Case Study 1: July - Sept 2022
Case Study 2: April 2022

APT40

The authoring agencies assess that this group conduct malicious cyber operations for the PRC Ministry of State Security (MSS)



Australian organisations
(previously targeted organizations in various countries, including AU & US)

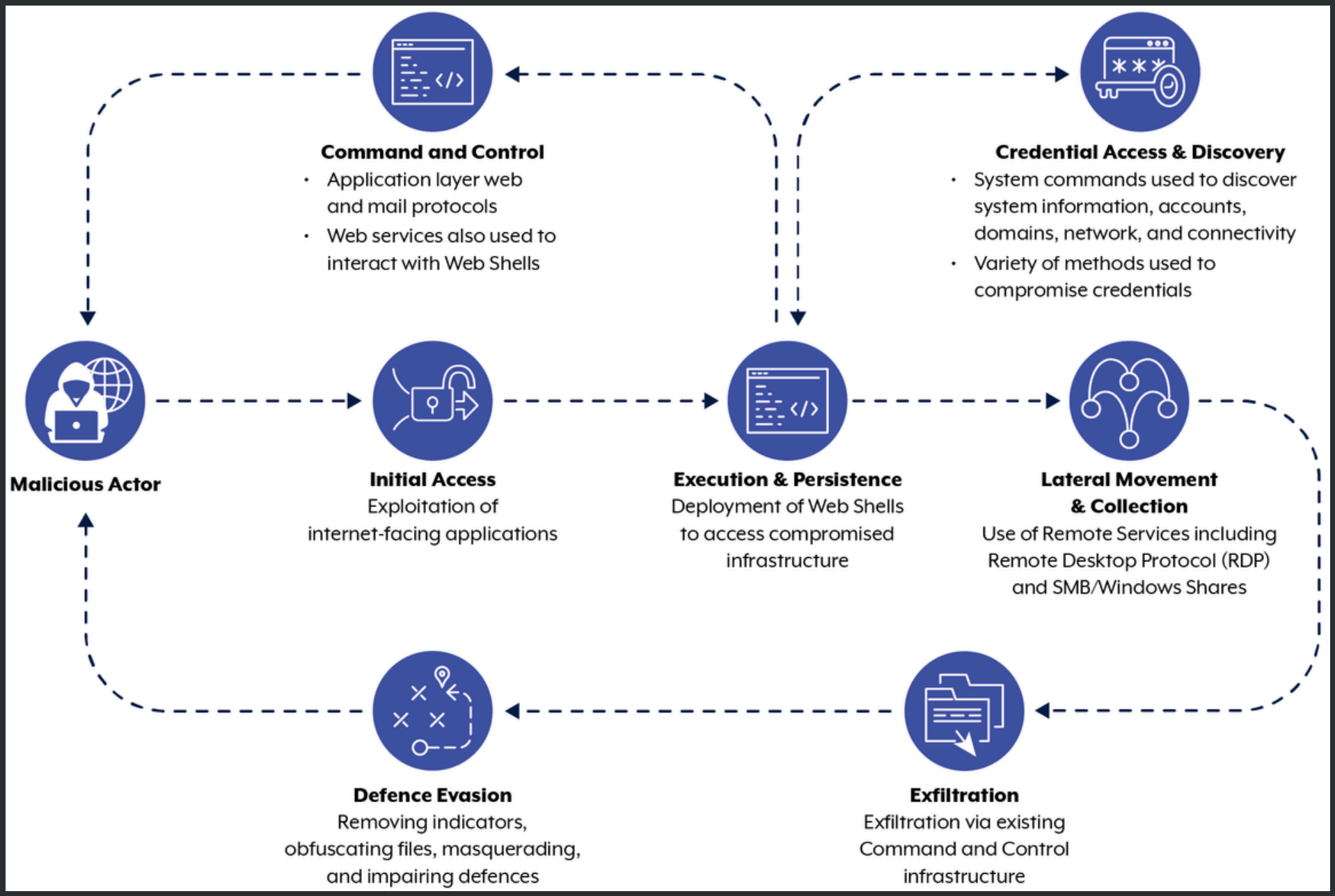
- Compromised devices, including small-office/home-office (SOHO) devices, as operational infrastructure and last-hop redirectors

- T1594 : Search Victim-Owned Websites
- T1190 : Exploit Public-Facing Application
- T1078.002: Domain Accounts
- T1059: Command and Scripting Interpreter
- T1072: Software Deployment Tools
- T1505.003: Web Shell
- T1552.001: Credentials In Files
- T1558.003: Kerberoasting
- T1021.002: SMB/Windows Admin Shares
- T1213 : Data from Information Repositories
- T1041 : Exfiltration Over C2 Channel
- T1059.004: Unix Shell
- T1068 : Exploitation for Privilege Escalation
- T1056.003: Web Portal Capture
- T1111 : Multi-Factor Authentication Interception
- T1040 : Network Sniffing
- T1046 : Network Service Discovery
- T1071.001: Web Protocols
- T1001.003:Protocol Impersonation

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: ASD's ACSC and CISA
Date: 9 July 2024

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action



TTP Flowchart for APT40 activity

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: ASD's ACSC and CISA
Date: 9 July 2024

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action

Initial Discovery

Actor testing of a custom web application built for the organisation

Host Enumeration

T1082 System Information Discovery

Host enumeration and establishing persistence

First observed logon with use of legitimate credentials

Network Reconnaissance

T1021.002 Remote Services: SMB/Windows Admin Shares

T1135 Network Share Discovery

Network-based reconnaissance and actor activity including: mounting of SMB shares, network-based scanning and enumeration of domains

Exploitation

T1190 Exploit Public-Facing Application

Web application exploitation and web shell creation

Malicious Interaction

First observed interaction of organisation machine with known state-sponsored infrastructure

Re-establishment of Connection

T1090 Proxy

Actor re-established connection of ssf tool (similar to activity on 28 July among other dates)

Case Study 1 Timeline

Twitter/X: @_rectifyq
Tiktok: @rectifyq

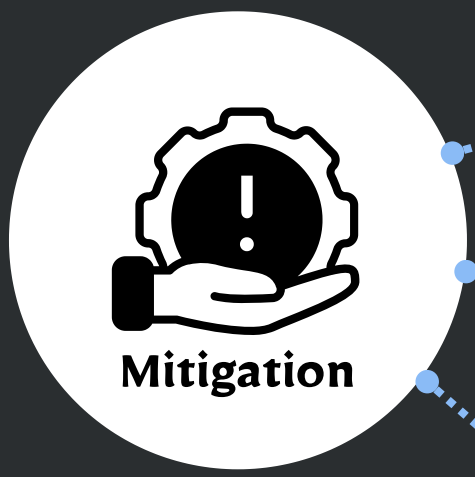
Source: ASD's ACSC and CISA
Date: 9 July 2024

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action

01. Detect process execution from C:\Windows\Temp.

02. Detect process execution from a world writable location in a subdirectory of the Windows OS install location.

03. Detect process execution from C:\Users\Public* and other world writable folders within Users.



01. Logging

02. Patch management

03. Network Segmentation

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: ASD's ACSC and CISA
Date: 9 July 2024

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action

[Historically, APT40 targeted MY as well]
Refer:
MA-892.112022: MyCERT Alert - IOCs and TTPs Associated with APT40 - 18 Nov 2022
Cyberbit - APT40

MA-892.112022: MyCERT Alert - IOCs and TTPs Associated with APT40

18 Nov 2022 Alert apt40, threat actor, ttp, phishing, malware

1.0 Introduction

MyCERT observed the APT40—aka BRONZE MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, MUDCARP, Periscope, Temp.Periscope, and Temp.Jumper, has been active since at least 2009. The APT40 has targeted governmental organisations, companies, and universities in a wide range of industries including biomedical, robotics, and maritime research, targeting countries such as Cambodia, Belgium, Germany, Hong Kong, Philippines, Norway, Saudi Arabia, Switzerland, the United States, the United Kingdom and Malaysia.

Victims Across the Years

As mentioned, APT40 targeted many companies and organizations worldwide. According to the indictment published in 2021 against the group, it attacked many universities, companies, and government organizations across the US, Malaysia, and Cambodia.

Below are a few examples to the group's victims:

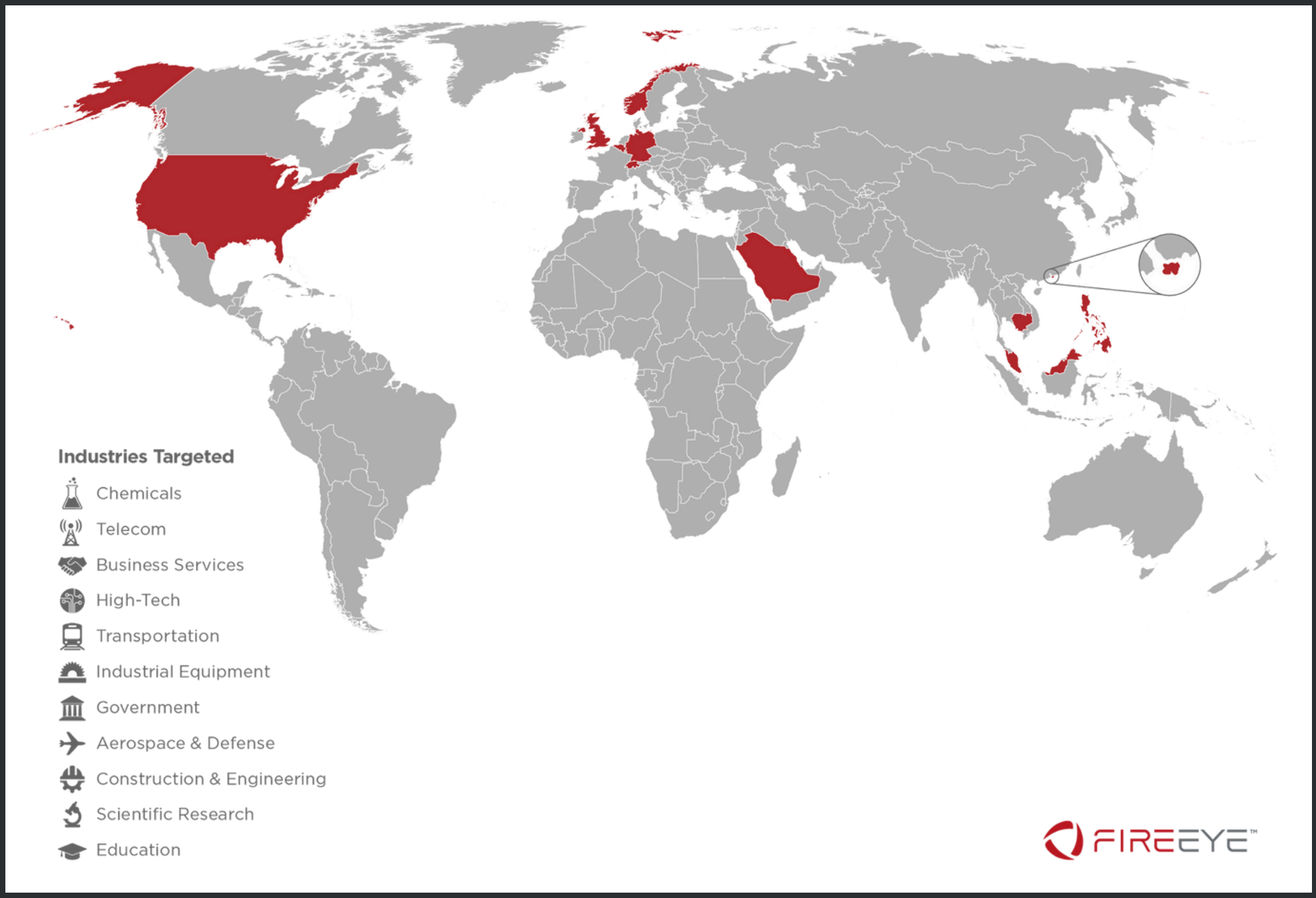
- A research facility in California and Florida, researching and developing vaccines.
- A university in California with a research institute involved in maritime research and a school of medicine.
- A university in Pennsylvania with a robotics program involved in autonomous vehicles and maritime craft.
- A university in Hawaii involved in maritime research.
- A university in Pennsylvania involved in maritime craft and research.
- A university in Maryland with an Applied Physics program.
- A university in Texas is involved in maritime research and development.
- A university in Washington with an Applied Physics program involved in maritime research.
- Mitsubishi Electric, an electronics manufacturer.
- A U.S. defense contractor, which is also involved in maritime research.
- A Cambodian government ministry.
- Two Saudi Arabian government ministries.
- A Malaysian political party.
- The U.S. Institute of Health.
- An IT company in California.

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: ASD's ACSC and CISA
Date: 9 July 2024

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action

[Historically, APT40 targeted MY as well]
Refer: APT40: Examining a China-Nexus Espionage Actor by Mandiant – 4 Mar 2019



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: ASD's ACSC and CISA
Date: 9 July 2024

Patch or Peril: A Veeam vulnerability incident

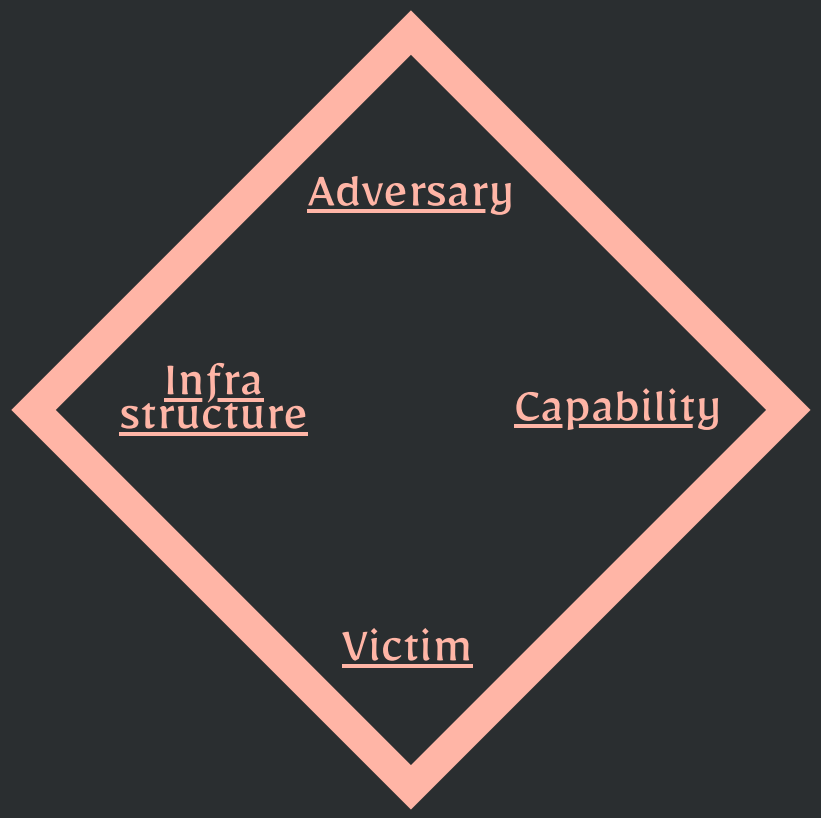
IoC: ✓

MITRE ATT&CK: ✓

Timeline:
Around April 2024

- 149.28.106[.]252
- 149.28.99[.]61
- 45.76.232[.]205
- 77.238.245[.]11:30001

EstateRansomware



UAE, France, Hong Kong, Malaysia, US

- EstateRansomware
- Initial Access through FortiGate Firewall SSL VPN via brute force
- SoftPerfect Netscan, AdFind, NirSoft utilities
- CVE-2023-27532 (Veeam Backup & Replication Software)
- Custom backdoor
- Creation of local rogue user account for lateral movement
- Use DC.exe to disable Win Defender
- Variant of Lockbit 3.0 Ransomware
- T1078 Valid Accounts
- T1133 External Remote Services
- T1053.005 – Scheduled Task/Job: Scheduled Task
- T1571 – Non-Standard Port
- T1505.001 – Server Software Component: SQL Stored Procedures
- T1555 – Credentials from Password Stores
- T1018 – Remote System Discovery
- T1087.002 – Account Discovery: Domain Account
- T1562.001 – Impair Defenses: Disable or Modify Tools
- T1204.002 – User Execution: Malicious File
- T1569.002 – System Services: Service Execution
- T1486 – Data Encrypted for Impact

