SecurityScorecard

# Tracking Adversaries through signals intelligence

POC 2023 Seoul, South Korea

Ryan Sherstobitoff
SVP, Threat Research & Intelligence

# AGENDA

1. What is SIGINT
2. Use of Signals intelligence
3. Foreign SIGINT operations

# Who am I?

- SVP Threat Research & Intelligence @ SecurityScorecard
- Former McAfee ATR (with a focus on Korea and Asia)
- POC 2019, 2020 speaker

STRIKE Team
SecurityScorecard Threat Research,
Intelligence, Knowledge and Engagement

# About STRIKE

STRIKE SecurityScorecard Threat Research, Intelligence, Knowledge and Engagement Team

- Team of threat researchers and developers focused on making the world a safer place
- Responding and engaging in threat research and analysis of major 0-days
- Developing capabilities to collect signals at scale

# What is SIGINT?

# Brief History of SIGINT

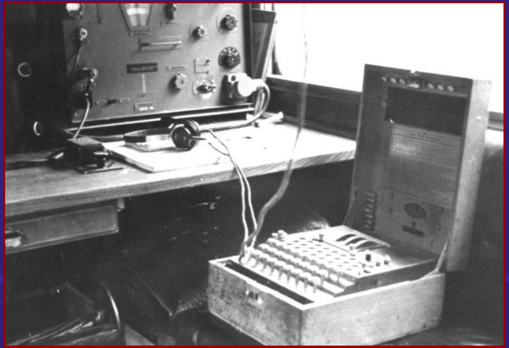
- Historically since world WW1 SIGINT was the practice of intercepting and decoding enemy communications (radio, etc)

- Transmissions evolved to including encryption / encoding methods - *introduction of modern cryptology*

- The US/UK and other 5-eye nations had to employ cryptologists “code breakers” to decode enemy messages

Bletchley Park United Kingdom - home of the code breakers (cira WW2)

US Army Signals Intelligence (circa 1943 - source Wikipedia)

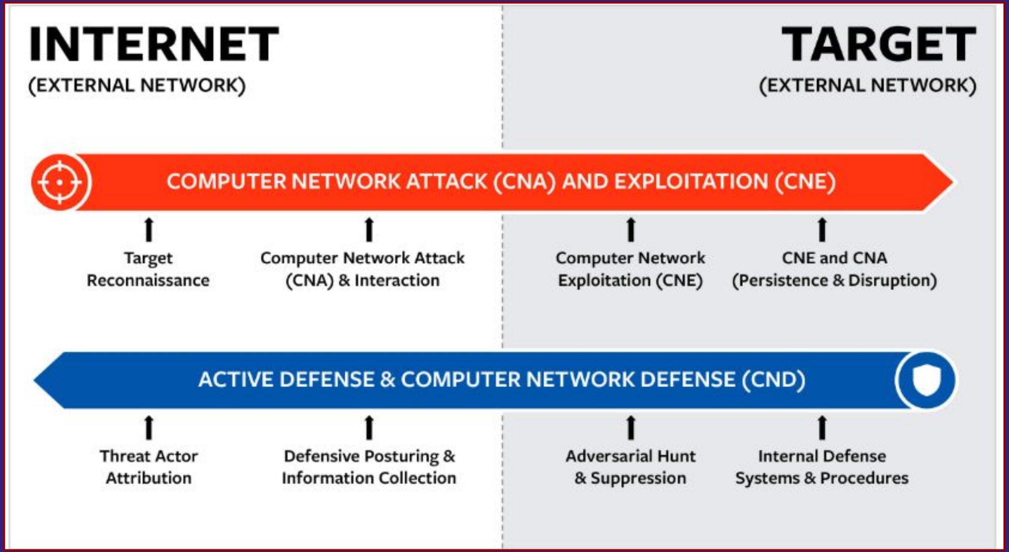


German Enigma Machine (circa 1941 - source Wikipedia)

# Modern Era of SIGINT

- SIGINT has since evolved to encompass sophisticated methods (often reserved for Nation-States)

- Signals can and are often collected via CNE/CNA (Computer Network Exploitation / Computer Network Attack) programs


INTERNET
(EXTERNAL NETWORK)
TARGET
(EXTERNAL NETWORK)
COMPUTER NETWORK ATTACK (CNA) AND EXPLOITATION (CNE)
Target Reconnaissance
Computer Network Attack (CNA) & Interaction
Computer Network Exploitation (CNE)
CNE and CNA (Persistence & Disruption)
ACTIVE DEFENSE & COMPUTER NETWORK DEFENSE (CND)
Threat Actor Attribution
Defensive Posturing & Information Collection
Adversarial Hunt & Suppression
Internal Defense Systems & Procedures

CNA/CNE (source https://www.fdd.org/analysis/2018/11/06/evolving-menace/)

# Use of Signals Intelligence

# SIGINT Technological Overview

- Operation of large scale SIGINT networks to intercept and collect signals (passive/active)
- Collection of signals at-scale (big data collection & analysis)
- Correlation of signals to identify patterns of activity - *actionable insights*

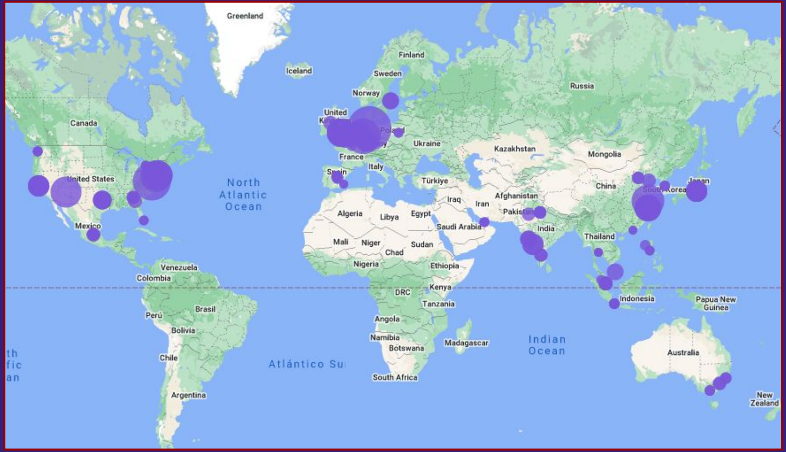
# SIGINT Technological Overview

- Traffic interception
  - TCP packet inspection through passive sniffing (span port capture)
  - Network signature detection applied to traffic live
- Passive Scanning
  - Scanning IPv4
- Active crawling
  - Crawling and scraping data from underground and open sources

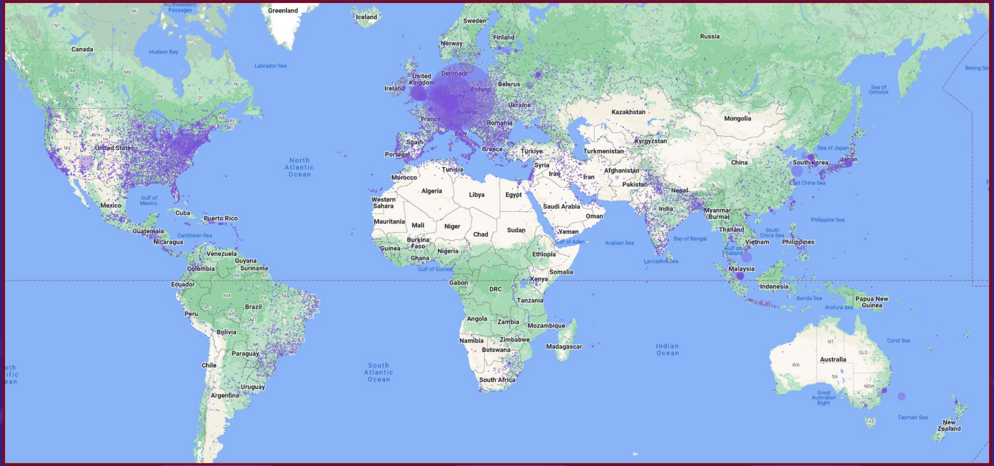
# Types of SIGINT

## Passive Sensor / Passive Scanning

- "Listening in" to network communications and collecting network borne signals
- Scanning the attack surfaces of organizations world-wide (IPv4 scanning)



SecurityScorecard Global Passive SIGINT sensor network collection points



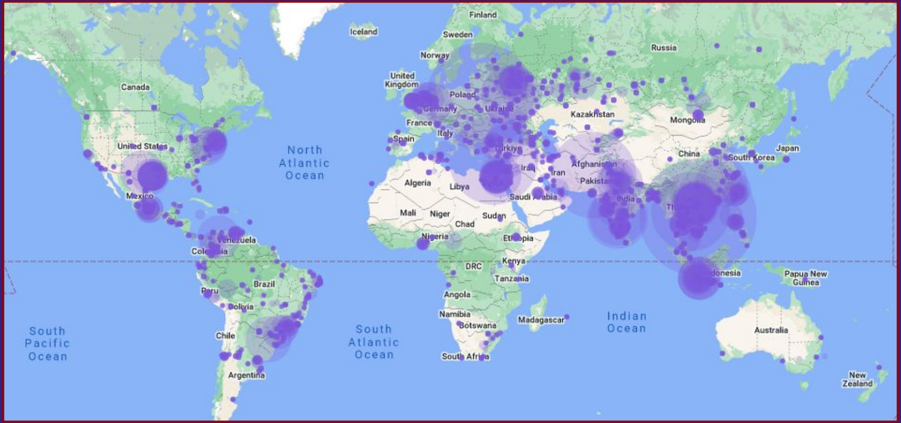
Global Attack Surface through attack surface SIGINT

SecurityScorecard

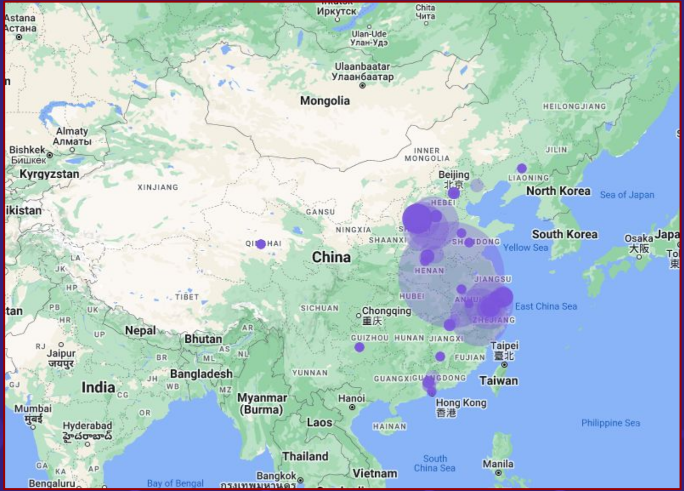
# Types of SIGINT

## Passive Sensor Collection

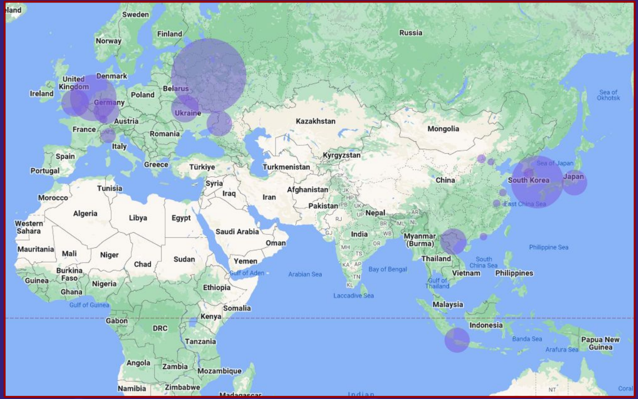
- Analyzing global network traffic through passive collection
- Applying network detection signatures at scale to “collected” traffic to and from assets (TCP flows for example)