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 10 July 2024

Patch or Peril: A Veeam vulnerability incident

GROUP-IB

PROFILE

EstateRansomware

Type:
Ransomware

Geography:
UAE, France, Hong Kong, Malaysia, US

Discovery:
3 April 2024

Modus operandi:

- Initial access: Gained entry through FortiGate Firewall SSL VPN via brute force
- Backdoor deployment: Deployed a persistent backdoor ("svchost.exe") via Scheduled task
- Lateral Movement: Moved laterally using remote desktop protocol
- Credential Harvesting: Using tools like SoftPerfect Netscan, AdFind, and NirSoft utilities to gather credentials and network information
- Exploitation: Targeted CVE-2023-27532, activated xp_cmdshell, and created new account
- Ransomware Deployment: Disabled Windows Defender, deployed Ransomware and PsExec.exe via RDP, and executed the Ransomware using PsExec.exe.
- Evasion: Deletion of windows event logs and tools used for the attack

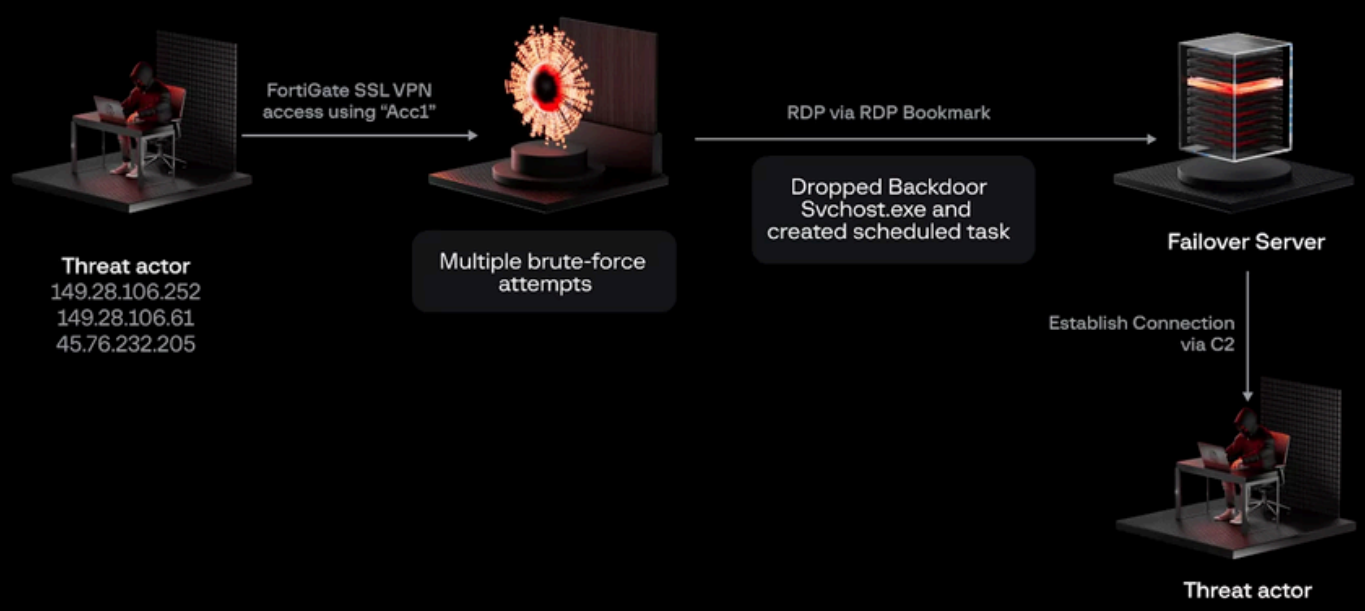
Notable features:

- Custom backdoor svchost.exe that establishes back connect and receives commands using SOCKS
- Brings in exploit tools that targets CVE-2023-27532
- Creation of local rogue user account for lateral movement
- Usage of DC.exe, a defender control software to permanently disable Windows Defender
- Variant of Lockbit 3.0 Ransomware was used to encrypt files and clear logs

Group-IB, 2024

Attack flow from Initial access to establishing foothold

GROUP-IB

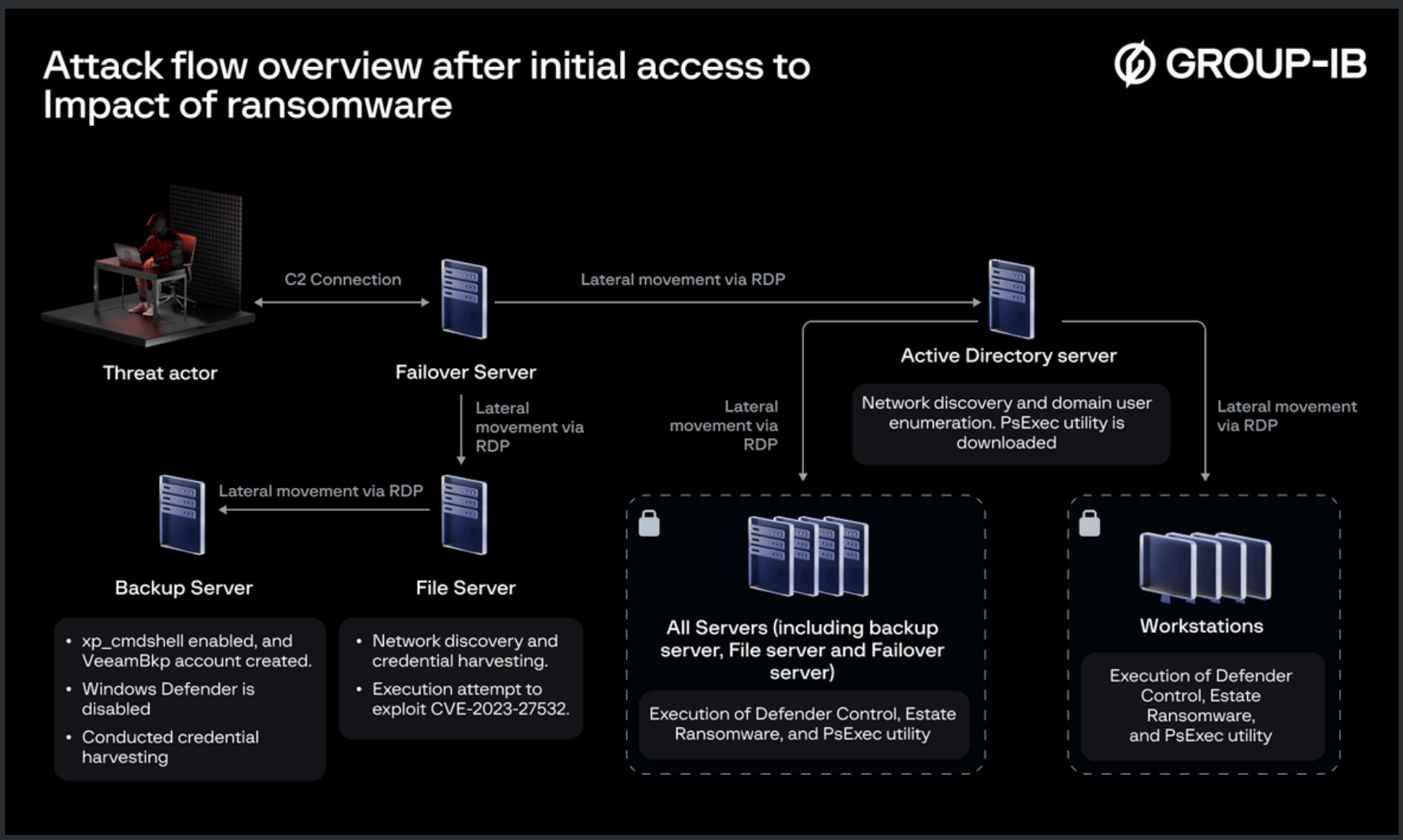


Group-IB, 2024

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 10 July 2024

Patch or Peril: A Veeam vulnerability incident



Twitter/X: @_rectifyq
Tiktok: @rectifyq

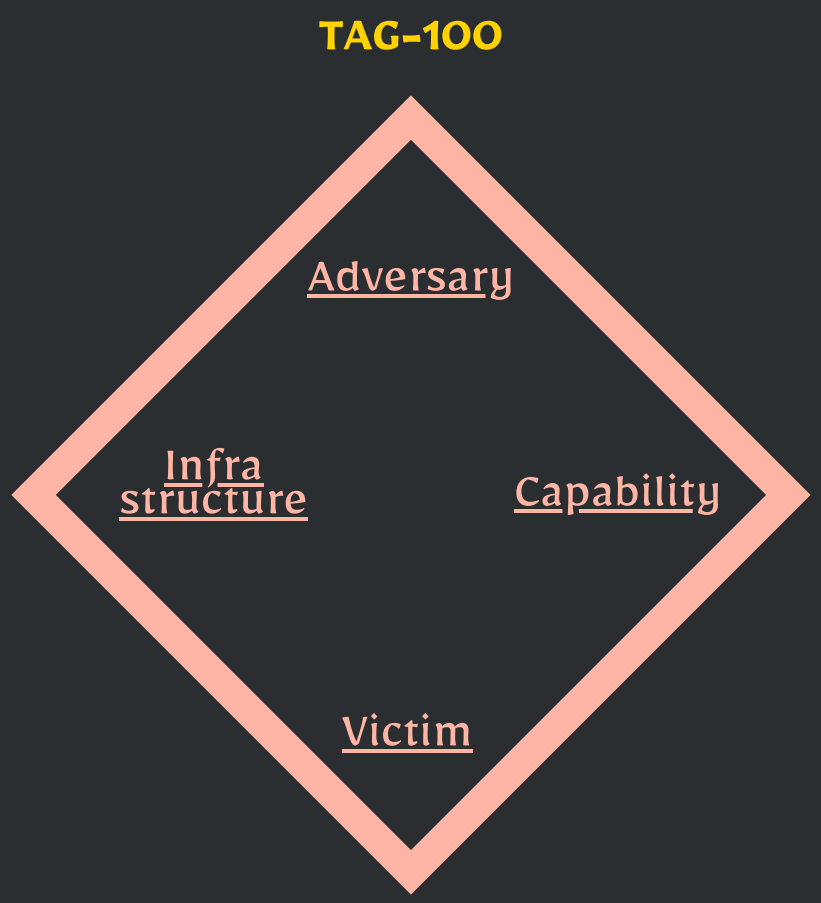
Source: Group IB
Date: 10 July 2024

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

IoC: ☑

MITRE ATT&CK: ☑

Timeline:
Since at least February 2024



- TAG-100 command-and-control (C2) infrastructure
- TAG-100 Exploitation Servers
- TAG-100 Cobalt Strike C2 Domain: www.megtech[.]xyz

- Cobalt Strike
- SparkRAT/LESLIELOADER
- Go backdoors Pantegana
- T1583.003 Acquire Infrastructure: Virtual Private Server
- T1595.002 Active Scanning: Vulnerability Scanning
- T1190 : Exploit Public-Facing Application
- T1055 : Process Injection
- T1027.009 Obfuscated Files or Information: Embedded Payloads
- T1027.013 Obfuscated Files or Information: Encrypted/Encoded File
- T1071 : Application Layer Protocol
- T1102.002 Web Service: Bidirectional Communication

- 2 Asia-Pacific intergovernmental organizations
- Multiple diplomatic and trade entities
- Recon and exploitation victims: wide range of internet-facing appliances belonging to organizations in at least 15 countries, including Cuba, France, Italy, Japan, and Malaysia

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Recorded Future
Date: 16 July 2024

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

Figure 1: *Geographical breakdown of TAG-100 targeting and victimology (Source: Recorded Future)*

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Recorded Future
Date: 16 July 2024

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

TAG-100 Exploitation of Internet-Facing Appliances

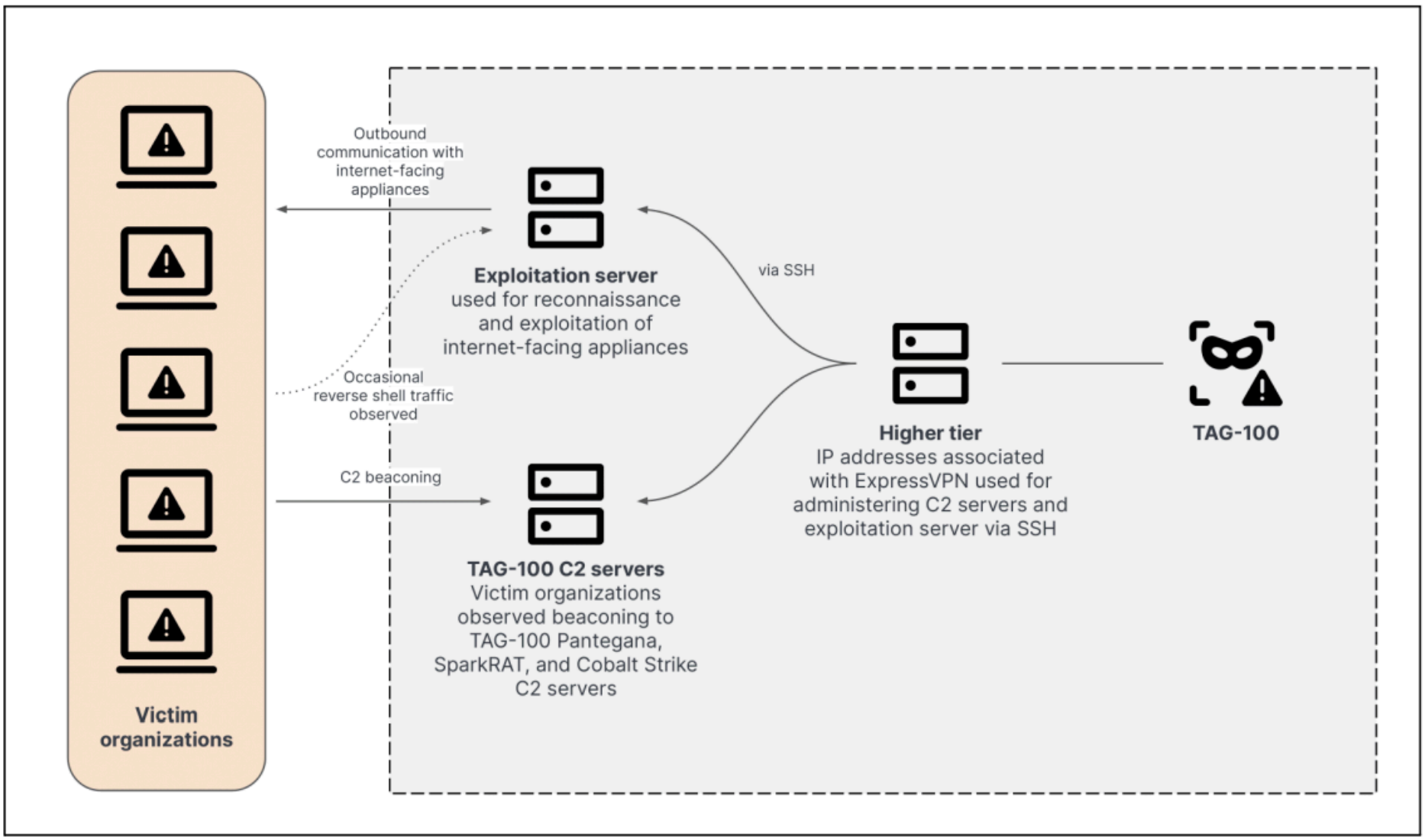


Figure 2: *Overview of TAG-100 operations (Source: Recorded Future)*

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Recorded Future
Date: 16 July 2024