Global sources of exploit traffic



Country Specific Sources of exploit traffic

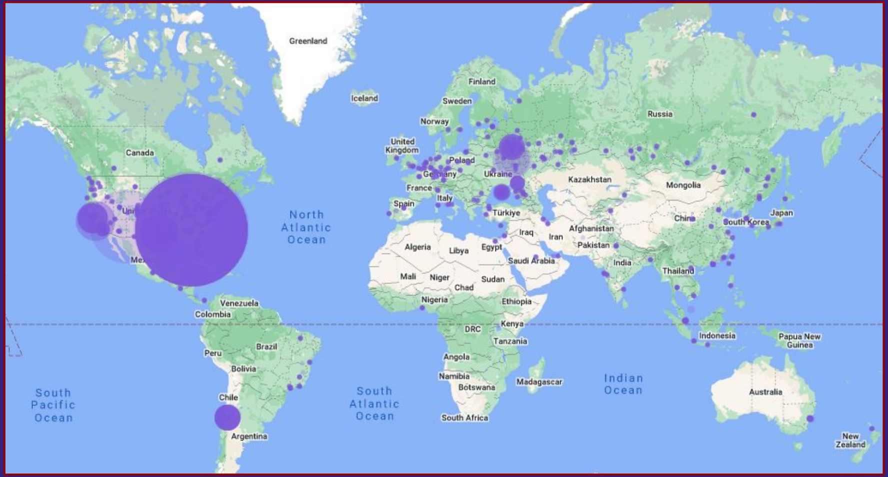


Global Sources of Brute Force Traffic

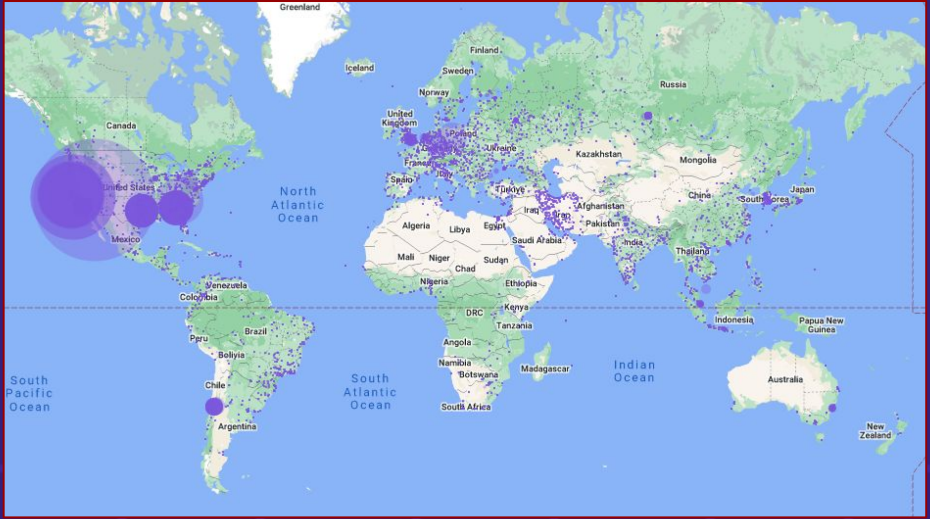
# Types of SIGINT

## TOR and Encrypted Communications

- Adversaries often use TOR as a means of anonymizing their traffic
- You can analyze outbound traffic and look for “bad guys”



Global destinations for RDP traffic through TOR

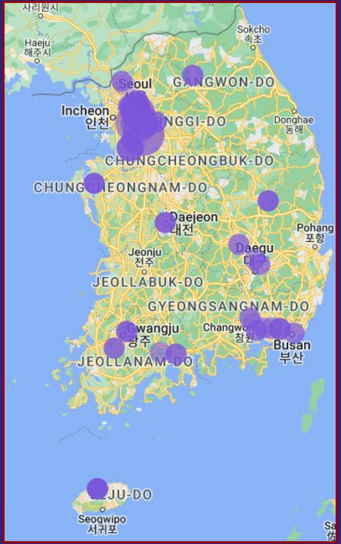


Global Destinations for TOR traffic (users exiting TOR and contacting clear web)

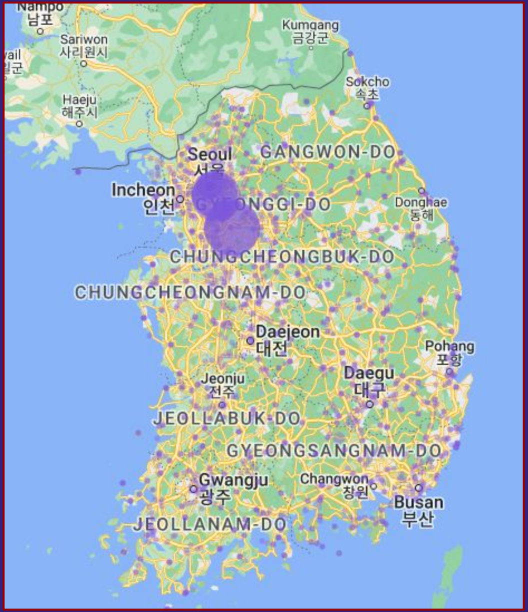
# SIGINT for Defensive Cyber

## Enumerating Attack Surface in South Korea

- Can enumerate the attack surface of Korea as a country (drill down into specific orgs)
- Identify what is exposed and what can be exploited - further drilling into observed attacks



Inbound Attacks on South Korea as seen by Passive SIGINT

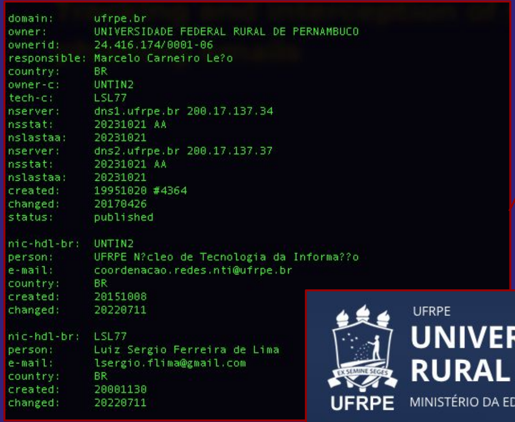


South Korea attack surface as seen by Passive SIGINT

# Types of SIGINT

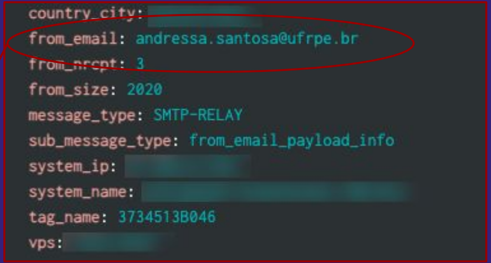
## Spam & Phishing Email interception

- Operation of SMTP relays globally
- Tracking and interception of spam and phishing emails
- Some are compromised users used to send spam and phishing “early indicators of hacking”



```
domain:      ufrpe.br
owner:       UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
ownerid:     24.416.174/0001-06
responsible: Marcelo Carneiro Le?o
country:     BR
owner-c:     UNTIN2
tech-c:      LSL77
nserver:     dns1.ufrpe.br 200.17.137.34
nsstat:      20231021 AA
nslastaa:    20231021
nserver:     dns2.ufrpe.br 200.17.137.37
nsstat:      20231021 AA
nslastaa:    20231021
created:     19951020 #4364
changed:     20170426
status:      published

nic-hdl-br:  UNTIN2
person:      UFRPE N?cleo de Tecnologia da Informa??o
e-mail:      coordenacao.redes.nti@ufrpe.br
country:     BR
created:     20151008
changed:     20220711

nic-hdl-br:  LSL77
person:      Luiz Sergio Ferreira de Lima
e-mail:      lsergio.flima@gmail.com
country:     BR
created:     20001130
changed:     20220711
```

UFRPE
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
MINISTÉRIO DA EDUCAÇÃO

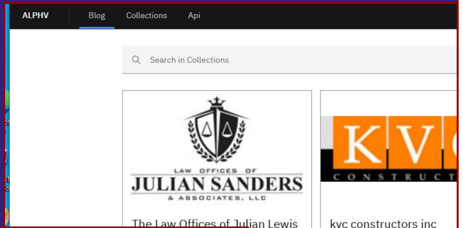


```
country_city: [redacted]
from_email: andressa.santosa@ufrpe.br
from_nrcpt: 3
from_size: 2020
message_type: SMTP-RELAY
sub_message_type: from_email_payload_info
system_ip: [redacted]
system_name: [redacted]
tag_name: 3734513B046
vps: [redacted]
```

Intercepted email

# Types of SIGINT

## Crawling Ransomware Operator sites



The Law Offices of Julian Lewis … FULL

…ia personal … The Law … and

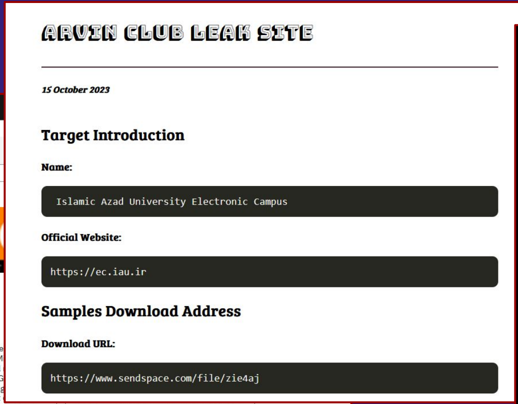
kvc constructors inc

Fri Oct 20 2023

KVC Constructors is a privately he… construction company based in M… Shores, Florida. We provide a full … construction services, including G… Construction, Construction Manag… and Design-Build to a diverse list …

Uploads — 1

Attachments — 8



ARVIN CLUB LEAK SITE

*15 October 2023*

**Target Introduction**

**Name:**

```
Islamic Azad University Electronic Campus
```

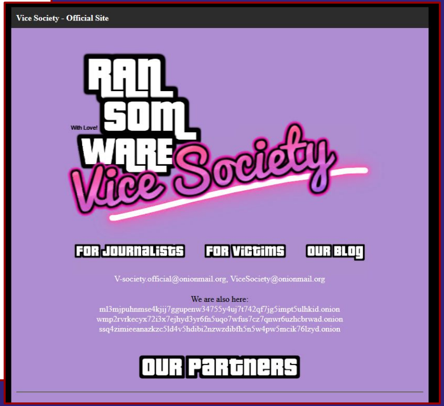
**Official Website:**

```
https://ec.iau.ir
```

**Samples Download Address**

**Download URL:**

```
https://www.sendspace.com/file/zie4aj
```

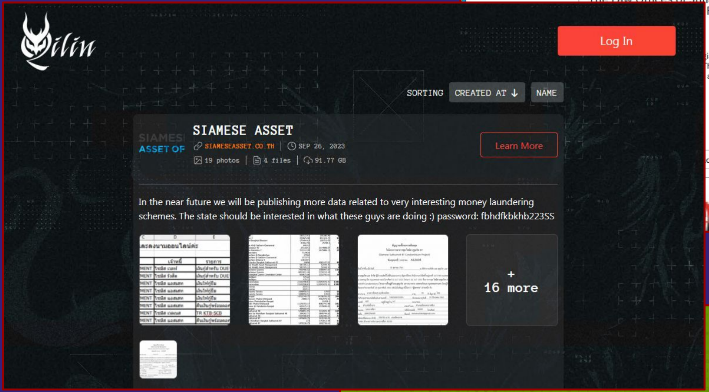


Vice Society - Official Site

V-society.official@onionmail.org, ViceSociety@onionmail.org

We are also here:
ml3mjpuhnmse4kjij7ggupenw34755y4uj7t742qf7jg5impt5ulhkid.onion
wmp2rvrkecyx72i3x7ejhyd3yr6fn5uqo7wfus7cz7qnwr6uzhcbrwad.onion
ssq4zimieeanazkzc5ld4v5hdibi2nzwzdibfh5n5w4pw5mcik76lzyd.onion

OUR PARTNERS

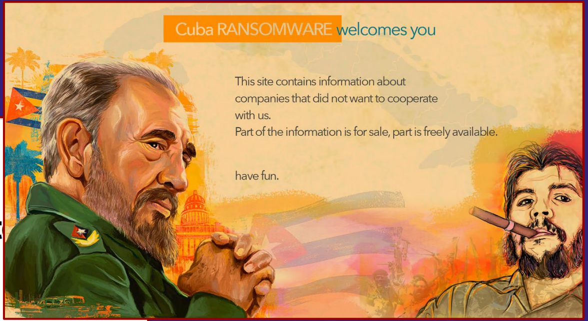


SIAMESE ASSET

SIAMESEASSET.CO.TH | SEP 26, 2023

19 photos | 4 files | 91.77 GB

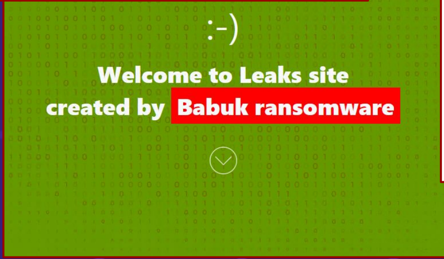
In the near future we will be publishing more data related to very interesting money laundering schemes. The state should be interested in what these guys are doing :) password: fbhdfkbkhb223SS



Cuba RANSOMWARE welcomes you

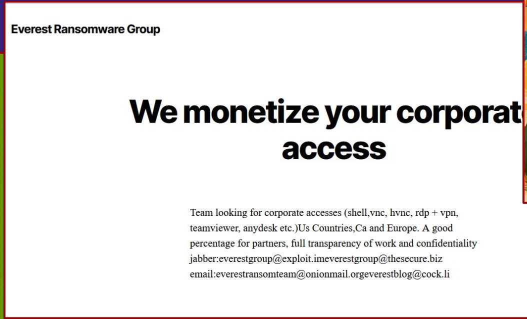
This site contains information about companies that did not want to cooperate with us.
Part of the information is for sale, part is freely available.

have fun.



:-)

Welcome to Leaks site created by Babuk ransomware



Everest Ransomware Group

# We monetize your corporat access

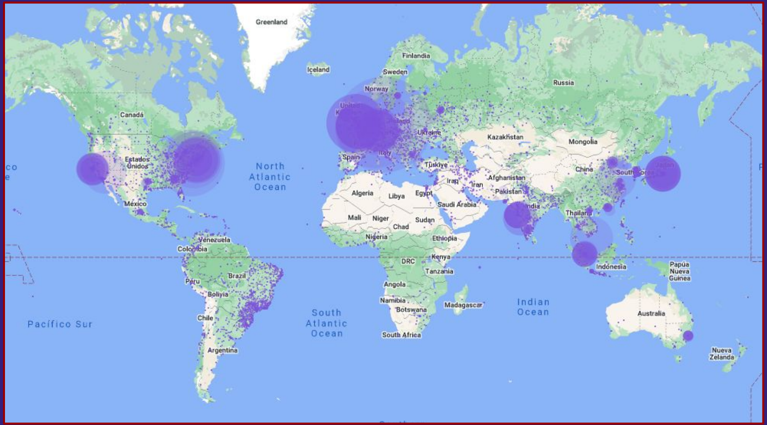
Team looking for corporate accesses (shell,vnc, hvnc, rdp + vpn, teamviewer, anydesk etc.)Us Countries,Ca and Europe. A good percentage for partners, full transparency of work and confidentiality
jabber:everestgroup@exploit.imeverestgroup@thesecure.biz
email:everestransomteam@onionmail.orgeverestblog@cock.li

SecurityScorecard

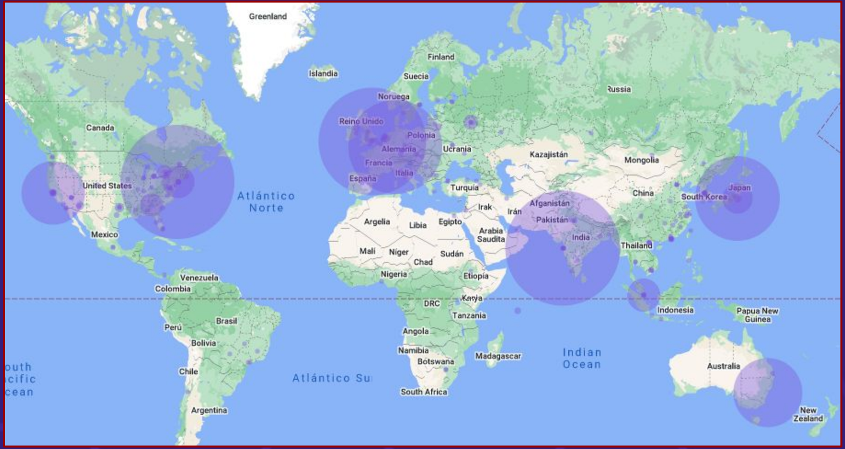
# SIGINT Network Visibility

## What signals can be collected

- Observations of source/destination traffic in general (ability to drill down into port specific info)
- Identification of global sources of malware traffic



Global sources of Network Connections (systems accessing the internet)

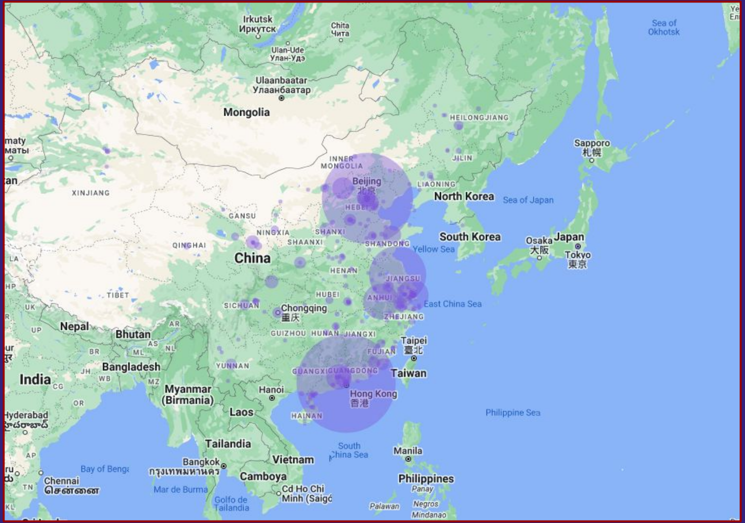


Global sources for Remote Desktop Traffic

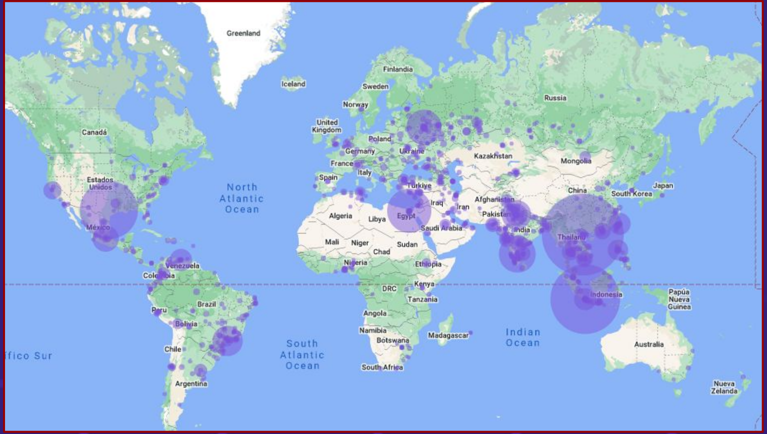
# Foreign SIGINT

## Passive Scanning and Passive Detection

- Collection of Foreign SIGINT inside state sponsored countries
- Collection of signals indicating sources for malicious traffic



SecurityScorecard Foreign SIGINT Collections (CN Region)



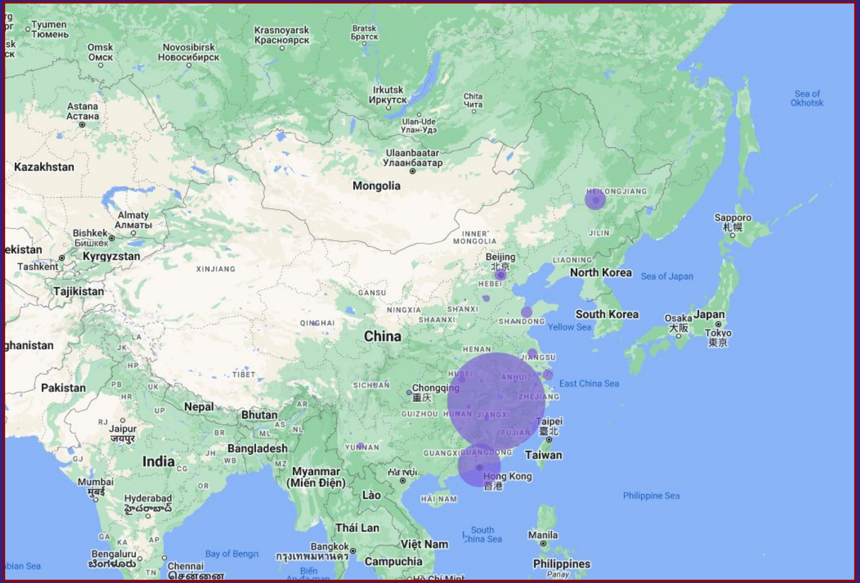
Global Sources of tagged  Malware Traffic

SecurityScorecard

# Foreign SIGINT Operations

# Foreign SIGINT

## Enumerating the Chinese Attack Surface

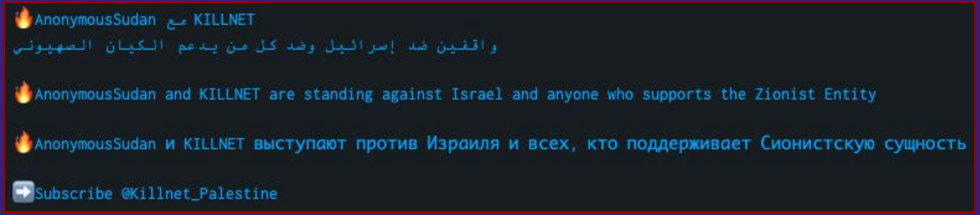


ModBus Devices on CN IPv4 space

# Collecting Hacker Chatter

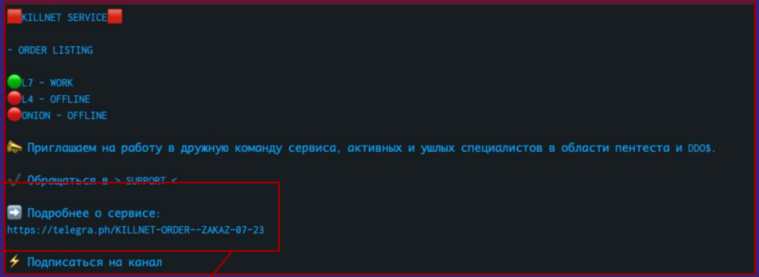
## Foreign SIGINT Operations

- Collecting Signals from adversary messaging platforms
- “Chatter” reveals insights about attacker TTPs



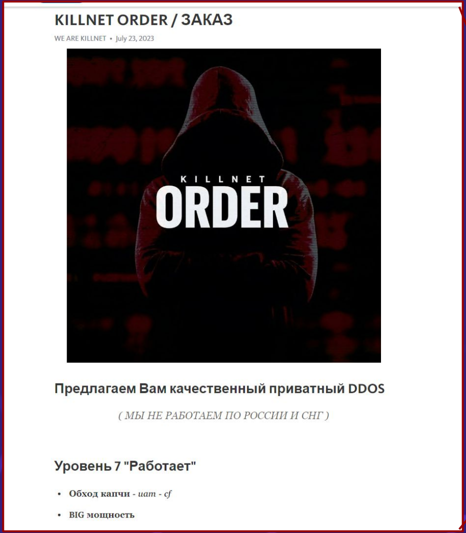
```
🔥AnonymousSudan مع KILLNET
واقفين ضد إسرائيل وضد كل من يدعم الكيان الصهيوني

🔥AnonymousSudan and KILLNET are standing against Israel and anyone who supports the Zionist Entity

🔥AnonymousSudan и KILLNET выступают против Израиля и всех, кто поддерживает Сионистскую сущность

➡️Subscribe @Killnet_Palestine
```

Adversary Dark Web chatter collection



```
🟥KILLNET SERVICE🟥

- ORDER LISTING

🟢L7 - WORK
🔴L4 - OFFLINE
🔴ONION - OFFLINE

📯 Приглашаем на работу в дружную команду сервиса, активных и ушлых специалистов в области пентеста и DDO$.

✔ Обращаться в > SUPPORT <

➡️ Подробнее о сервисе:
https://telegra.ph/KILLNET-ORDER--ZAKAZ-07-23

⚡ Подписаться на канал
```

Adversary Dark Web chatter collection



KILLNET ORDER / ЗАКАЗ

WE ARE KILLNET • July 23, 2023

Предлагаем Вам качественный приватный DDOS

*( МЫ НЕ РАБОТАЕМ ПО РОССИИ И СНГ )*

Уровень 7 "Работает"

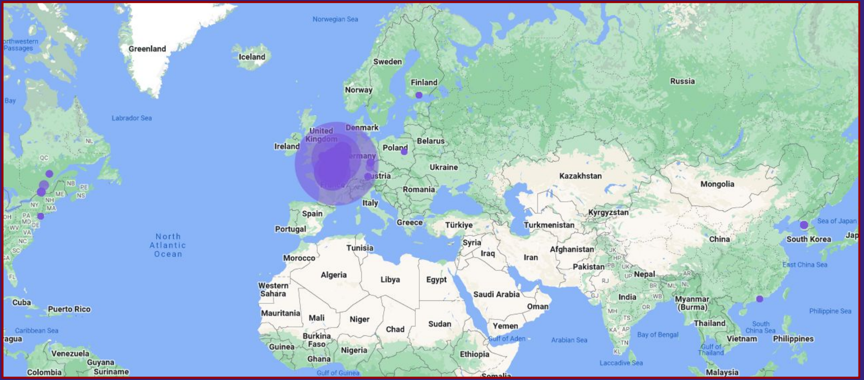
- **Обход капчи** - *uam* - *cf*
- **BIG мощность**