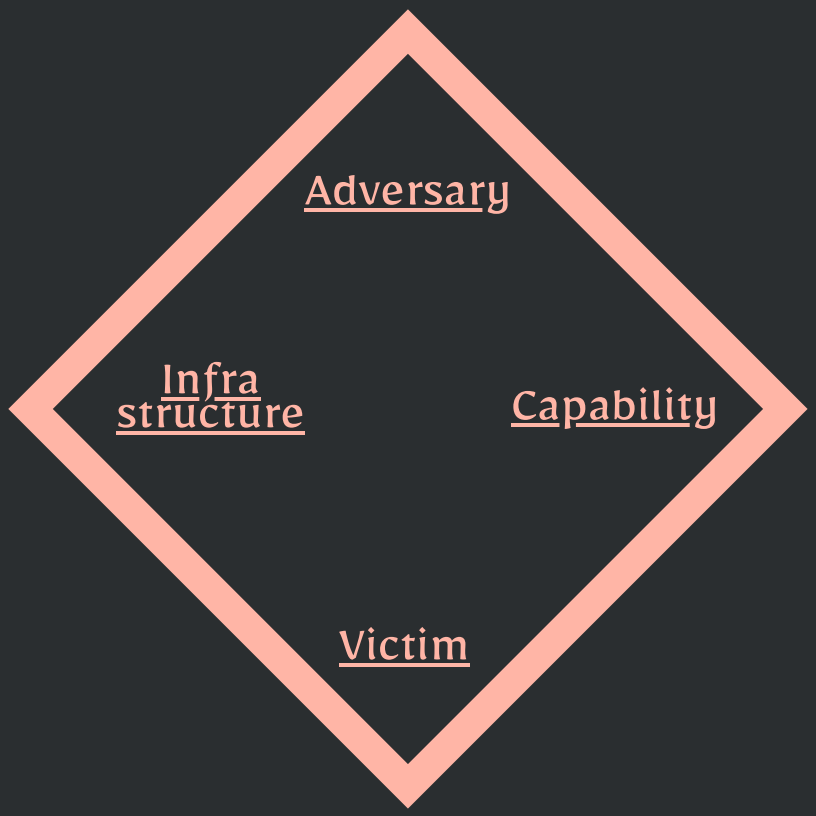
Beware the RAT: Android Remote Access malware strikes in Malaysia

IoC: ✓

~~MITRE ATT&CK~~ Fraud Matrix: ✓

Timeline:
Since at least February 2024

- Phishing website impersonating local legitimate brand to host the malicious app



- CraxsRAT
- Phishing
- 2nd Factor Capture
- App Overlay
- Credentials Capture
- Keylogger
- Password Stealer
- Phone Number Capture
- SMS/Push Interception
- Screencapture
- Device Remote Access
- Enabling Accessibility for Malware
- Access from Fraudster Dev.
- Device Remote Access
- 2nd Factor Bypass
- Authentication ByPasss

- Malaysia-based financial organization's client.
- Number of org. whose customers are under target so far: 3+
- Potential Motivation: Financial (credential stolen and unauthorized withdrawal of funds from victim's bank)

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 31 July 2024

Beware the RAT: Android Remote Access malware strikes in Malaysia

GROUP-IB

PROFILE

Craxs Rat

Type: Android Malware	Regions Targeted: Malaysia	Period of activity: At least Feb 2024 - Current
Initial Vector: Phishing	Sample Detected: 210+	Distinctive Features: Remote Administration Tool
The number of organizations whose customers are under target so far: 3+		

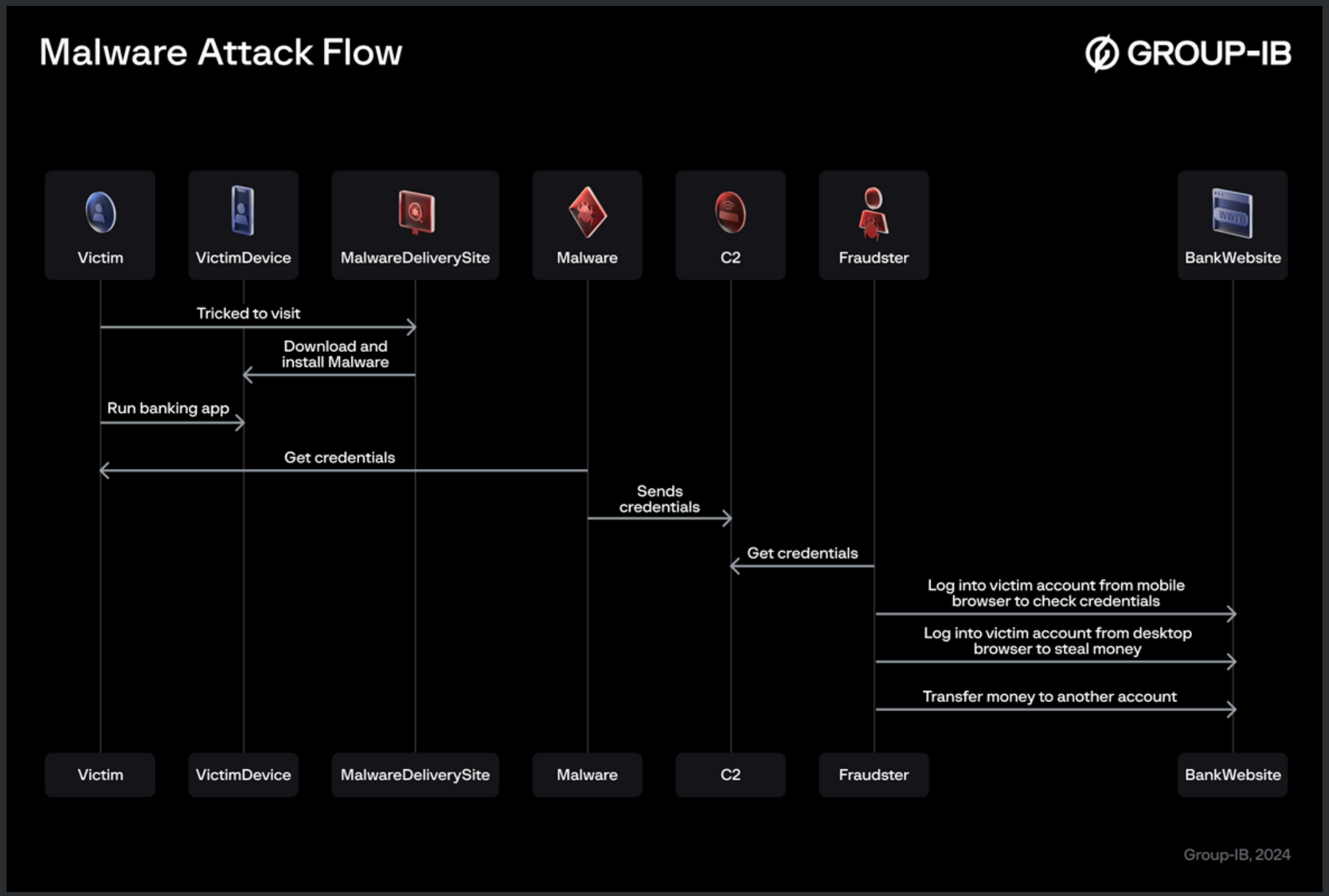
Group-IB, 2024

Resource development	Trust abuse	End-user interaction	Credential access	Account access	Defence evasion
2 techniques	2 techniques	1 techniques	8 techniques	2 techniques	2 techniques
Malware 0	Branded Resource 0	Phishing 0	2nd Factor Capture 0	Access from Fraudster Device 0	2nd Factor Bypass 0
Phishing Resource 0	Enabling Accessibility Service for Malware 0		App Overlay 0	Device Remote Access 0	Accessibility Service 0
			Credentials Capture 0		Authentication By-pass 0
			Keylogger 0		Android Accessibility Service 0
			Password Stealer 0		
			Phone Number Capture 0		
			SMS/Push Interception 0		
			Screen Capture 0		

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 31 July 2024

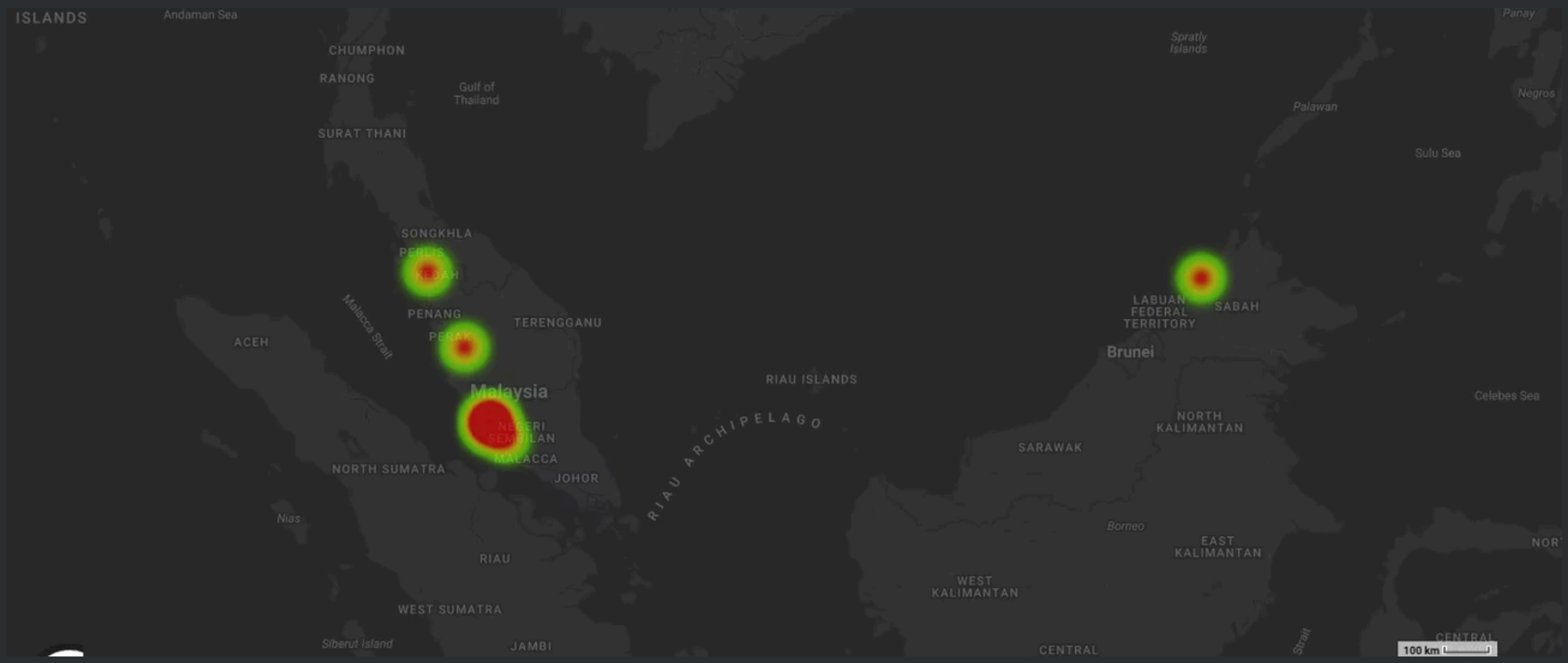
Beware the RAT: Android Remote Access malware strikes in Malaysia



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 31 July 2024

Beware the RAT: Android Remote Access malware strikes in Malaysia



Geographical distribution of
Victims in this campaign

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 31 July 2024

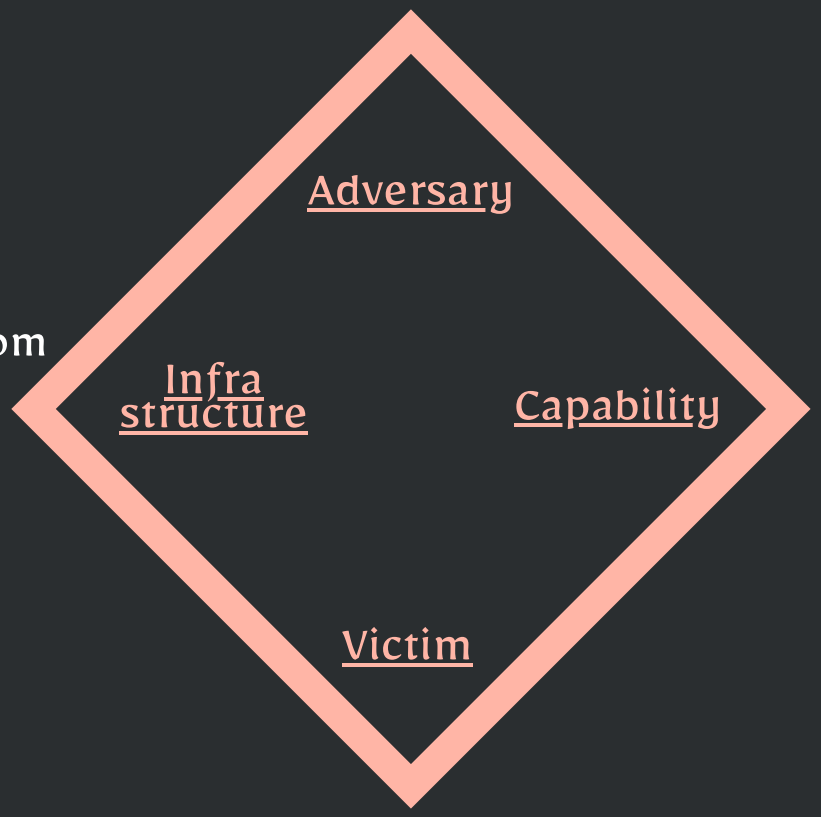
Deciphering the Brain Cipher Ransomware

IoC: ☒

MITRE ATT&CK : ☒

Timeline:
Since at least April 2024

Brain Cipher
(aka SenSayQ,
EstateRansomware,
Reborn Ransomware)



- brain.support[@]cyberfear.com
- qn.support[@]cyberfear.com
- hxxp://mybm<redacted>[.]onion

- Brain Cipher
- EstateRansomware
- RebornRansomware
- Intrude via vulnerable VPN service/weak VPN password
- Use of LockBit samples for Windows
- Use of Babuk samples for Linux
- T1486 : Data Encrypted for Impact

- Geography of victims seems to be random
- **Brain Cipher's victims**: ID, PH, PT, IL, ZA, TH
- **EstateRansomware/SenSayQ/Noname groups victims**: FR, MY, HK, US, IT, LB
- **RebornRansomware**: FR, CN, KW, ID

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 14 August 2024

Deciphering the Brain Cipher Ransomware

GROUP-IB

PROFILE

Brain Cipher Ransomware

(aka SenSayQ, EstateRansomware, RebornRansomware)

Geography of Victims:

Period of activity:

At least from April 2024

Modus Operandi:

- The group most probably intrudes via vulnerable VPN service or weak VPN password.
- For encryption of Windows operating systems, they use Lockbit samples, whereas for the encryption of Linux-based operating systems a variant of the Babuk malware was used.
- Ransom notes contain contact email address and/or TOR website with a chat room.