# Foreign SIGINT Operations: Tracking North Korean Cyber Actors

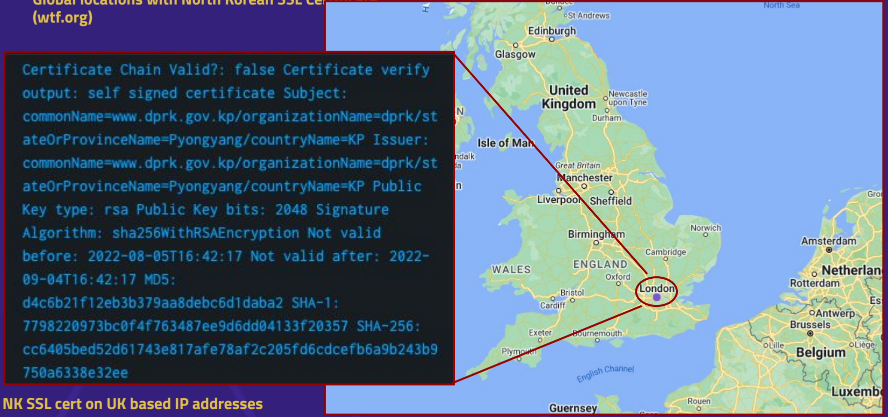
# Foreign SIGINT Ops

## Tracking NK Suspicious Infrastructure

- SSL Certificate that contains Pyongyang and WTF.org in the metadata (*looks suspicious!*)
- Another certificate containing dprk.gov.kp metadata found on an asset in London (*why is it there??*)
- Other non Pyongyang infrastructure could be North Korean hop-points to route traffic through (previous TTP)
- NK based certs contain a revealing email further tying showing NK
  - `postmaster@star-co.net.kp`
- Also appears in North Korean IP address space
  - `175.45.176.30`
  - `175.45.176.29`
  - `175.45.178.21`



Global locations with North Korean SSL Certificate
(wtf.org)



```
Certificate Chain Valid?: false Certificate verify
output: self signed certificate Subject:
commonName=www.dprk.gov.kp/organizationName=dprk/st
ateOrProvinceName=Pyongyang/countryName=KP Issuer:
commonName=www.dprk.gov.kp/organizationName=dprk/st
ateOrProvinceName=Pyongyang/countryName=KP Public
Key type: rsa Public Key bits: 2048 Signature
Algorithm: sha256WithRSAEncryption Not valid
before: 2022-08-05T16:42:17 Not valid after: 2022-
09-04T16:42:17 MD5:
d4c6b21f12eb3b379aa8debc6d1daba2 SHA-1:
7798220973bc0f4f763487ee9d6dd04133f20357 SHA-256:
cc6405bed52d61743e817afe78af2c205fd6cdcefb6a9b243b9
750a6338e32ee
```

NK SSL cert on UK based IP addresses

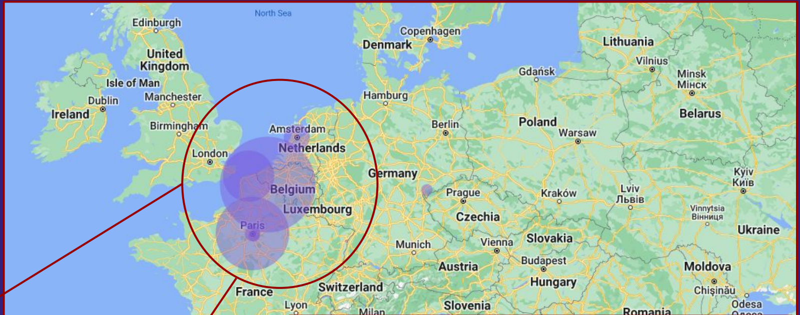
SSL Certificates containing star-co.net.kp

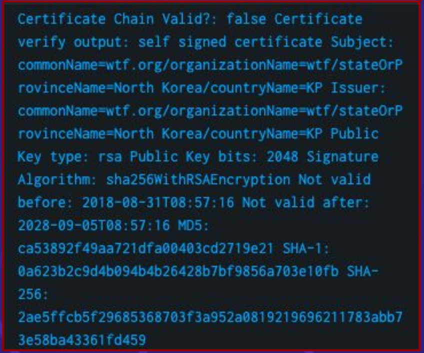
SecurityScorecard

# Foreign SIGINT Ops (continued)

## Tracking NK Suspicious Infrastructure

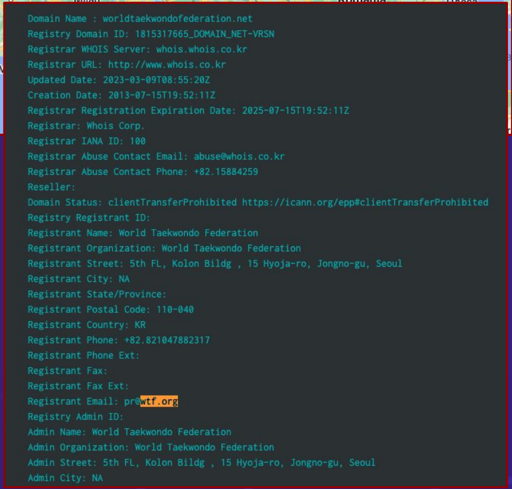
- ○ North Korean self-signed SSL certificate containing a domain wtf.org, which redirects to World Taekwondo - *not affiliated with North Korea*
- ○ Actual domain (wtf.org) hosted in South Korea IP space
- ○ Self-signed certs appear predominantly in European IP infrastructure
- ○ Concentrated in providers NK has used before





```
Certificate Chain Valid?: false Certificate
verify output: self signed certificate Subject:
commonName=wtf.org/organizationName=wtf/stateOrP
rovinceName=North Korea/countryName=KP Issuer:
commonName=wtf.org/organizationName=wtf/stateOrP
rovinceName=North Korea/countryName=KP Public
Key type: rsa Public Key bits: 2048 Signature
Algorithm: sha256WithRSAEncryption Not valid
before: 2018-08-31T08:57:16 Not valid after:
2028-09-05T08:57:16 MD5:
ca53892f49aa721dfa00403cd2719e21 SHA-1:
0a623b2c9d4b094b4b26428b7bf9856a703e10fb SHA-
256:
2ae5ffcb5f29685368703f3a952a0819219696211783abb7
3e58ba43361fd459
```

SSL Certificate Containing NK metadata



```
Domain Name : worldtaekwondofederation.net
Registry Domain ID: 1815317665_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.whois.co.kr
Registrar URL: http://www.whois.co.kr
Updated Date: 2023-03-09T08:55:20Z
Creation Date: 2013-07-15T19:52:11Z
Registrar Registration Expiration Date: 2025-07-15T19:52:11Z
Registrar: Whois Corp.
Registrar IANA ID: 100
Registrar Abuse Contact Email: abuse@whois.co.kr
Registrar Abuse Contact Phone: +82.15884259
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: World Taekwondo Federation
Registrant Organization: World Taekwondo Federation
Registrant Street: 5th FL, Kolon Bildg , 15 Hyoja-ro, Jongno-gu, Seoul
Registrant City: NA
Registrant State/Province:
Registrant Postal Code: 110-040
Registrant Country: KR
Registrant Phone: +82.821047882317
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pr@wtf.org
Registry Admin ID:
Admin Name: World Taekwondo Federation
Admin Organization: World Taekwondo Federation
Admin Street: 5th FL, Kolon Bildg , 15 Hyoja-ro, Jongno-gu, Seoul
Admin City: NA
```

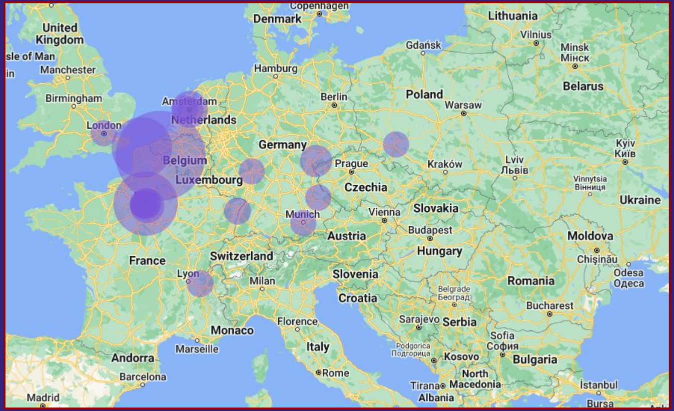
WTF.org is contained in World Taekwondo Federation WHOIS

SecurityScorecard

# Foreign SIGINT Ops (continued)

## Tracking NK Suspicious Infrastructure

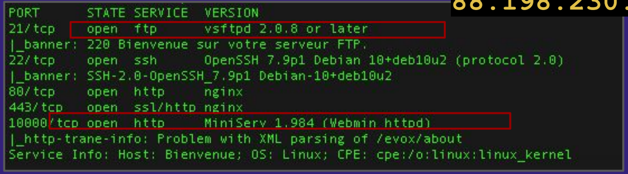
- There is many commonalities between systems in different countries (vsftp, some cases MiniServ, etc)
- Some running on port 7443 which has been used before for fake TLS type traffic in implants before
- Software tech-stack running on systems almost identical to each other



Infrastructure with self-signed certificate

Germany (Hetzner)

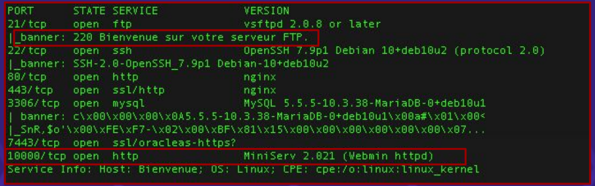
88.198.230.216



```
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_banner: 220 Bienvenue sur votre serveur FTP.
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
80/tcp    open  http     nginx
443/tcp   open  ssl/http nginx
10000/tcp open  http     MiniServ 1.984 (Webmin httpd)
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: Host: Bienvenue; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

France (OVH)

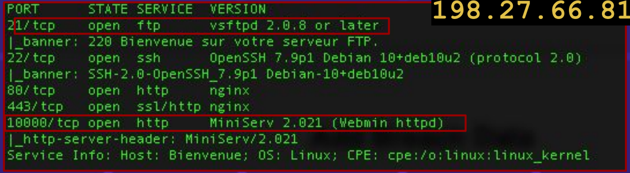
178.32.220.170



```
PORT      STATE SERVICE               VERSION
21/tcp    open  ftp                   vsftpd 2.0.8 or later
|_banner: 220 Bienvenue sur votre serveur FTP.
22/tcp    open  ssh                   OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
80/tcp    open  http                  nginx
443/tcp   open  ssl/http              nginx
3306/tcp  open  mysql                 MySQL 5.5.5-10.3.38-MariaDB-0+deb10u1
| banner: c\x00\x00\x00\x0A5.5.5-10.3.38-MariaDB-0+deb10u1\x00a#\x01\x00<
|_SnR,$o'\x00\xFE\xF7-\x02\x00\xBF\x81\x15\x00\x00\x00\x00\x00\x00\x07...
7443/tcp  open  ssl/oracleas-https?
10000/tcp open  http                  MiniServ 2.021 (Webmin httpd)
Service Info: Host: Bienvenue; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Canada (OVH)

198.27.66.81

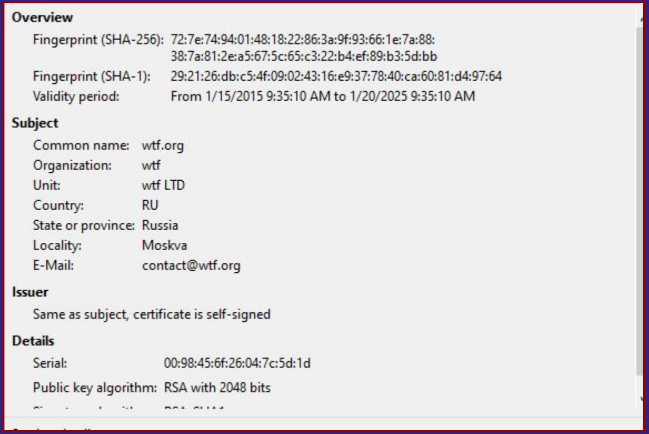


```
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
|_banner: 220 Bienvenue sur votre serveur FTP.
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
80/tcp    open  http     nginx
443/tcp   open  ssl/http nginx
10000/tcp open  http     MiniServ 2.021 (Webmin httpd)
|_http-server-header: MiniServ/2.021 [redacted]
Service Info: Host: Bienvenue; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

# Foreign SIGINT Ops (continued)

## Tracking NK Suspicious Infrastructure

- There are variations of the WTF certificate that include Russia/Moskva metadata, but with same WTF.org domain
- Appearing in United States on a VPS hosting provider Ramnode - *same FTP variation as seen before*
- Network Flow traffic indicates connections through MikroTik routers with VPN



**Overview**

Fingerprint (SHA-256): 72:7e:74:94:01:48:18:22:86:3a:9f:93:66:1e:7a:88:
38:7a:81:2e:a5:67:5c:65:c3:22:b4:ef:89:b3:5d:bb

Fingerprint (SHA-1): 29:21:26:db:c5:4f:09:02:43:16:e9:37:78:40:ca:60:81:d4:97:64

Validity period: From 1/15/2015 9:35:10 AM to 1/20/2025 9:35:10 AM

**Subject**

Common name: wtf.org
Organization: wtf
Unit: wtf LTD
Country: RU
State or province: Russia
Locality: Moskva
E-Mail: contact@wtf.org

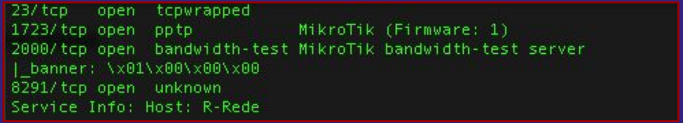
**Issuer**

Same as subject, certificate is self-signed

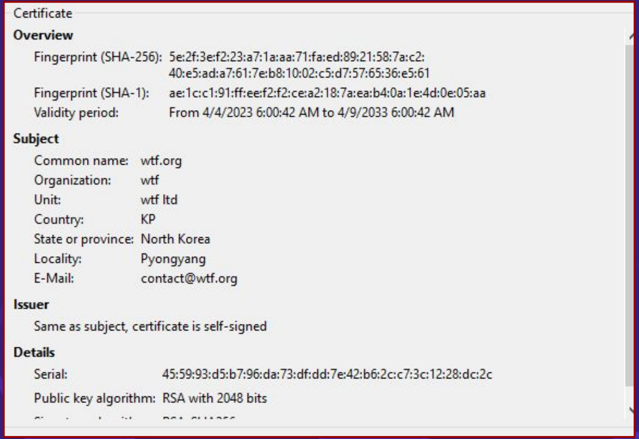
**Details**

Serial: 00:98:45:6f:26:04:7c:5d:1d
Public key algorithm: RSA with 2048 bits

SSL Certificate RUSSIA variation on IP asset in United States