Notable Features:

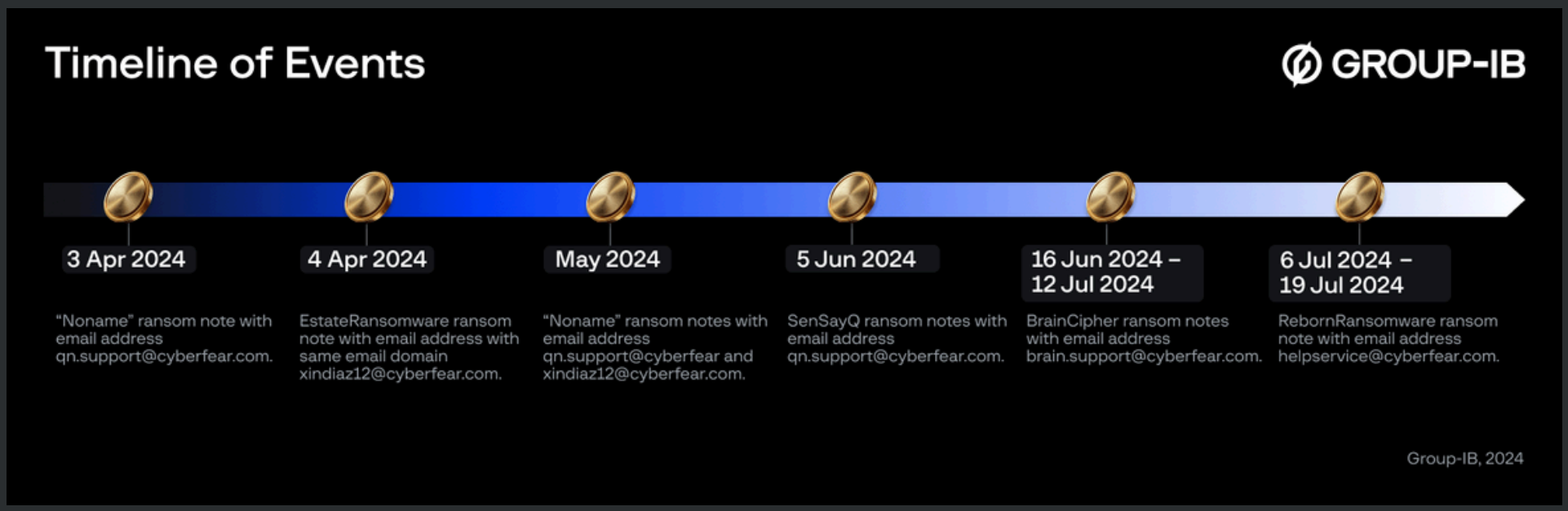
- They most likely do not exfiltrate data as they claimed.
- Threat actors keep changing the format of the ransom notes and name of their group.
- The geography of their victims seems to be random.

Group-IB, 2024

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 14 August 2024

Deciphering the Brain Cipher Ransomware



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 14 August 2024

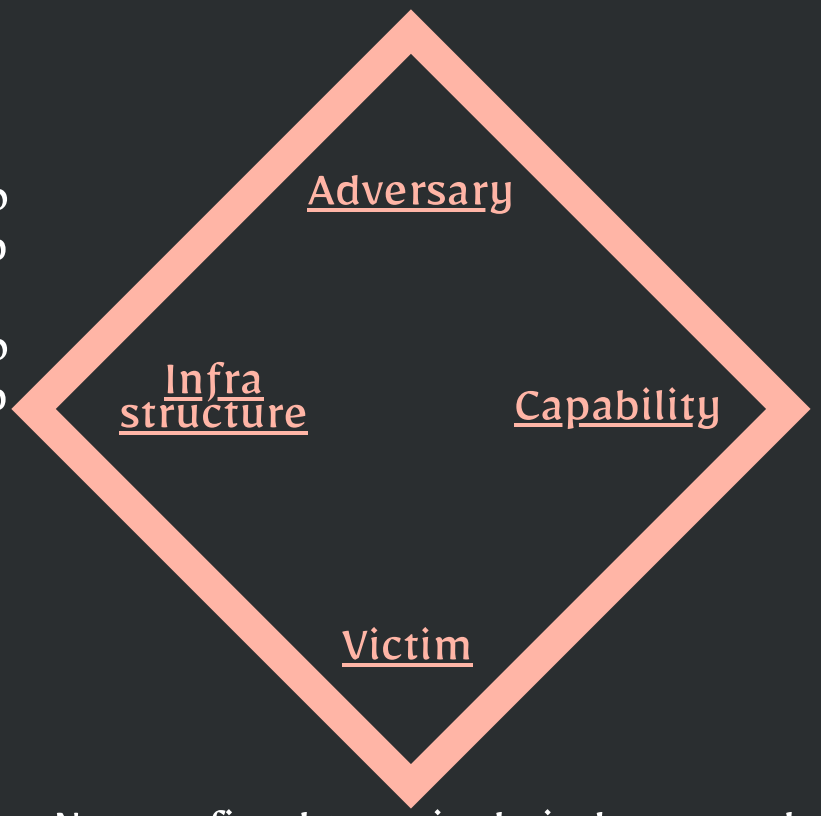
RansomHub ransomware-as-a-service

IoC: ✗

MITRE ATT&CK : ✓

Timeline:
Since February 2024

RansomHub
(Ransomware-as-a-service)
- recruited numerous former Scattered Spider affiliates



- http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/
- http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly
- http://an2ce4pqpf2ipvba2djurxi5pnxxhu3uo7ackul6eafcundqtly7bhid.onion

- RansomHub Ransomware
- LummaC2 Stealer
- Initial access:
  - purchase compromised valid domain accounts (T1078.002)
  - and external remote services (T1133) - AteraAgent and Splashtop
- Built-in Active Directory tools
- T1018 : Remote System Discovery
- T1046 : Network Service Discovery
- Netscan, smbexec, Impacket, PsExec
- T1570 : Lateral Tool Transfer
- Exfil: rclone -> Mega
- T1021 : Remote Services
- disableAV.bat - Terminate antivirus solution (T1562.001)

- Not confined to a single industry and targets companies across various sectors, primarily: Healthcare, Finance, Government
- Most frequent: US, UK, ES, FR, IT
- Less focus on: LATAM, META, APAC
- MY entities - one of the victims
- They do not initiate any attacks in the Commonwealth of Independent States (CIS) region, KP, CN, RO, and CU

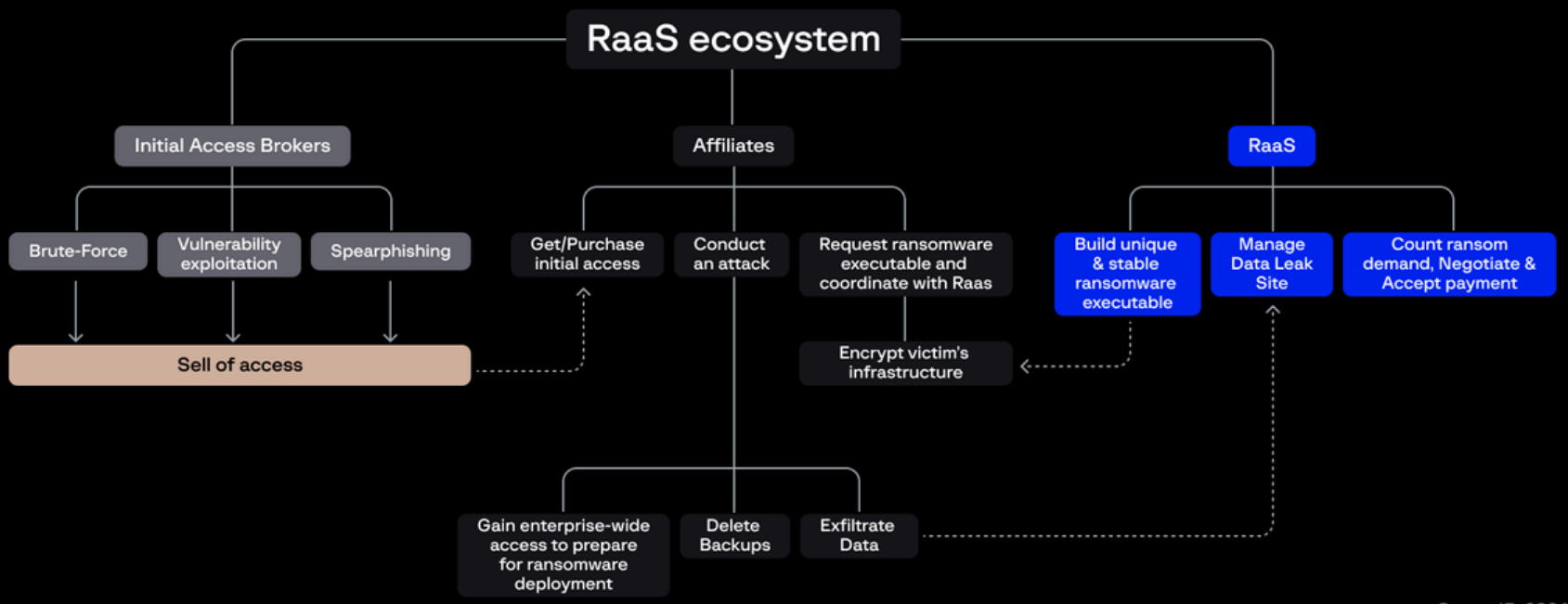
Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 28 August 2024

RansomHub ransomware-as-a-service

Ransomware-as-a-Service Ecosystem

GROUP-IB



Group-IB, 2024

GROUP-IB

PROFILE

RansomHub (aka koley)

First Discovery: February 2024

Targeted Industries:

- Agriculture
- Automotive
- Consumer Goods
- Education
- Financial Services
- Food and Beverages
- Government and Military
- Healthcare
- Hospitality
- Information Technology & Software
- Legal Services
- Logistics and Shipping
- Manufacturing
- Media & Entertainment
- Pharmaceutical
- Real Estate
- Retail and E-commerce
- Telecommunications

Geography of Victims:

- Australia
- New Zealand
- India
- Indonesia
- Japan
- Malaysia
- South Korea
- Sri Lanka
- Thailand
- Vietnam
- Afghanistan
- Egypt
- Kuwait
- Libya
- South Africa
- UAE
- Austria
- Denmark
- France
- Germany
- Italy
- Netherlands
- Norway
- Poland
- Romania
- Serbia
- Slovakia
- Spain
- Sweden
- Switzerland
- United Kingdom
- Canada
- United States
- Mexico
- Brazil
- Chile
- Colombia
- El Salvador
- Honduras
- Peru

Group-IB, 2024

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 28 August 2024

RansomHub ransomware-as-a-service

Number of Attacks by Country

GROUP-IB

Group-IB, 2024

Number of Attacks by Industry

GROUP-IB

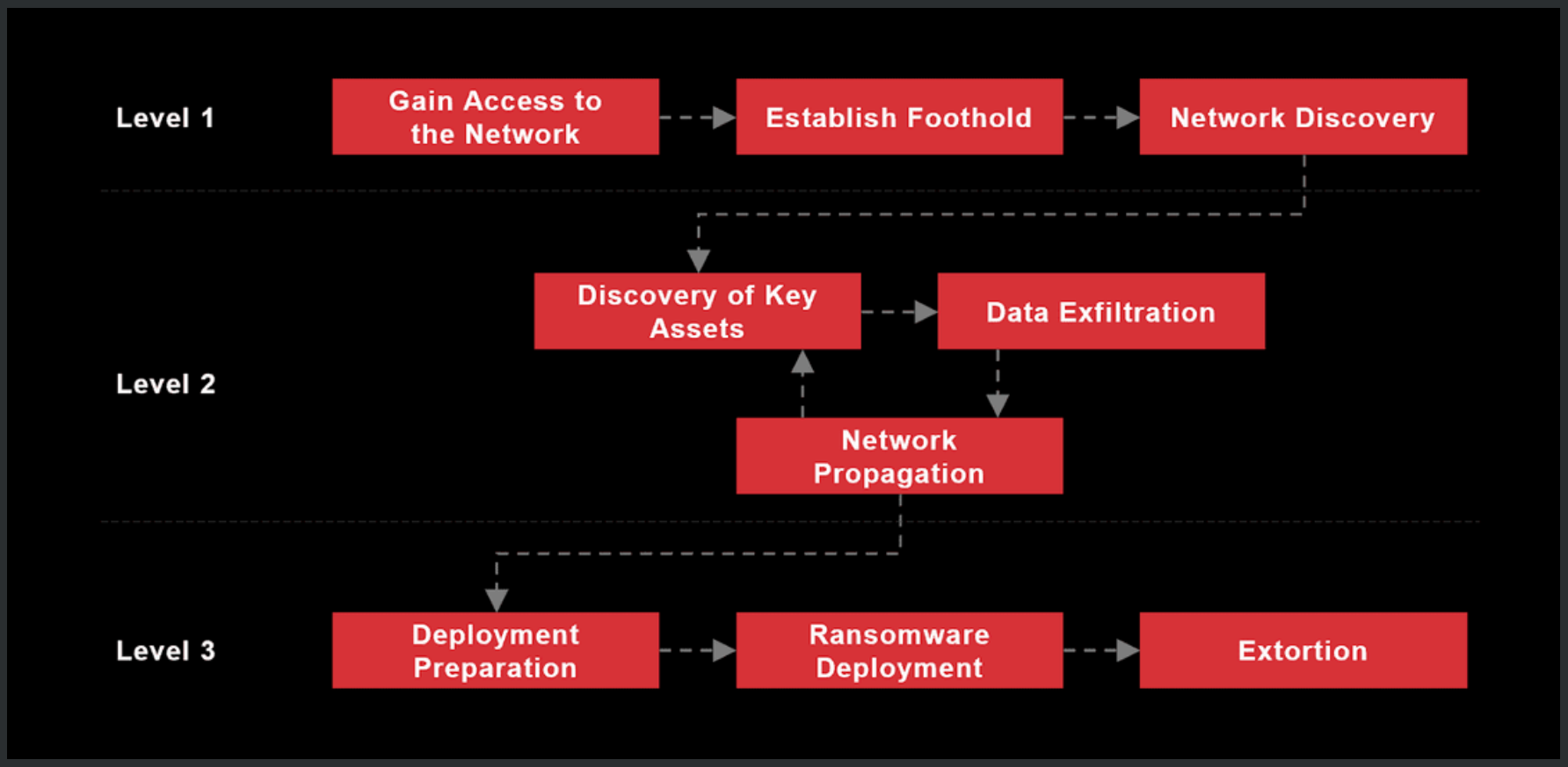
IT	16	Education	4	Clothing & Apparel	2
Real Estate	9	Transportation	4	Consulting Messaging &	2
Financial Services	9	Consumer Goods	3	Telecommunication	2
Healthcare	8	Agriculture & Farming	3	Commerce & Shopping	2
Food & Beverage	6	Software	3	Content & Publishing	1
Government & Military	6	Science & Engineering	3	Sales & Marketing	1
Manufacturing	5	Energy	3	Customer Service	1
Media & Entertainment	5	Hardware	2		

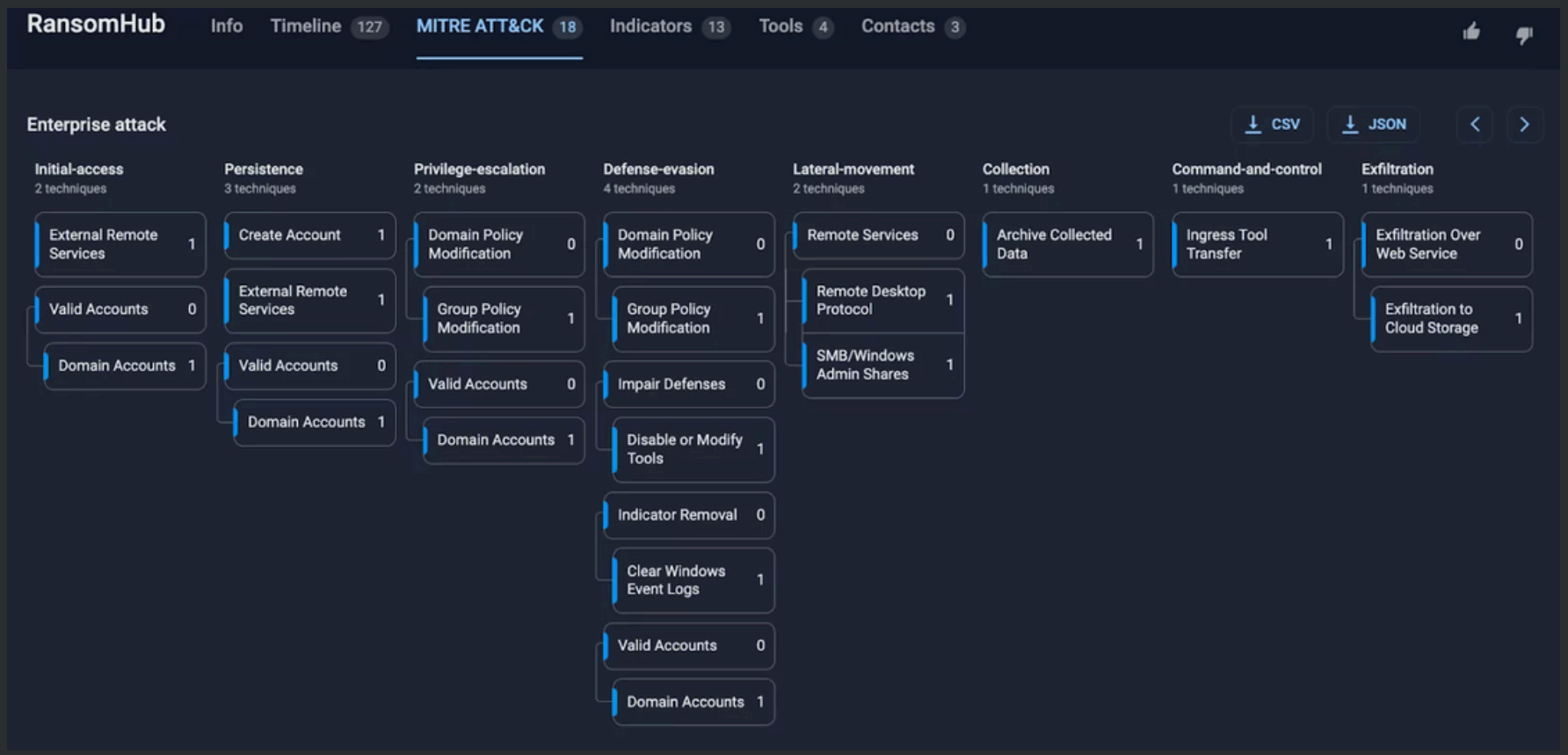
Group-IB, 2024

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 28 August 2024

RansomHub ransomware-as-a-service





Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group IB
Date: 28 August 2024

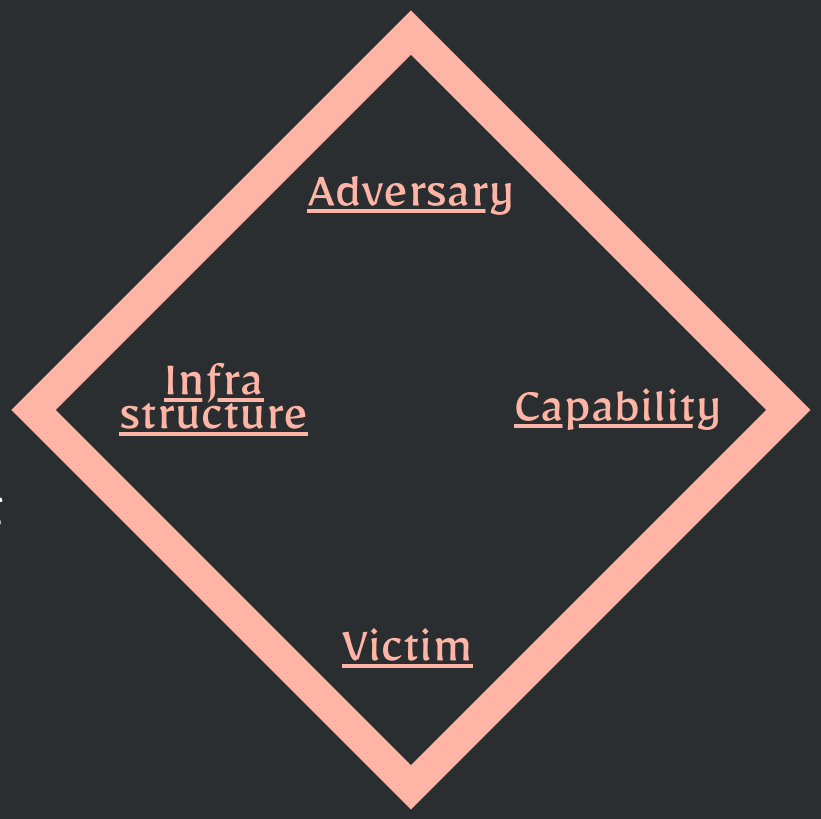
The Intricate Babylon RAT Campaign Targets Malaysian Politicians, Government

IoC: ☑

MITRE ATT&CK : ☑

Timeline:
Since July 2024

- 64.176.65.152
- workhub-microsoft-team.com
- 149.28.19.207
- fund.sekretariatparti.org



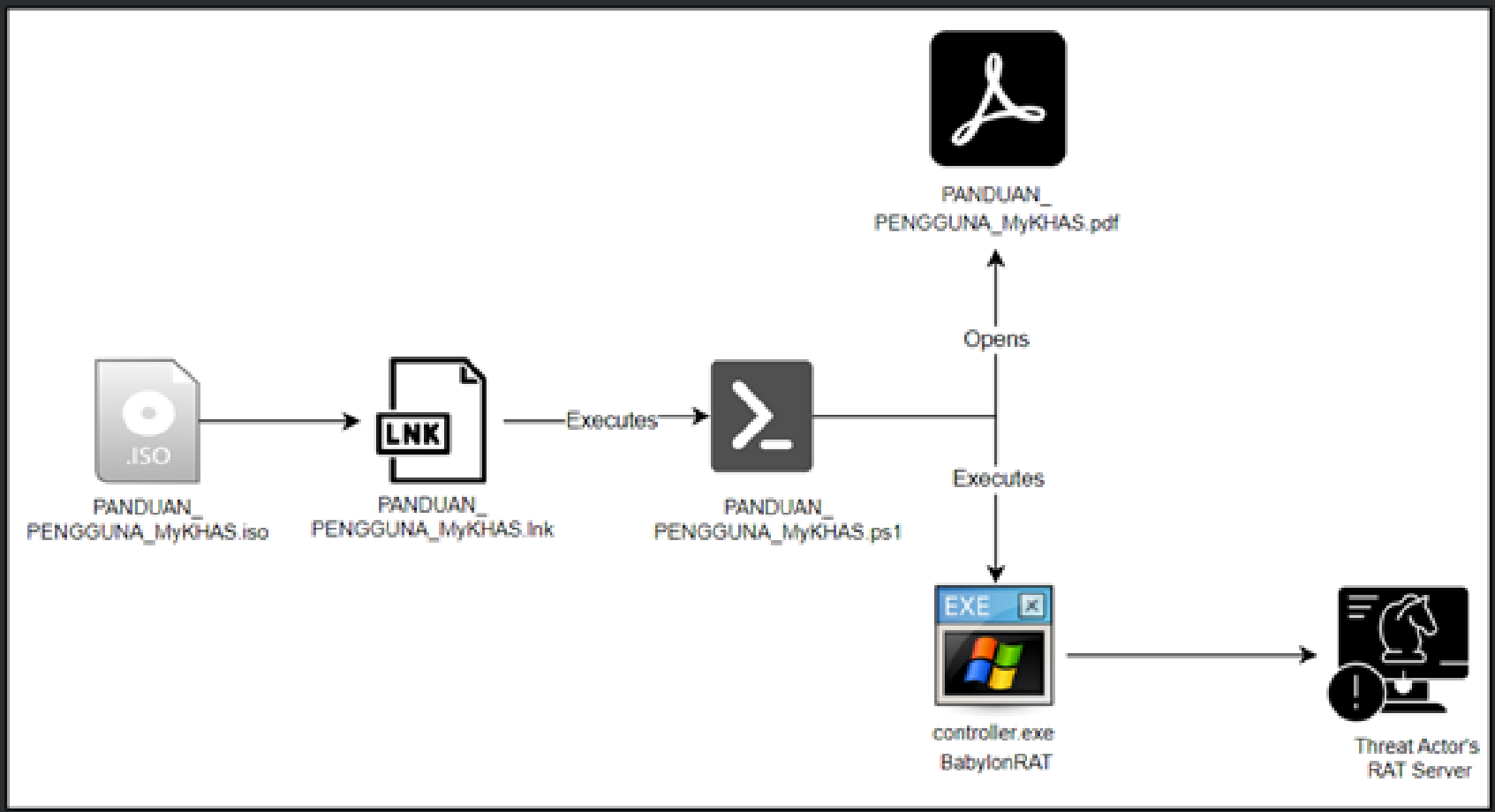
- Targeting political figures and government officials within Malaysia

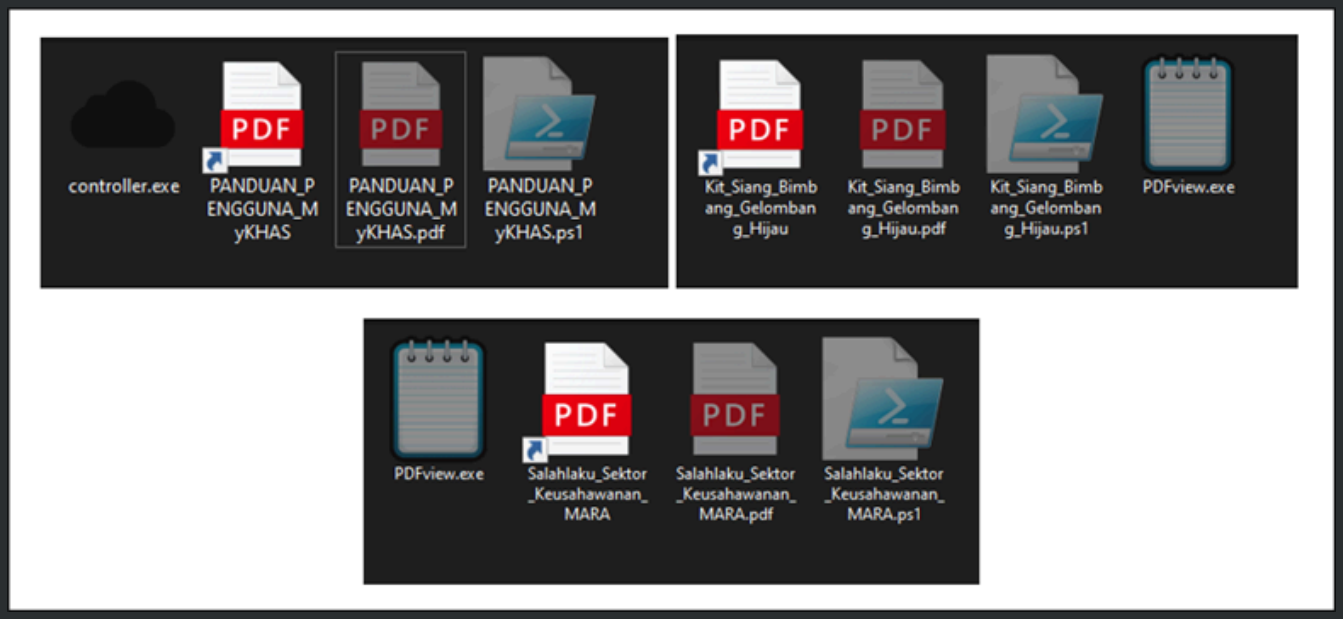
- Babylon RAT
- T1204.002 User Execution: Malicious File
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027.007 Dynamic API Resolution
- T1027.012 LNK Icon Smuggling
- T1027.013 Encrypted/Encoded File
- T1555.003 Credentials from Web Browsers
- T1082 : System Information Discovery
- T1115 : Clipboard Data
- T1056.001 Keylogging
- T1071.001 Web Protocols
- T1041 : Exfiltration Over C2 Channel

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cyble
Date: 4 September 2024

The Intricate Babylon RAT Campaign Targets Malaysian Politicians, Government





Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Cyble
Date: 4 September 2024

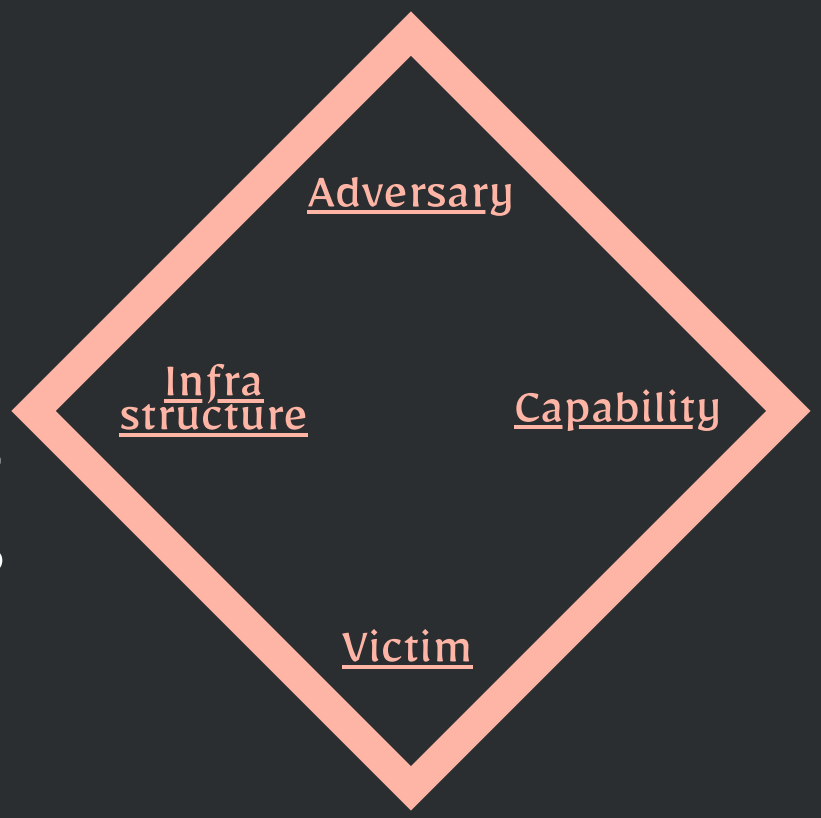
Inside the Dragon: DragonForce Ransomware Group