```
23/tcp   open  tcpwrapped
1723/tcp open  pptp           MikroTik (Firmware: 1)
2000/tcp open  bandwidth-test MikroTik bandwidth-test server
|_banner: \x01\x00\x00\x00
8291/tcp open  unknown
Service Info: Host: R-Rede
```



Certificate

**Overview**

Fingerprint (SHA-256): 5e:2f:3e:f2:23:a7:1a:aa:71:fa:ed:89:21:58:7a:c2:
40:e5:ad:a7:61:7e:b8:10:02:c5:d7:57:65:36:e5:61

Fingerprint (SHA-1): ae:1c:c1:91:ff:ee:f2:f2:ce:a2:18:7a:ea:b4:0a:1e:4d:0e:05:aa

Validity period: From 4/4/2023 6:00:42 AM to 4/9/2033 6:00:42 AM

**Subject**

Common name: wtf.org
Organization: wtf
Unit: wtf ltd
Country: KP
State or province: North Korea
Locality: Pyongyang
E-Mail: contact@wtf.org

**Issuer**

Same as subject, certificate is self-signed

**Details**

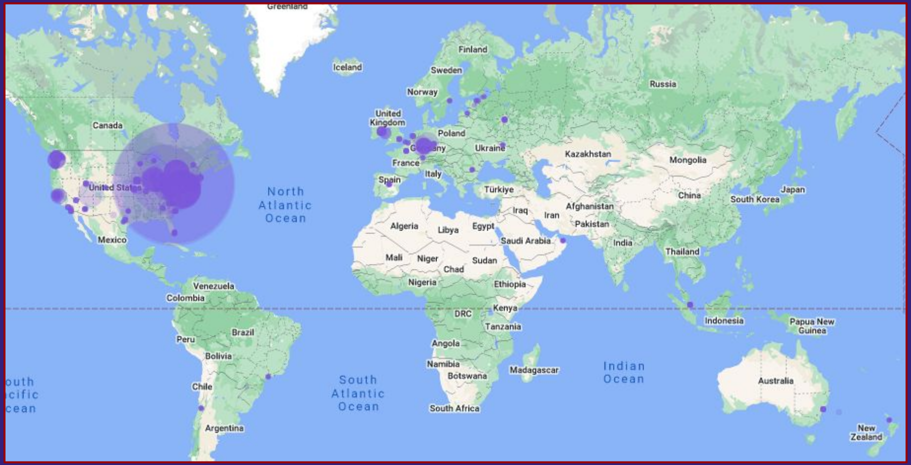
Serial: 45:59:93:d5:b7:96:da:73:df:dd:7e:42:b6:2c:c7:3c:12:28:dc:2c
Public key algorithm: RSA with 2048 bits

SSL Certificate North Korean version on European IPs

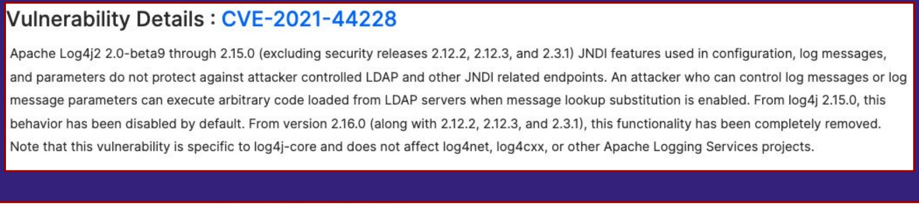
# Foreign SIGINT Ops

## Tracking Adversaries through Foreign SIGINT operations

- Bad guys trying to exploit these CISA Known Exploited Vulns (CVE-2021-44228, CVE-2021-35394, CVE-2019-3929, CVE-2020-5902, CVE-2017,7577)

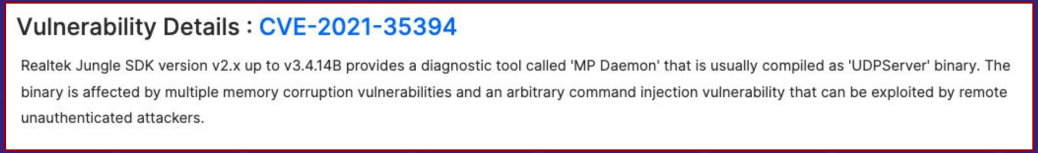


Destination locations for exploitation of clear web assets



Vulnerability Details : CVE-2021-44228

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.



Vulnerability Details : CVE-2021-35394

Realtek Jungle SDK version v2.x up to v3.4.14B provides a diagnostic tool called 'MP Daemon' that is usually compiled as 'UDPServer' binary. The binary is affected by multiple memory corruption vulnerabilities and an arbitrary command injection vulnerability that can be exploited by remote unauthenticated attackers.

# Foreign SIGINT Operations: Investigating PRC APT Activity

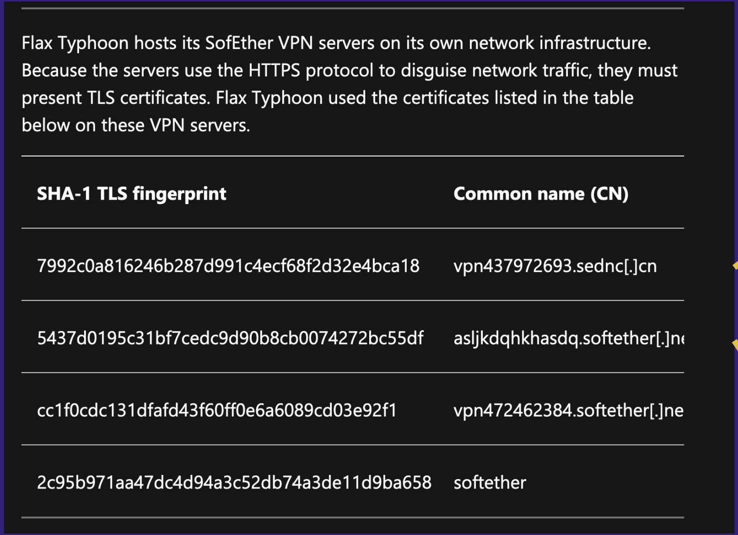
# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: New CN APT

- The STRIKE Team consulted SecurityScorecard's internal SIGINT collections to develop further insight into the activity of Flax Typhoon, a new, PRC-attributed APT group identified by Microsoft.
- This data helped the STRIKE Team identify a population of servers the group appears to use in addition to those Microsoft identified in its report.

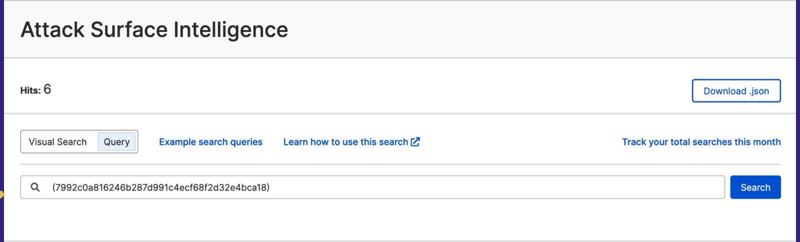
# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: New CN APT



Flax Typhoon hosts its SofEther VPN servers on its own network infrastructure. Because the servers use the HTTPS protocol to disguise network traffic, they must present TLS certificates. Flax Typhoon used the certificates listed in the table below on these VPN servers.

| SHA-1 TLS fingerprint | Common name (CN) |
|---|---|
| 7992c0a816246b287d991c4ecf68f2d32e4bca18 | vpn437972693.sednc[.]cn |
| 5437d0195c31bf7cedc9d90b8cb0074272bc55df | asljkdqhkhasdq.softether[.]n |
| cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1 | vpn472462384.softether[.]ne |
| 2c95b971aa47dc4d94a3c52db74a3de11d9ba658 | softether |

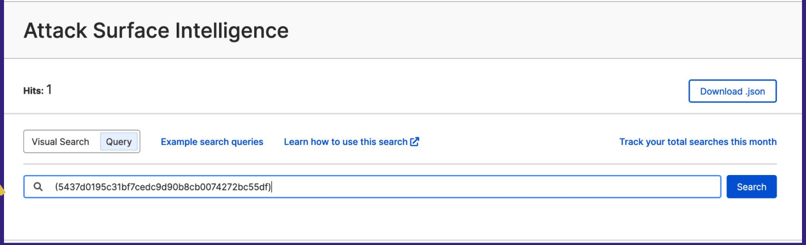


Attack Surface Intelligence

Hits: 6

(7992c0a816246b287d991c4ecf68f2d32e4bca18)

Download .json
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month
Search



Attack Surface Intelligence

Hits: 1

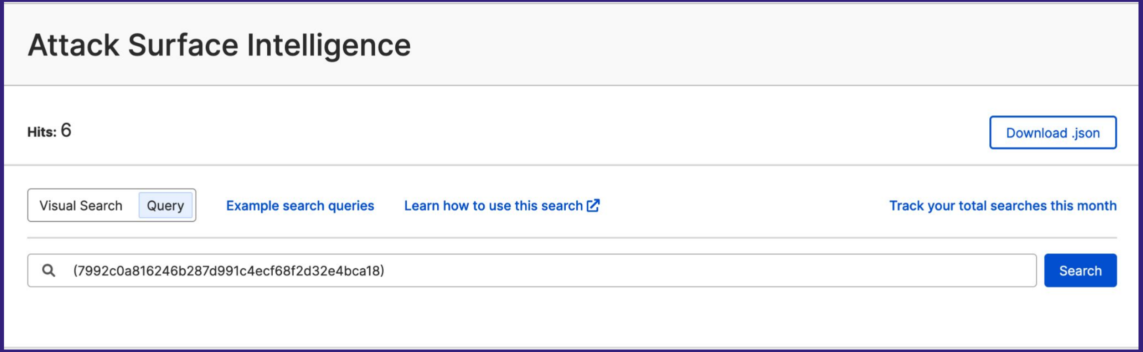
(5437d0195c31bf7cedc9d90b8cb0074272bc55df)

Download .json
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month
Search

Source of image at left:
https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

Images at right: SecurityScorecard's Attack Surface Intelligence Module

# Foreign SIGINT Ops (continued)



Attack Surface Intelligence

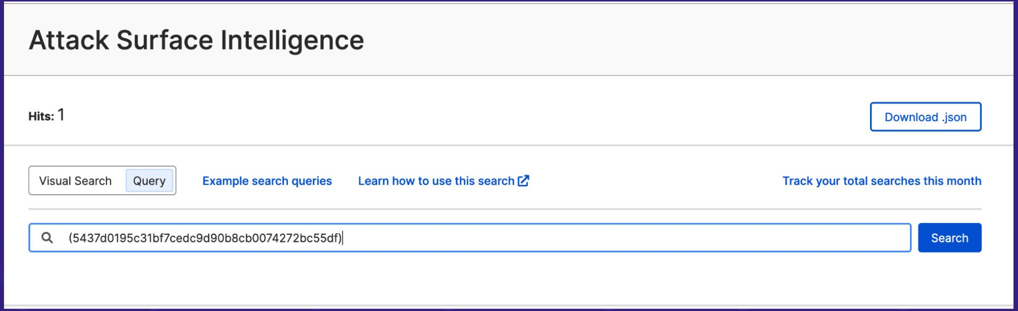
Hits: 6

Download .json
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month

(7992c0a816246b287d991c4ecf68f2d32e4bca18)

## Tracking Suspicious Infrastructure: New CN APT

- **7992c0a816246b287d991c4ecf68f2d32e4bca18**
  - 92.253.235[.]9
  - 45.204.1[.]203
  - 45.195.149[.]164
  - 182.61.132[.]155
  - 103.51.145[.]76
- **5437d0195c31bf7cedc9d90b8cb0074272bc55df**
  - 120.53.104[.]31



Attack Surface Intelligence

Hits: 1

Download .json
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month

(5437d0195c31bf7cedc9d90b8cb0074272bc55df)

# Foreign SIGINT Ops (continued)

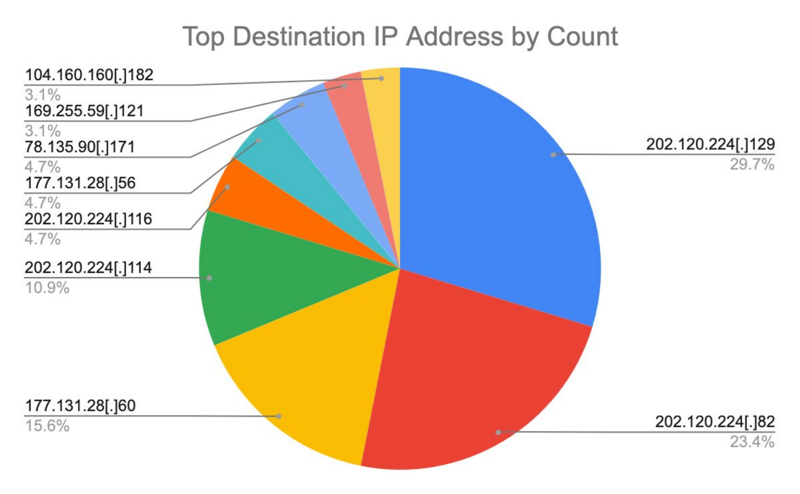
## Tracking Suspicious Infrastructure: New CN APT

- **The STRIKE Team investigated the newly-identified IP addresses further.**
  - A strategic partner's network flow (NetFlow) data yielded four Chinese IP addresses that communicated with one of these new Flax Typhoon-linked IoCs.
- **SecurityScorecard's attribution data linked all of these Chinese IP addresses to the same Chinese university, Fudan University.**
  - Concerns about Fudan University's possible role in PRC intelligence-gathering have previously surfaced in public commentary; these findings may raise similar concerns.

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: New CN APT

- **Four Chinese IP addresses communicated especially regularly with one of the IP addresses with a Flax Typhoon-linked TLS certificate. Those IP addresses are:**
  - 202.120.224[.]129
  - 202.120.224[.]82
  - 202.120.224[.]114
  - 202.120.224[.]116

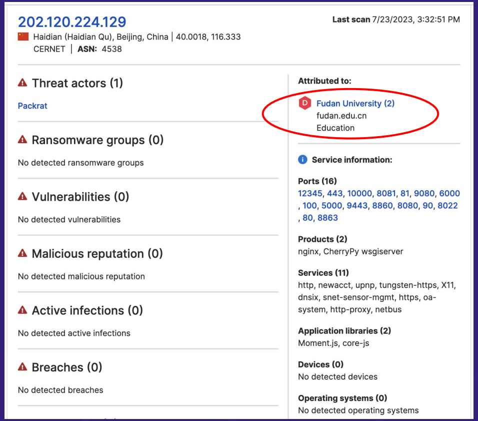


SecurityScorecard

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: New CN APT

- SecurityScorecard attributes each of these IP addresses to Fudan University:



202.120.224.129

Last scan 7/23/2023, 3:32:51 PM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (2)
fudan.edu.cn
Education

**Service information:**

**Ports (16)**
12345, 443, 10000, 8081, 81, 9080, 6000, 100, 5000, 9443, 8860, 8080, 90, 8022, 80, 8863

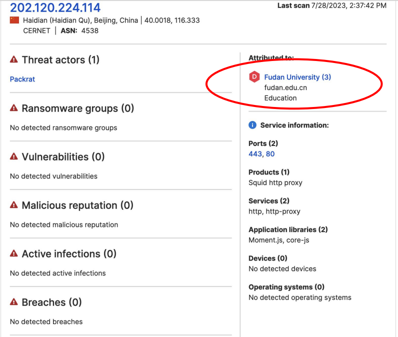
**Products (2)**
nginx, CherryPy wsgiserver

**Services (11)**
http, newacct, upnp, tungsten-https, X11, dnsix, snet-sensor-mgmt, https, oa-system, http-proxy, netbus

**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems



202.120.224.114

Last scan 7/28/2023, 2:37:42 PM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (3)
fudan.edu.cn
Education

**Service information:**

**Ports (2)**
443, 80

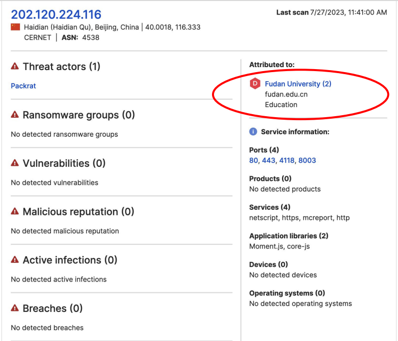
**Products (1)**
Squid http proxy

**Services (2)**
http, http-proxy

**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems



202.120.224.116

Last scan 7/27/2023, 11:41:00 AM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (2)
fudan.edu.cn
Education

**Service information:**

**Ports (4)**
80, 443, 4118, 8003

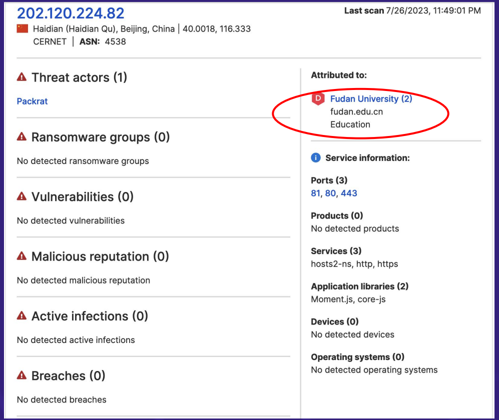
**Products (0)**
No detected products

**Services (4)**
netscript, https, mcreport, http

**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems



202.120.224.82

Last scan 7/26/2023, 11:49:01 PM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (2)
fudan.edu.cn
Education

**Service information:**

**Ports (3)**
81, 80, 443

**Products (0)**
No detected products

**Services (3)**
hosts2-ns, http, https

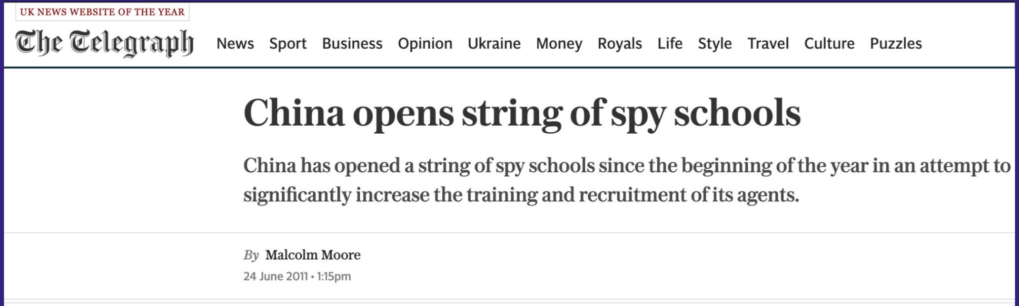
**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: New CN APT

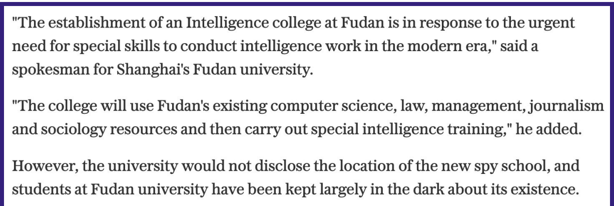

UK NEWS WEBSITE OF THE YEAR
The Telegraph
News Sport Business Opinion Ukraine Money Royals Life Style Travel Culture Puzzles

### China opens string of spy schools

China has opened a string of spy schools since the beginning of the year in an attempt to significantly increase the training and recruitment of its agents.

*By* Malcolm Moore

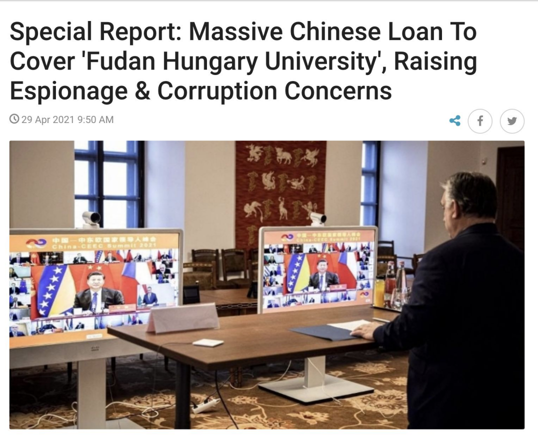
24 June 2011 • 1:15pm



"The establishment of an Intelligence college at Fudan is in response to the urgent need for special skills to conduct intelligence work in the modern era," said a spokesman for Shanghai's Fudan university.

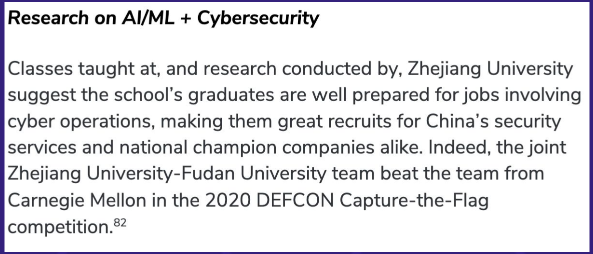
"The college will use Fudan's existing computer science, law, management, journalism and sociology resources and then carry out special intelligence training," he added.

However, the university would not disclose the location of the new spy school, and students at Fudan university have been kept largely in the dark about its existence.



### Special Report: Massive Chinese Loan To Cover 'Fudan Hungary University', Raising Espionage & Corruption Concerns

29 Apr 2021 9:50 AM

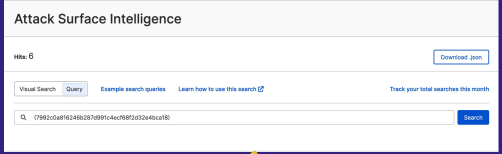


***Research on AI/ML + Cybersecurity***

Classes taught at, and research conducted by, Zhejiang University suggest the school's graduates are well prepared for jobs involving cyber operations, making them great recruits for China's security services and national champion companies alike. Indeed, the joint Zhejiang University-Fudan University team beat the team from Carnegie Mellon in the 2020 DEFCON Capture-the-Flag competition.[82]

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: New CN APT

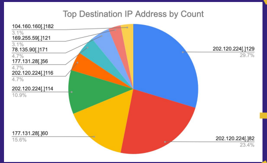


Attack Surface Intelligence

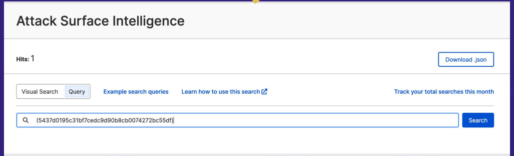
**Hits:** 6

(7992c0a816246b287d991c4ecf68f2d32e4bca18)

Download .json
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month
Search



Top Destination IP Address by Count

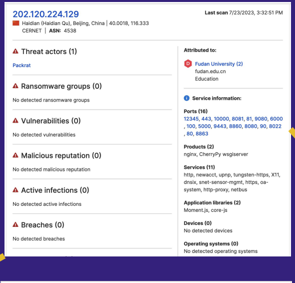


Attack Surface Intelligence

**Hits:** 1

(5437d0195c31bf7cedc9d90b8cb0074272bc55df)

Download .json
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month
Search



202.120.224.129

**Last scan** 7/23/2023, 3:32:51 PM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (2)
fudan.edu.cn
Education

**Service information:**

**Ports (16)**
12345, 443, 10000, 8081, 81, 9080, 6000, 100, 5000, 9443, 8860, 8080, 90, 8022, 80, 8863

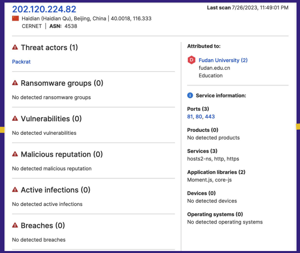
**Products (2)**
nginx, CherryPy wsgiserver

**Services (11)**
http, newacct, upnp, tungsten-https, X11, dnsix, snet-sensor-mgmt, https, oa-system, http-proxy, netbus

**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems



202.120.224.82

**Last scan** 7/26/2023, 11:49:01 PM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (2)
fudan.edu.cn
Education

**Service information:**

**Ports (3)**
81, 80, 443

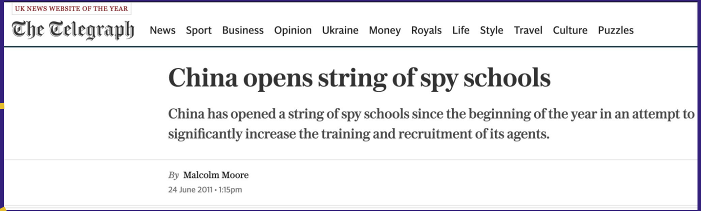
**Products (0)**
No detected products

**Services (3)**
hosts2-ns, http, https

**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems



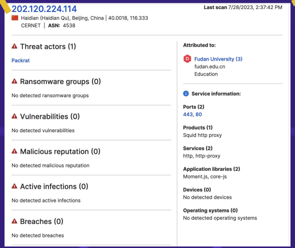
UK NEWS WEBSITE OF THE YEAR

The Telegraph

China opens string of spy schools

China has opened a string of spy schools since the beginning of the year in an attempt to significantly increase the training and recruitment of its agents.

*By* Malcolm Moore
24 June 2011 • 1:15pm



202.120.224.114

**Last scan** 7/28/2023, 2:37:42 PM

Haidian (Haidian Qu), Beijing, China | 40.0018, 116.333
CERNET | **ASN:** 4538

Threat actors (1)

Packrat

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Breaches (0)

No detected breaches

**Attributed to:**

Fudan University (3)
fudan.edu.cn
Education

**Service information:**

**Ports (2)**
443, 80

**Products (1)**
Squid http proxy

**Services (2)**
http, http-proxy

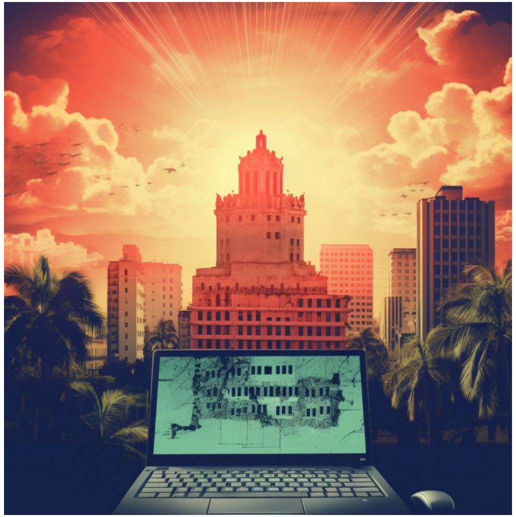
**Application libraries (2)**
Moment.js, core-js

**Devices (0)**
No detected devices

**Operating systems (0)**
No detected operating systems

STRIKE SecurityScorecard Threat Research, Intelligence, Knowledge and Engagement Team

# Foreign SIGINT Operations: Investigating New Cuba Ransomware IoCs



# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: Cuba Ransomware Group

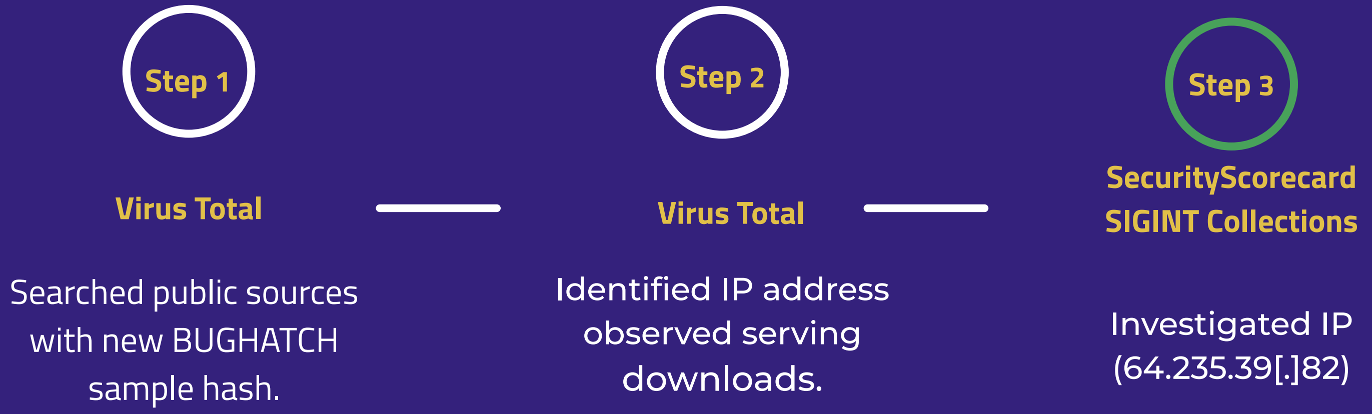
- **Cuba Ransomware group first surfaced in 2019; became more prominent in 2021.**
- **Notable features:**
    - Use of custom C2 malware (BUGHATCH)
    - Likely Russia-based

Source: Speartip.com

SecurityScorecard

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: Cuba Ransomware Group



**Step 1**

**Virus Total**

Searched public sources with new BUGHATCH sample hash.

**Step 2**

**Virus Total**

Identified IP address observed serving downloads.

**Step 3**

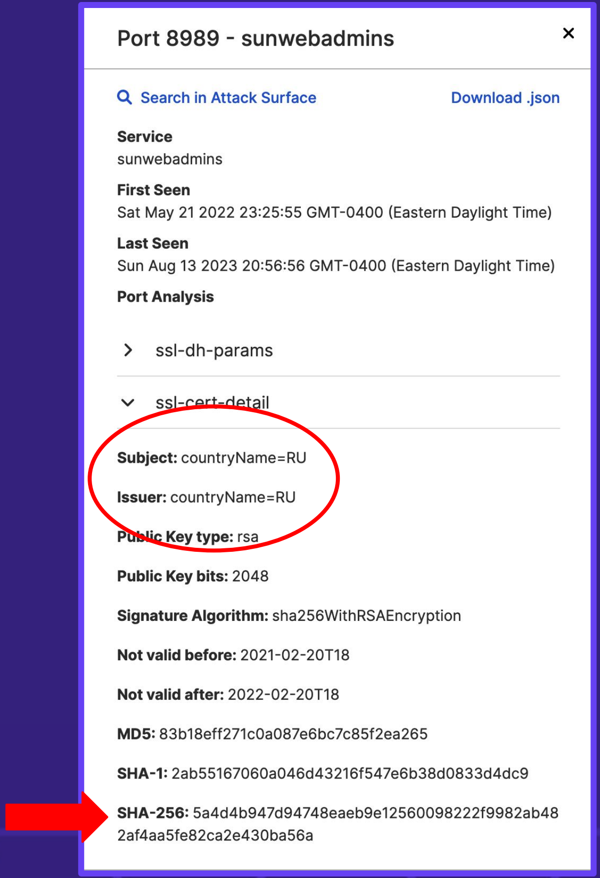