IoC: ✓

MITRE ATT&CK : ✓

Timeline:
Since August 2023

DragonForce Ransomware
(Ransomware-as-a-Service)



- 185[.]73[.]125[.]8
- 94[.]232[.]46[.]202
- 69[.]4[.]234[.]20
- 2[.]147[.]68[.]96
- 185[.]59[.]221[.]75
- hxxp://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid[.]onion

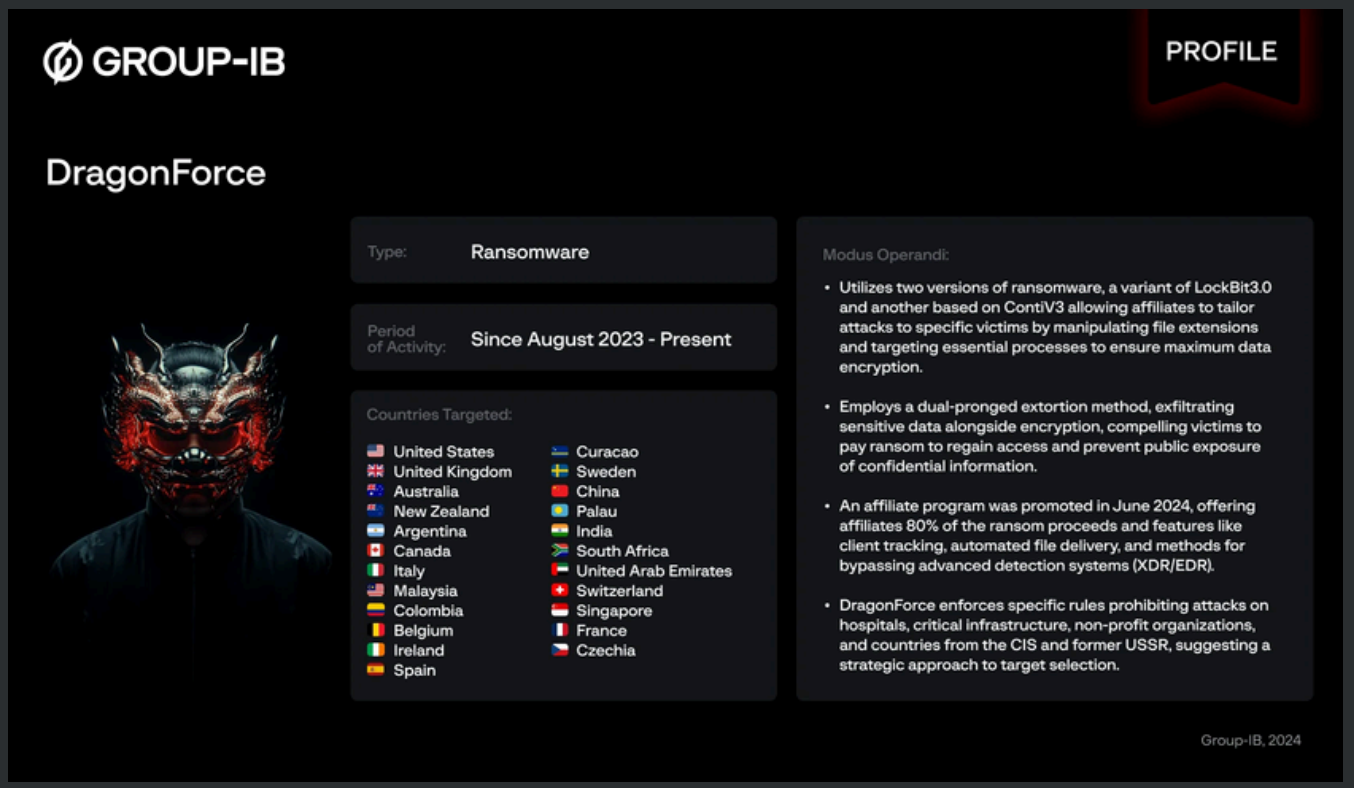
- US, UK, AU, NZ, AR, CA, IT, **MY**, CO, BE, IE, ES, CW, SE, CN, PW, IN, ZA, AE, CH, SG, FR, CZ
- Specific Rules -prohibit attack on
  - Hospitals
  - Critical Infrastructure
  - Non-profit orgs.
  - Countries from CIS and former USSR

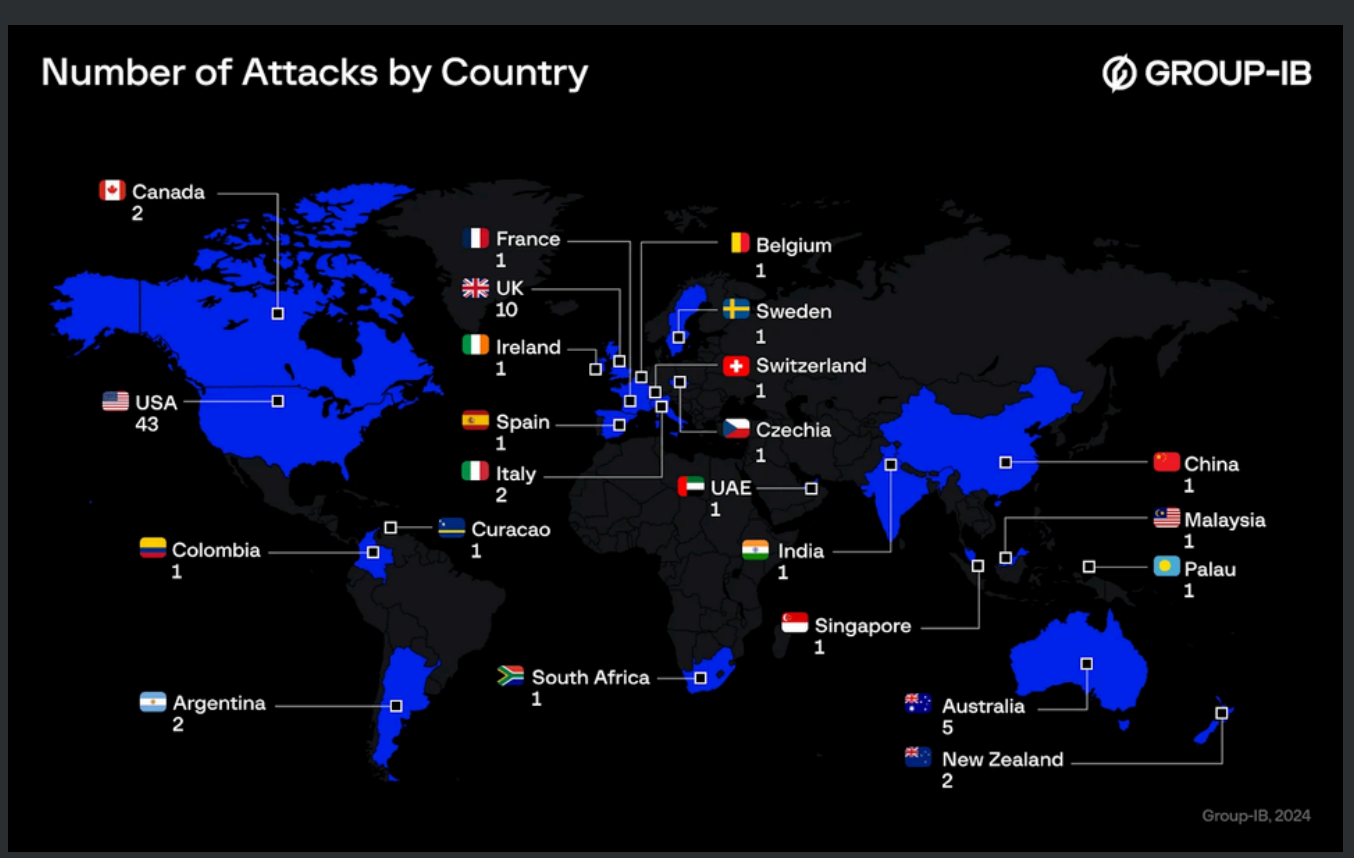
- Variant of Lockbit 3.0
- Another is based on ContiV3
- SystemBC, Cobalt Strike, Mimikatz
- Dual pronged extortion
- T1078 Valid Accounts
- T1059.001 PowerShell
- T1078.002 Domain Accounts
- T1547.001 Registry Run Keys / Startup Folder
- T1543.003 Windows Service
- T1070.001 Clear Windows Event Logs
- T1003.001 LSASS Memory
- T1482 Domain Trust Discovery
- T1018 Remote System Discovery
- T1016 System Network Configuration Discovery
- T1082 : System Information Discovery
- T1083 File and Directory Discovery
- T1021.001 Remote Desktop Protocol
- T1071.001 Web Protocols
- T1486 Data Encrypted for Impact

Source: Group-IB
Date: 25 September 2024

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Inside the Dragon: DragonForce Ransomware Group





Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group-IB
Date: 25 September 2024

Inside the Dragon: DragonForce Ransomware Group

Правила DragonForce

1. **Ограничения на цели:** Запрет атак на больницы, критическую инфраструктуру, некоммерческие организации, страны СНГ и бывшего СССР.
2. **Коммуникация с клиентами:** Требование уважительного общения с компаниями, готовыми к сотрудничеству.
3. **Процедура оплаты:** Первоначальный платеж команде вносится на кошелек партнерской программы. Последующие платежи – на кошелек команды. Возможно требование депозита в 1 BTC перед первым платежом.
4. **Ответственность гаранта:** Гарант несет полную ответственность за приглашенного партнера и может быть заблокирован за его нарушения.
5. **Распределение платежей:** Команда получает 80% платежа, партнерская программа – 20%. Партнер обязан немедленно выплачивать 20% суммы.
6. **Передача кошелька для платежей:** Осуществляется через функцию в Actions, с указанием суммы в BTC.
7. **Настройка таймера:** Устанавливается при создании Build. Стандартно: 14 дней для доступа к Recovery, 7 дней для переговоров об оплате.
8. **Право на ведение переговоров:** Партнерская программа DraongForce Ransomware оставляет за собой право вести переговоры с компанией в некоторых случаях. (пример, партнер ведет себя ни адекватно, ни уважительно, не выполняет свои обязательства)
9. **Требование к загрузке файлов:** Партнер обязан загружать файлы атакованной компании для получения оплаты.
10. **Запрет на политическое влияние:** Любые попытки политического влияния строго запрещены.
11. **Ответственность администратора/лидера команды:** Полная ответственность за действия команды и ознакомление сотрудников с правилами.
12. **Ограничение на скидки:** Максимальная доступная скидка – 45% от указанной суммы покупки декриптора и удаления файлов.
13. **Определение суммы выкупа:** Команда самостоятельно определяет сумму покупки в диапазоне от $100 до $1,000,000+.
14. **Тестовая расшифровка:** Работает в автоматическом режиме, с возможностью обращения в поддержку в исключительных случаях.
15. **Уровни доверия команд:** Различные уровни доверия, повышаемые индивидуально, с соответствующими привилегиями.
16. **Общее правило:** Уважение правил партнерской программы, клиентов и администрации.

Screenshot of the “Rules”

```
Hello [redacted]!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics.
All you need to do is contact us and pay.

Our communication process:

1. You contact us via email or Tox.
2. We send you a list of files that were stolen
3. We decrypt 3 files to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in the future.

Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

Contacts:

Email:   MitraGodbout@proton.me
Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

* If you want to contact us via Tox you need to download it from this link: https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe

YOUR ID: [redacted]

If you refuse to pay or do not get in touch with us, we start publishing your files.
After 7 days the email will no longer be available, and the opportunity to receive the decryptor will also no longer be available.

Sincerely, 01000100 01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101
```

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Group-IB
Date: 25 September 2024

Beyond the Surface: the evolution and expansion of the SideWinder APT group

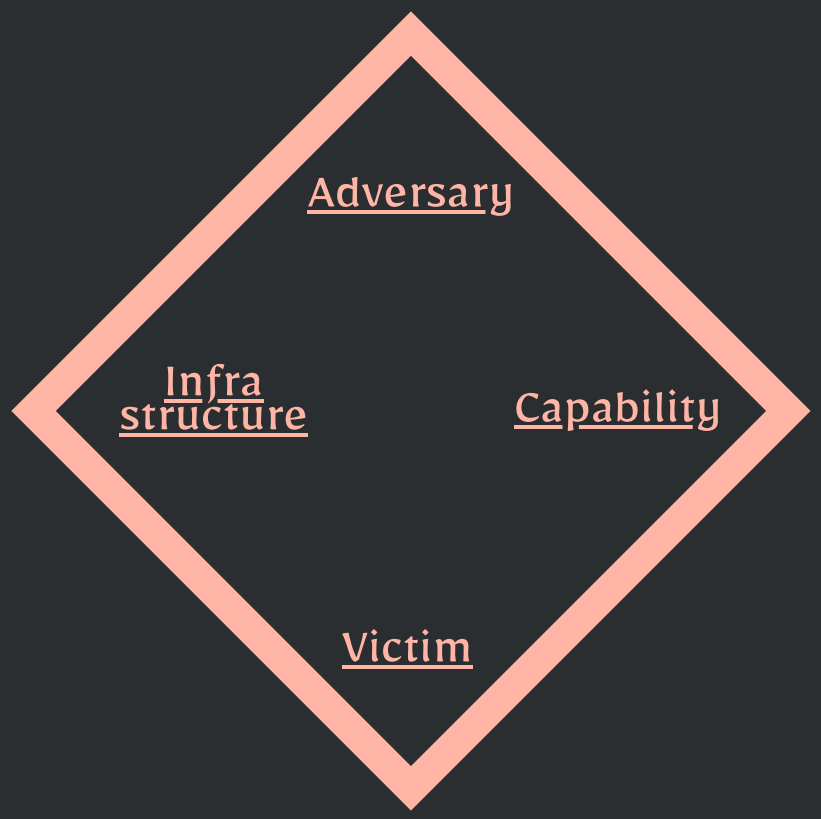
IoC: ☑

MITRE ATT&CK : ☒

Timeline:
Since 2012 (latest activity:2024)

- nextgen[.]paknavy-govpk[.]net
- premier[.]moittpk[.]org
- cabinet-division-pk[.]fia-gov[.]com
- navy-lk[.]direct888[.]net
- srilanka-navy[.]lforvk[.]com
- portdjibouti[.]pmd-office[.]org
- portdedjibouti[.]shipping-policy[.]info
- mofa-gov-sa[.]direct888[.]net
- mod-gov-bd[.]direct888[.]net
- mmcert-org-mm[.]donwloaded[.]com
- opmcm-gov-np[.]fia-gov[.]net
- ...

SideWinder
(aka T-APT-04 or RattleSnake)



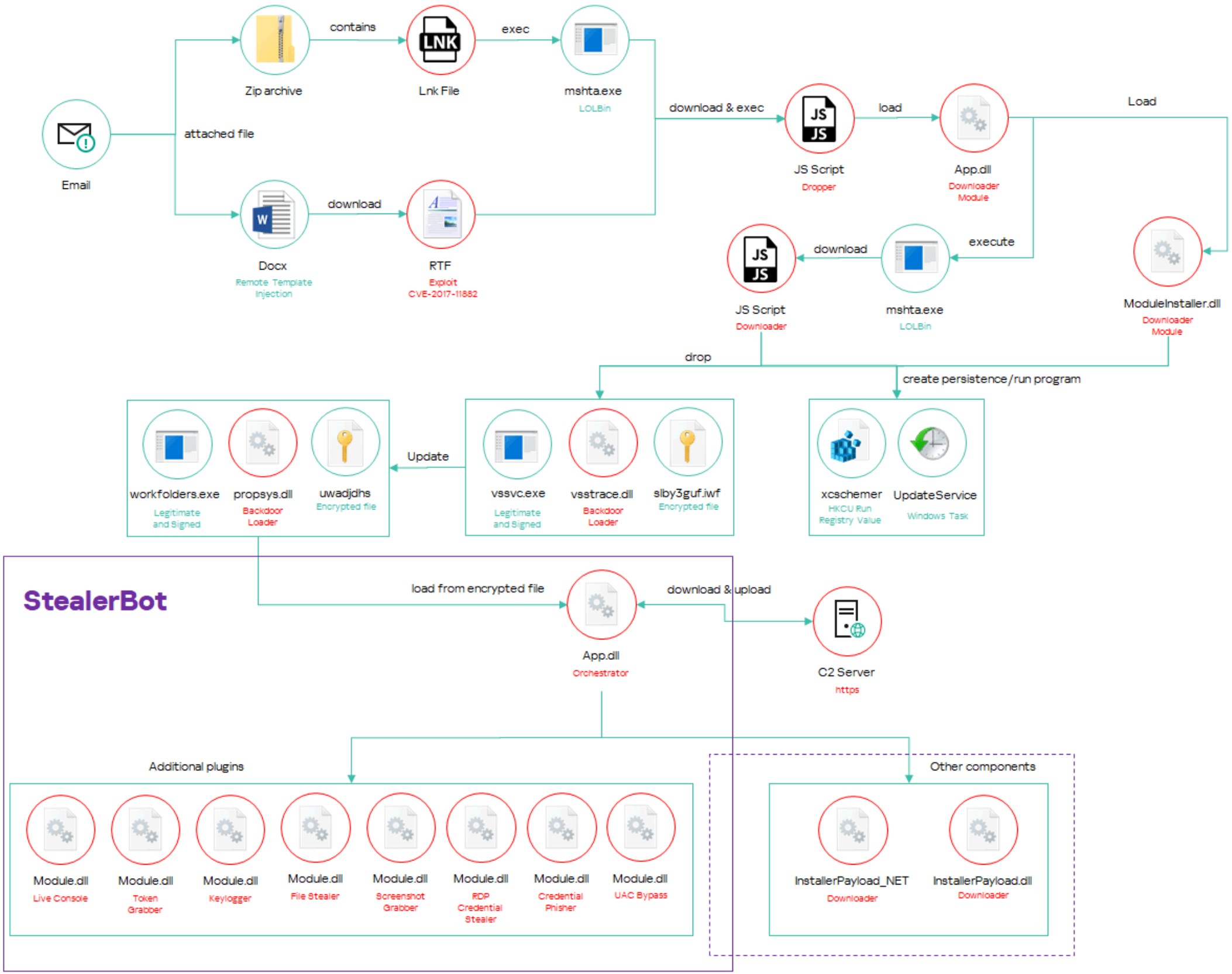
- StealerBot
- CVE-2017-11882 exploit
- T1566 : Phishing
- T1221 : Template Injection
- T1218.005 : Mshta
- T1059.007 : Javascript
- T1053.005 : Scheduled Task
- T1547.001 : Registry Run Keys / Startup Folder
- T1056.001: Keylogging
- T1113 : Screen Capture
- T1083 : File and Directory Discovery
- T1548.002 : Bypass User Account Control
- T1573 : Encrypted Channel
- ....

- **Target countries**: BD, DJ, JO, MY, MV, MM, NP, PK, SA, LK, TR, AE
- **Target Sectors**: gov., mil., logistics, infrastructure and telecom., financial institutions, uni. and oil trading companies
- **Target diplomatic entities in**: AF, FR, CN, IN, ID, MA

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Securelist by Kaspersky
Date: 15 October 2024

Beyond the Surface: the evolution and expansion of the SideWinder APT group



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Securelist by Kaspersky
Date: 15 October 2024

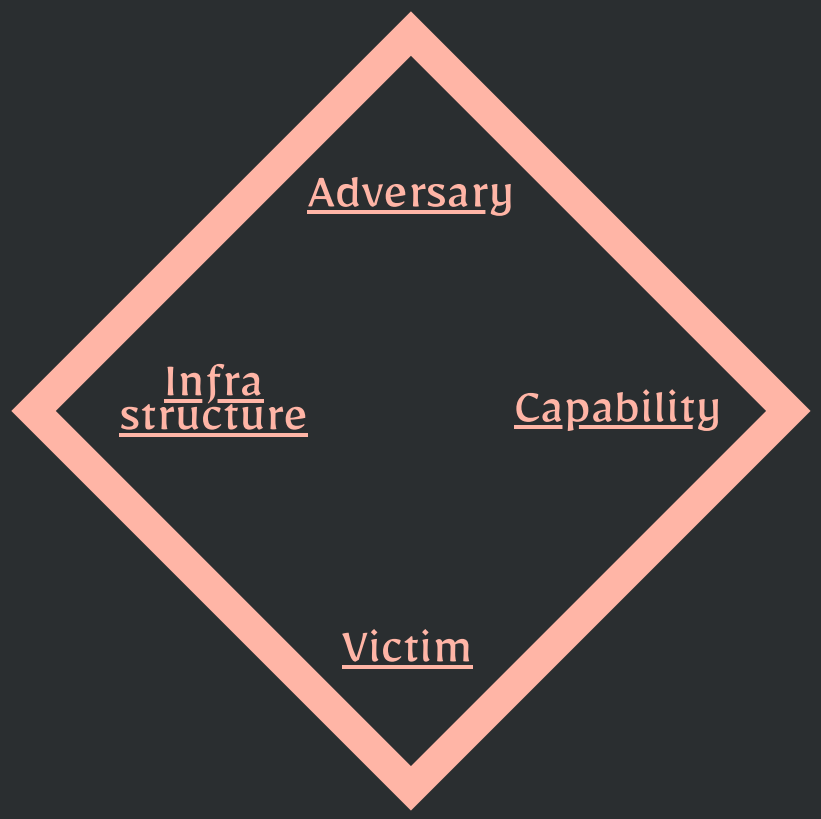
Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions

IoC: ☑

MITRE ATT&CK : ☒

Timeline:
Since 2020 (latest in Oct 2024)

Earth Estries
(may related to Salt Typhoon, FamousSparrow, GhostEmperor and UNC2286)



- frpc server
- SoftEther VPN
- Compromised server
- Open Dir C2
- DEMODEX C&C
- ...

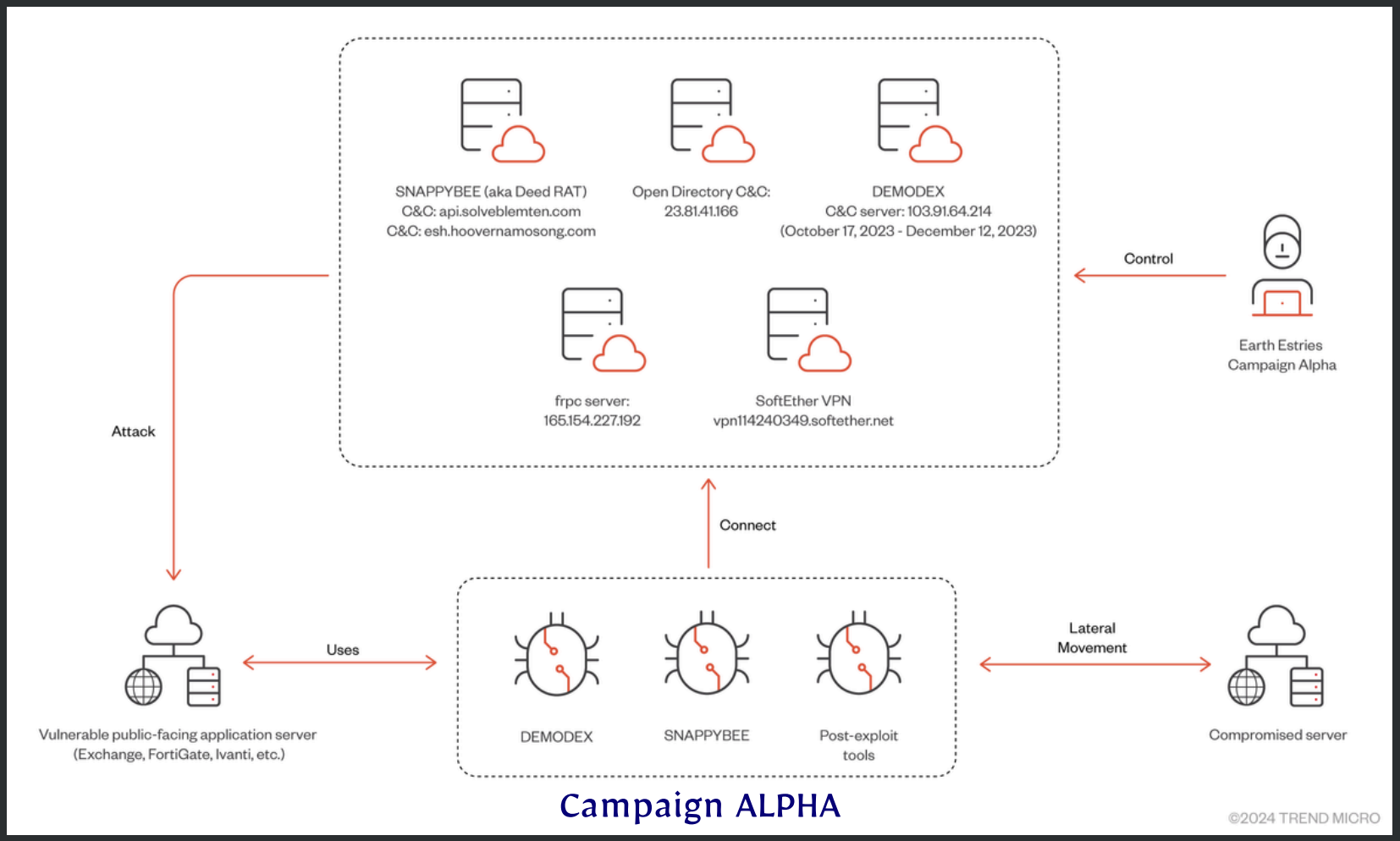
- **Target countries**: AF, BR, SZ, IN, ID, **MY**, PK, PH, ZA, TW, TH, US, VN
- **Target Sectors**: telco, tech, consulting, chemical, transport, gov, NGOs
- **Potential motivation:** Espionage

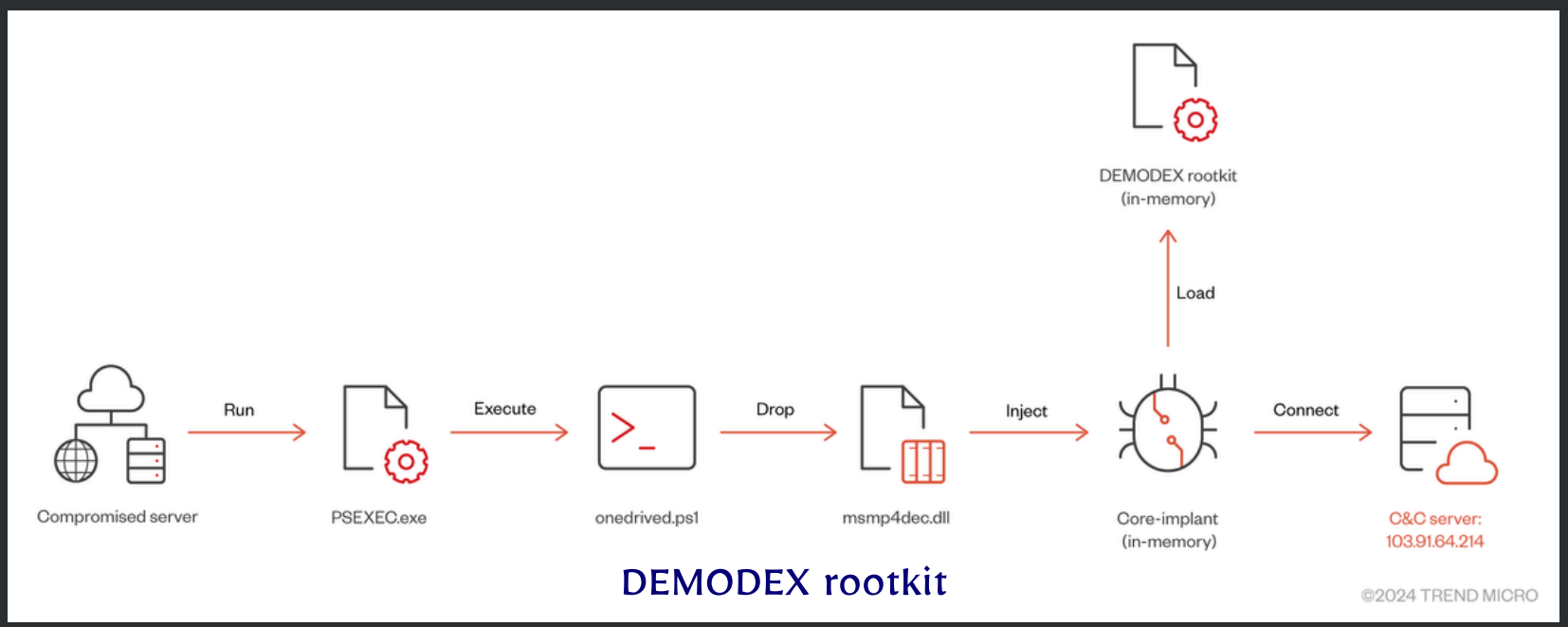
- Customized malware
- GHOSTSPIDER backdoor
- SNAPPYBEE backdoor
- DEMODEX rootkit
- Ivanti Connect VPN vuln
- Fortinet Forticlient vuln
- Sophos FW vuln
- Proxylogon Exchange serv. vuln
- LOLBINs
- frpc
- NeoReGeorg tunnel
- fscan
- T1190 : Exploit Public-Facing Application
- T1059.001 : PowerShell
- T1027 : Obfuscated Files or Information
- T1218.010 : Regsvr32
- T1574.001 : DLL Search Order Hijacking
- T1053.005 : Scheduled Task
- T1059.003 : Windows Command Shell
- T1543.003 : Windows Service
- T1047 : Windows Management Instrumentation
- S0029 : PsExec
- ...