**SecurityScorecard SIGINT Collections**

Investigated IP (64.235.39[.]82)

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: Cuba Ransomware Group

- Searched IP serving BUGHATCH download in Attack Surface Intelligence.
- SSL certificate provoked some suspicion.
    - Why a Russian subject and issuer at US IP address?



Port 8989 - sunwebadmins

**Service**
sunwebadmins

**First Seen**
Sat May 21 2022 23:25:55 GMT-0400 (Eastern Daylight Time)

**Last Seen**
Sun Aug 13 2023 20:56:56 GMT-0400 (Eastern Daylight Time)

**Port Analysis**

**Subject:** countryName=RU

**Issuer:** countryName=RU

**Public Key type:** rsa

**Public Key bits:** 2048

**Signature Algorithm:** sha256WithRSAEncryption

**Not valid before:** 2021-02-20T18

**Not valid after:** 2022-02-20T18

**MD5:** 83b18eff271c0a087e6bc7c85f2ea265

**SHA-1:** 2ab55167060a046d43216f547e6b38d0833d4dc9

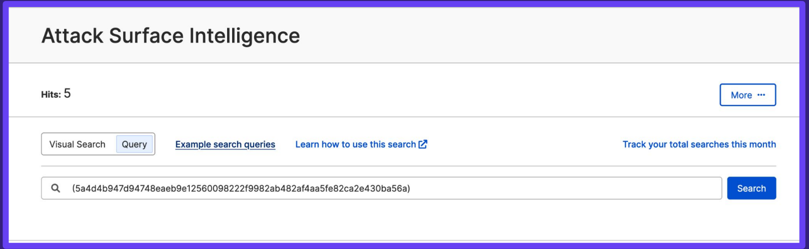
**SHA-256:** 5a4d4b947d94748eaeb9e12560098222f9982ab48
2af4aa5fe82ca2e430ba56a

SecurityScorecard

# Foreign SIGINT Ops (continued)

## Tracking Suspicious Infrastructure: Cuba Ransomware Group

- Searched certificate hash in SSC SIGINT data
- Found more IP addresses previously linked to Cuba with same hash
- Certificate hash itself is therefore probably a previously-unpublished Cuba IoC

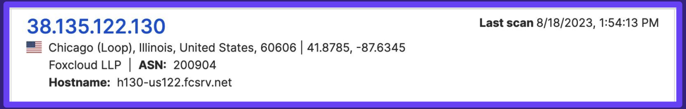


Attack Surface Intelligence

Hits: 5

(5a4d4b947d94748eaeb9e12560098222f9982ab482af4aa5fe82ca2e430ba56a)

More ···
Visual Search
Query
Example search queries
Learn how to use this search
Track your total searches this month
Search



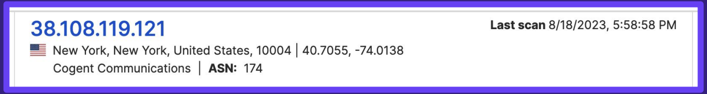
38.135.122.130

Last scan 8/18/2023, 1:54:13 PM

Chicago (Loop), Illinois, United States, 60606 | 41.8785, -87.6345

Foxcloud LLP | **ASN:** 200904

**Hostname:** h130-us122.fcsrv.net

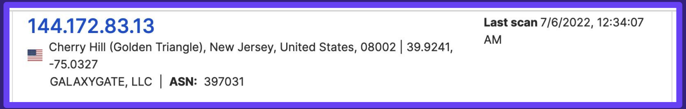


38.108.119.121

Last scan 8/18/2023, 5:58:58 PM

New York, New York, United States, 10004 | 40.7055, -74.0138

Cogent Communications | **ASN:** 174

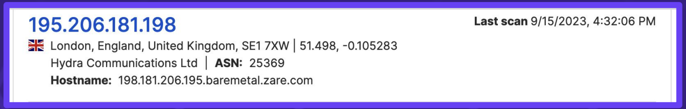


144.172.83.13

Last scan 7/6/2022, 12:34:07 AM

Cherry Hill (Golden Triangle), New Jersey, United States, 08002 | 39.9241, -75.0327

GALAXYGATE, LLC | **ASN:** 397031



195.206.181.198

Last scan 9/15/2023, 4:32:06 PM

London, England, United Kingdom, SE1 7XW | 51.498, -0.105283

Hydra Communications Ltd | **ASN:** 25369

**Hostname:** 198.181.206.195.baremetal.zare.com

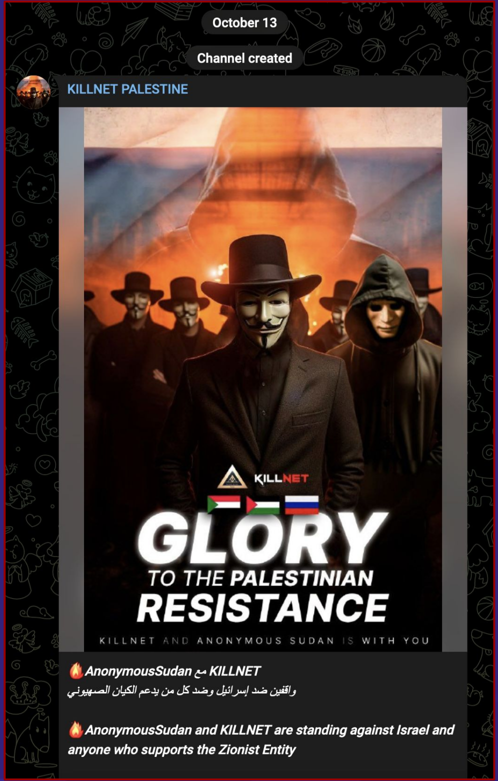
SecurityScorecard

# Foreign SIGINT Operations: DDW Chatter

# Collecting DDW Chatter

## Foreign SIGINT Operations

- Cyber and physical security-relevant collections regarding current Israel-Hamas war.
- Pairing these collections with our other SIGINT data can yield new insights into the conflict.



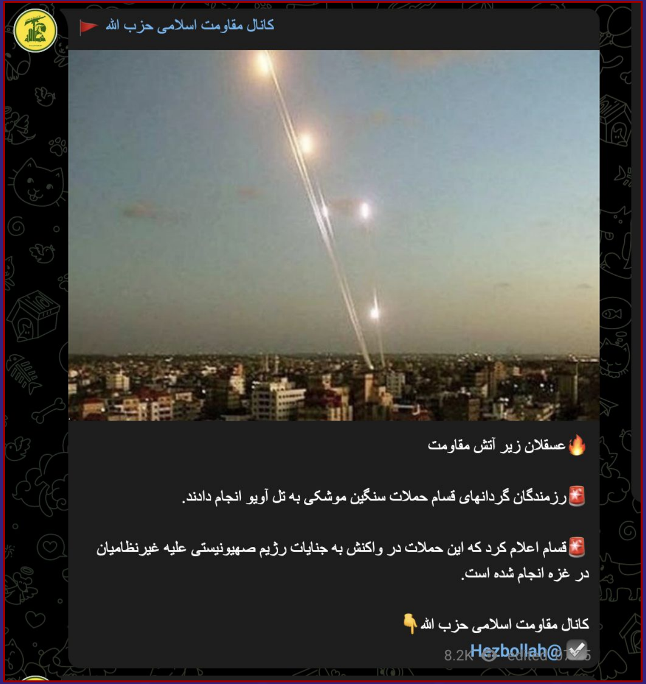
October 13

Channel created

KILLNET PALESTINE

*🔥AnonymousSudan مع KILLNET*
*واقفين ضد إسرائيل وضد كل من يدعم الكيان الصهيوني*

*🔥AnonymousSudan and KILLNET are standing against Israel and anyone who supports the Zionist Entity*



🚩 کانال مقاومت اسلامی حزب الله

🔥عسقلان زیر آتش مقاومت

🚨رزمندگان گردانهای قسام حملات سنگین موشکی به تل آویو انجام دادند.

🚨قسام اعلام کرد که این حملات در واکنش به جنایات رژیم صهیونیستی علیه غیرنظامیان در غزه انجام شده است.

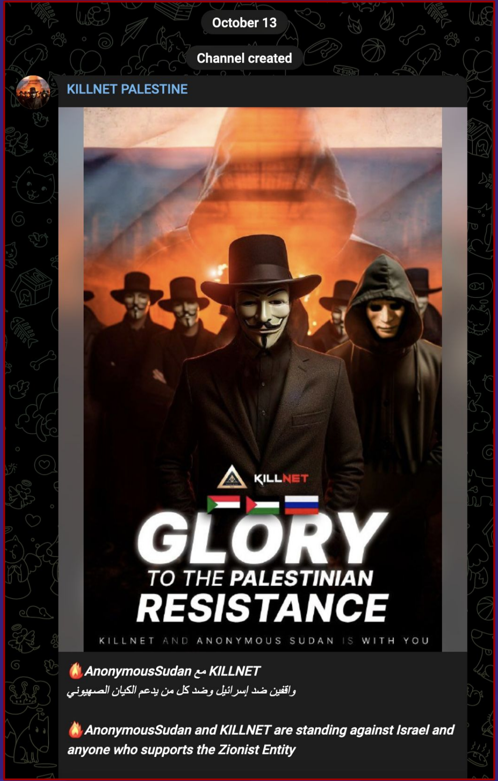
کانال مقاومت اسلامی حزب الله👇
Hezbollah@✅

8.2K

# Collecting DDW Chatter

## Foreign SIGINT Operations

- Chats generally reflect publicly reported trends
- SSC analysis can enrich public reporting



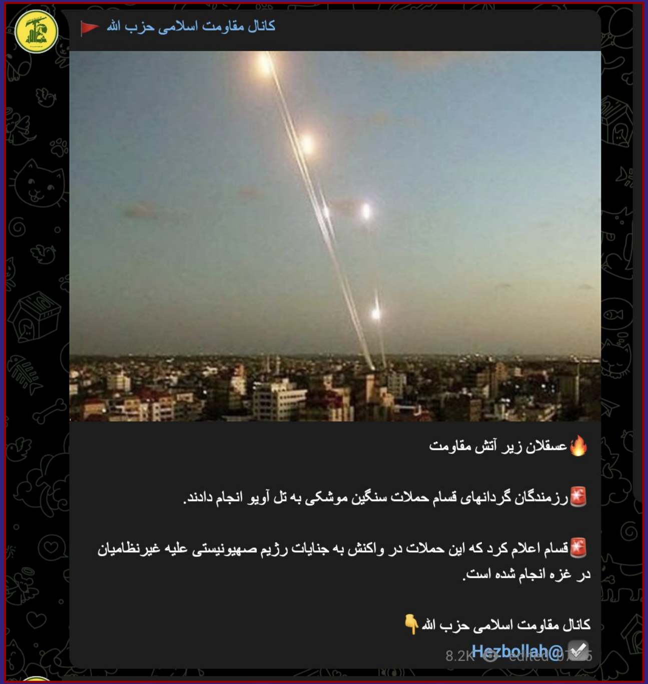
October 13

Channel created

KILLNET PALESTINE

🔥AnonymousSudan مع KILLNET
واقفين ضد إسرائيل وضد كل من يدعم الكيان الصهيوني

🔥AnonymousSudan and KILLNET are standing against Israel and anyone who supports the Zionist Entity



🚩 کانال مقاومت اسلامی حزب الله

🔥عسقلان زیر آتش مقاومت

🚨رزمندگان گردانهای قسام حملات سنگین موشکی به تل آویو انجام دادند.

🚨قسام اعلام کرد که این حملات در واکنش به جنایات رژیم صهیونیستی علیه غیرنظامیان
در غزه انجام شده است.

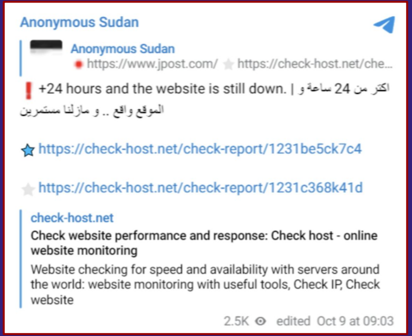
کانال مقاومت اسلامی حزب الله👇
Hezbollah@☑️

8.2K edited 07:55

# Analyzing Hacker Chatter

## Broader Cyber Trend

- Pro-Palestinian hacktivism, much of it from outside of the region
  - Russia-linked groups claim DDoS attacks against Israel



Anonymous Sudan

Anonymous Sudan
● https://www.jpost.com/ ★ https://check-host.net/che...

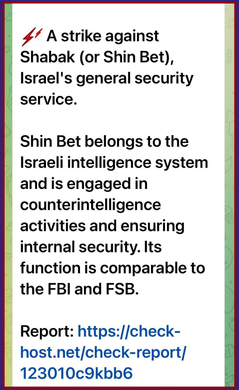
❗ +24 hours and the website is still down. | اكثر من 24 ساعة و الموقع واقع .. و مازلنا مستمرين

★ https://check-host.net/check-report/1231be5ck7c4

★ https://check-host.net/check-report/1231c368k41d

check-host.net
Check website performance and response: Check host - online website monitoring
Website checking for speed and availability with servers around the world: website monitoring with useful tools, Check IP, Check website

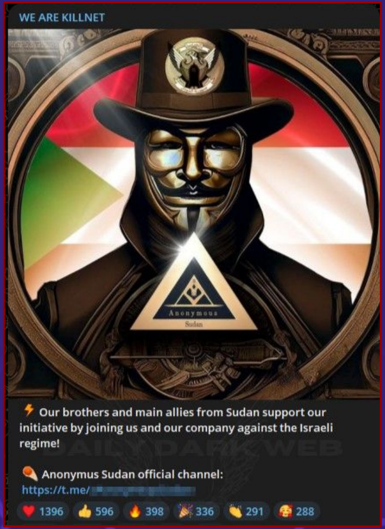
2.5K edited Oct 9 at 09:03



⚡ A strike against Shabak (or Shin Bet), Israel's general security service.

Shin Bet belongs to the Israeli intelligence system and is engaged in counterintelligence activities and ensuring internal security. Its function is comparable to the FBI and FSB.

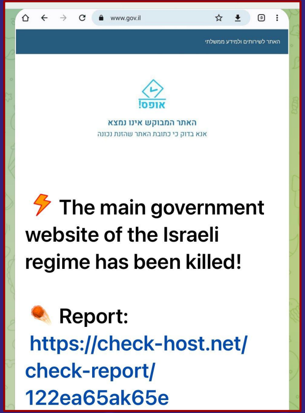
Report: https://check-host.net/check-report/123010c9kbb6



⚡ Our brothers and main allies from Sudan support our initiative by joining us and our company against the Israeli regime!

Anonymus Sudan official channel:
https://t.me/[redacted]

❤ 1396 👍 596 🔥 398 🎉 336 👏 291 😍 288



האתר המבוקש אינו נמצא
אנא בדוק כי כתובת האתר שהזנת נכונה

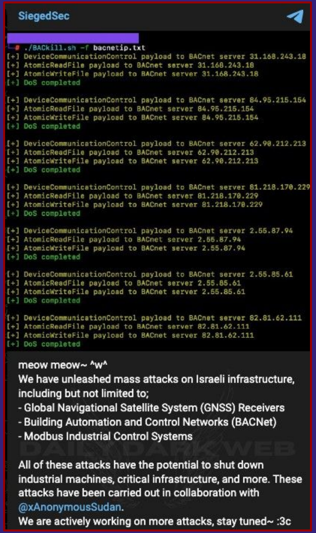
⚡ The main government website of the Israeli regime has been killed!

Report: https://check-host.net/check-report/122ea65ak65e

# Analyzing Hacker Chatter

## Enrichment using SSC SIGINT

- Hacktivists claim attack against Israeli ICS
- SSC scan data identifies more exposed servers than those listed in attack claim

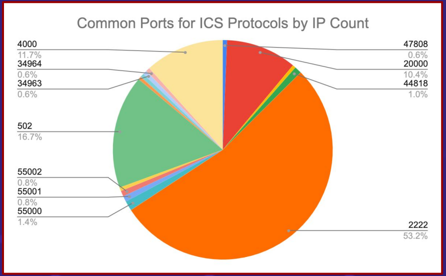


SiegedSec