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 25 November 2024

Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions

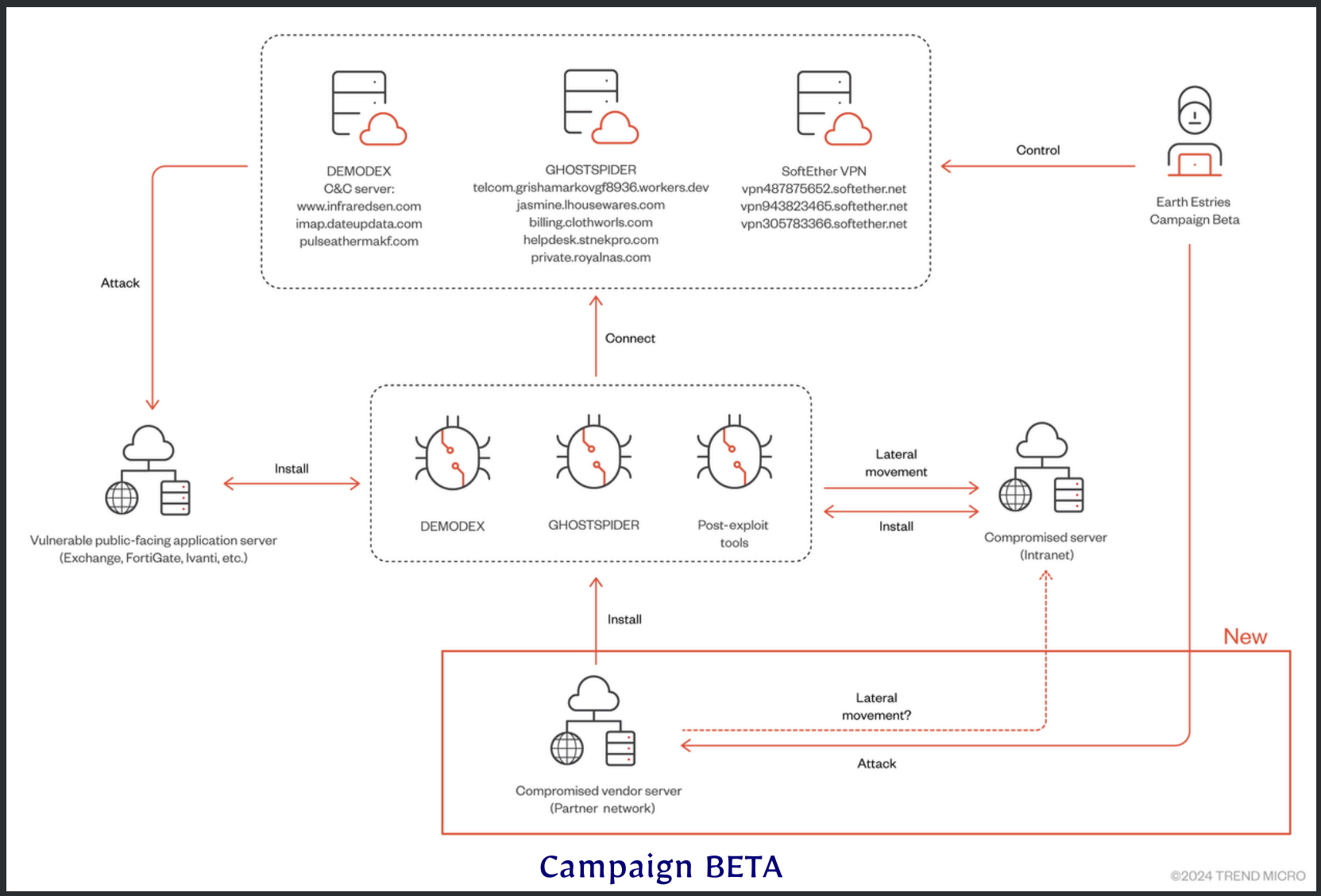




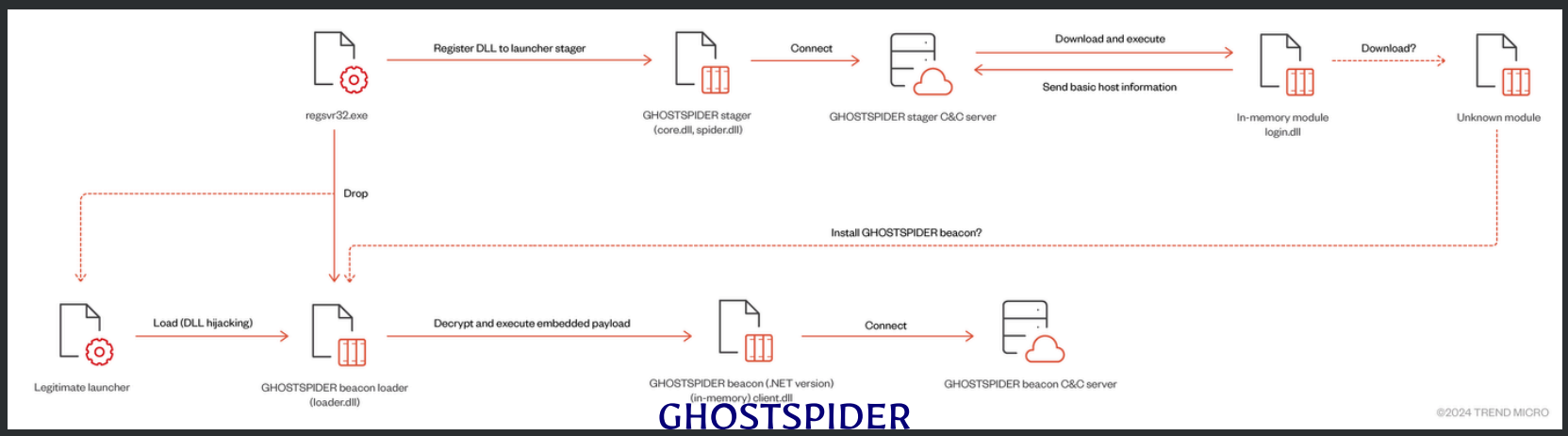
Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 25 November 2024

Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions



Campaign BETA

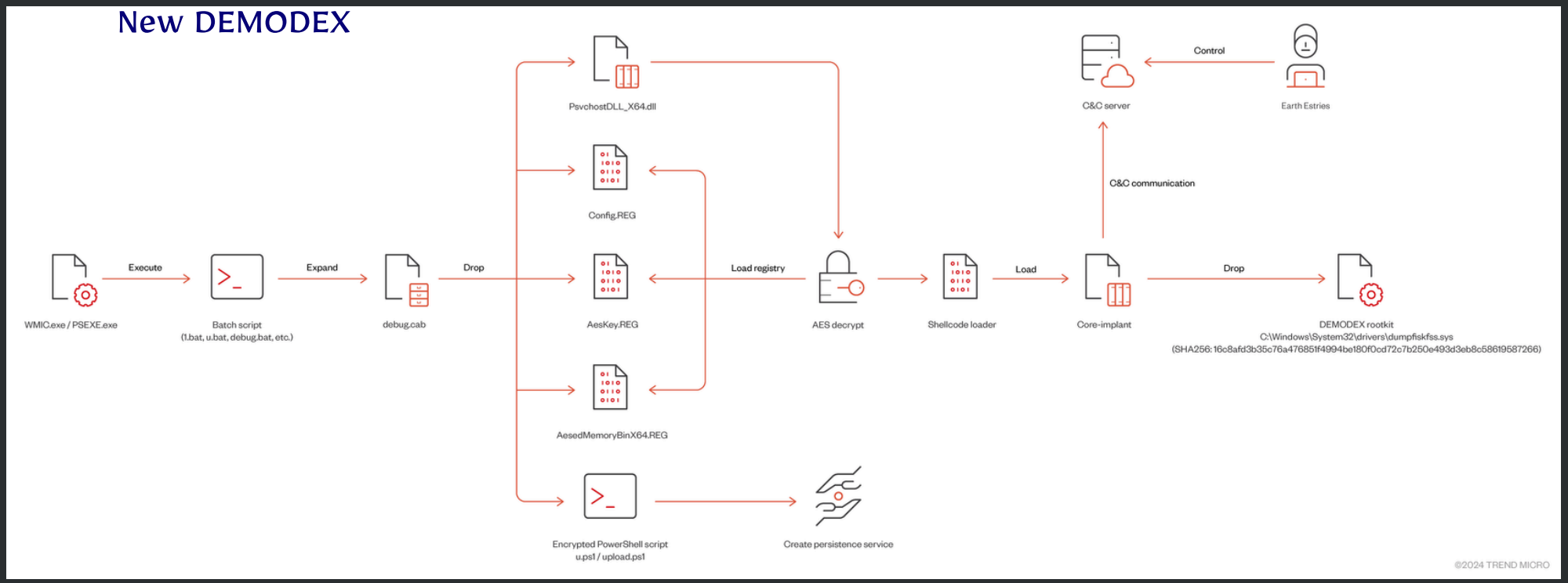


GHOSTSPIDER

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 25 November 2024

Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions



Attribution Overview

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 25 November 2024

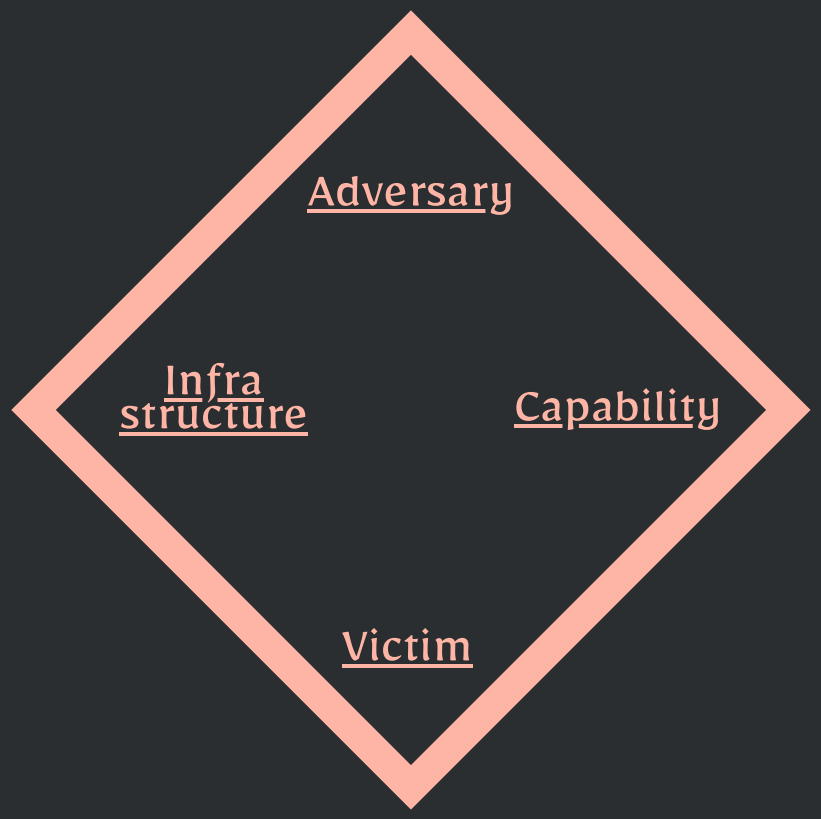
Python-Based NodeStealer Version Targets Facebook Ads Manager

IoC: ☑

MITRE ATT&CK : ☒

Timeline:
Around 20 November 2024

Vietnamese Threat Group
(as suggested by the password that was used to compress the malicious files)



- Telegram (Exfiltration)
- 88[.]216[.]99[.]5
- t[.]ly/MRAbJ
- ...

- **Target countries**: **Malaysia**
- **Target Sectors**: Education
- **Potential motivation:** Data Theft, exfiltration of sensitive information

- NODESTEALER malware
- T1566.002 : Spearphishing Link
- T1204.001 : Malicious Link
- T1059.001 : PowerShell
- T1059.003 : Windows Command Shell
- T1059.006 : Python
- T1027 : Obfuscated Files or Information
- T1053.005 : Scheduled Task
- T1574.002 : DLL Side-Loading
- T1547.001 : Registry Run Keys/Startup Folder
- T1027 : Obfuscated Files or Information
- T1140 : Deobfuscate/Decode Files or Information
- T1555.003 : Credentials from Web Browsers
- T1005 : Data from Local System
- T1580 : Archive Collected Data
- T1567 : Exfiltration over Web Services
- T1657 : Financial Theft

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 19 December 2024

Python-Based NodeStealer Version Targets Facebook Ads Manager

Notis Pelanggaran Hak Harta Intelek

20 November 2024

Kepada [redacted],

Kami adalah [redacted]. Pelanggan kami telah memberi kuasa kepada kami untuk memaklumkan anda tentang penggunaan kandungan hak cipta mereka tanpa kebenaran di platform:

Nama Halaman: [redacted]
ID Facebook: [redacted]
Bahan yang Melanggar: [redacted]
Pemilik Hak Cipta: [redacted]

Maklumat pelanggaran serta dokumen yang berkenaan.pdf

Selaras dengan undang-undang hak cipta dan hak berkaitan, kami memohon agar anda segera mengeluarkan kandungan yang melanggar dan menghalang penerbitan semula kandungan serupa. Sila lengkapkan penghapusan dalam masa 48 jam dari penerimaan notis ini.

Jika anda percaya notis ini salah, sila hubungi kami dalam masa 24 jam untuk siasatan lanjut. Sila sediakan maklumat berikut untuk semakan:

1. Nama dan maklumat hubungan anda
2. Butiran tentang kandungan yang didakwa melanggar
3. Bukti pemilikan atau kuasa anda untuk menerbitkan kandungan tersebut

Selepas 48 jam, kami akan melengkapkan dokumen undang-undang dan bertindak mengikut undang-undang untuk melindungi hak dan harta pelanggan kami.

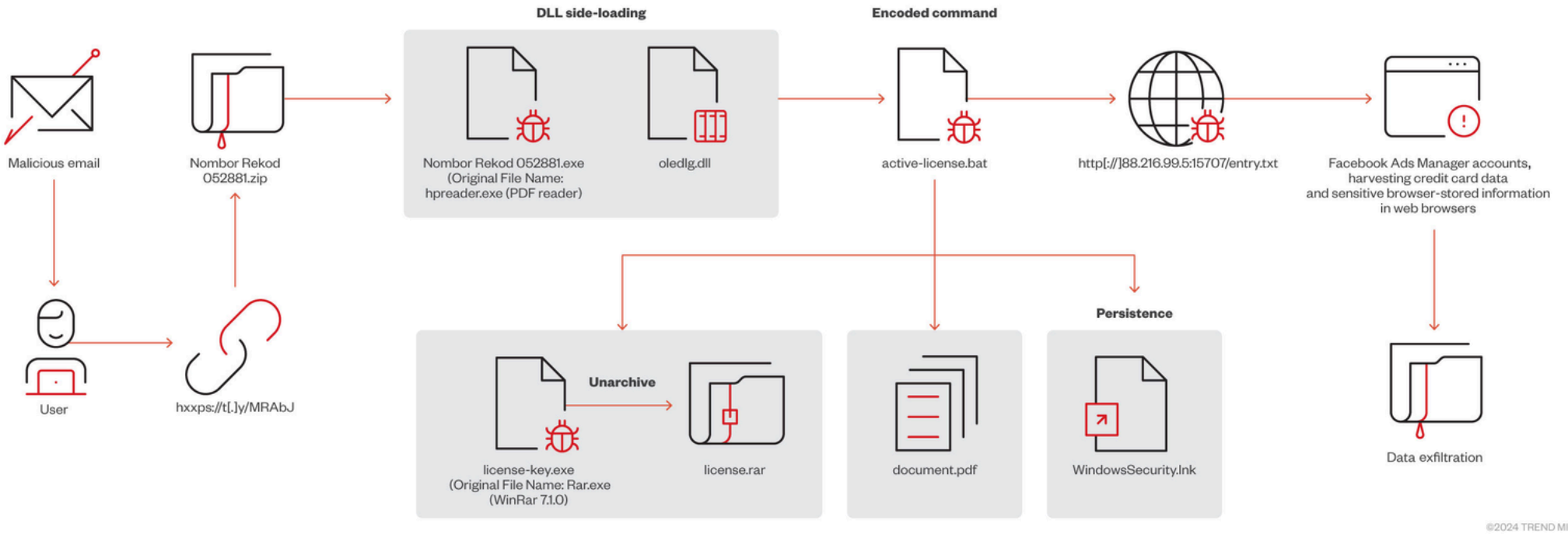
Terima kasih atas kerjasama dan pemahaman anda.

Yang benar,
[redacted]

Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 19 December 2024

Python-Based NodeStealer Version Targets Facebook Ads Manager



Twitter/X: @_rectifyq
Tiktok: @rectifyq

Source: Trend Micro
Date: 19 December 2024

Python-Based NodeStealer Version Targets Facebook Ads Manager

Other potentially similar campaigns using the same sideloaded dll, pdf decoy technique.