```
[redacted]
└─# ./BACkill.sh -f bacnetip.txt
[+] DeviceCommunicationControl payload to BACnet server 31.168.243.18
[+] AtomicReadFile payload to BACnet server 31.168.243.18
[+] AtomicWriteFile payload to BACnet server 31.168.243.18
[+] DoS completed

[+] DeviceCommunicationControl payload to BACnet server 84.95.215.154
[+] AtomicReadFile payload to BACnet server 84.95.215.154
[+] AtomicWriteFile payload to BACnet server 84.95.215.154
[+] DoS completed

[+] DeviceCommunicationControl payload to BACnet server 62.90.212.213
[+] AtomicReadFile payload to BACnet server 62.90.212.213
[+] AtomicWriteFile payload to BACnet server 62.90.212.213
[+] DoS completed

[+] DeviceCommunicationControl payload to BACnet server 81.218.170.229
[+] AtomicReadFile payload to BACnet server 81.218.170.229
[+] AtomicWriteFile payload to BACnet server 81.218.170.229
[+] DoS completed

[+] DeviceCommunicationControl payload to BACnet server 2.55.87.94
[+] AtomicReadFile payload to BACnet server 2.55.87.94
[+] AtomicWriteFile payload to BACnet server 2.55.87.94
[+] DoS completed

[+] DeviceCommunicationControl payload to BACnet server 2.55.85.61
[+] AtomicReadFile payload to BACnet server 2.55.85.61
[+] AtomicWriteFile payload to BACnet server 2.55.85.61
[+] DoS completed

[+] DeviceCommunicationControl payload to BACnet server 82.81.62.111
[+] AtomicReadFile payload to BACnet server 82.81.62.111
[+] AtomicWriteFile payload to BACnet server 82.81.62.111
[+] DoS completed
```

meow meow~ ^w^
We have unleashed mass attacks on Israeli infrastructure, including but not limited to;
- Global Navigational Satellite System (GNSS) Receivers
- Building Automation and Control Networks (BACNet)
- Modbus Industrial Control Systems

All of these attacks have the potential to shut down industrial machines, critical infrastructure, and more. These attacks have been carried out in collaboration with @xAnonymousSudan.
We are actively working on more attacks, stay tuned~ :3c



| Protocol | Port | Israeli IP Count |
|---|---|---|
| Ethernet/IP | 2222 | 4740 |
| Modbus TCP | 502 | 1490 |
| ROC PLus | 4000 | 1040 |
| DNP3 | 20000 | 926 |
| FL-net | 55000 | 128 |
| Ethernet/IP | 44818 | 92 |
| FL-net | 55001 | 75 |
| FL-net | 55002 | 75 |
| BACnet | 47808 | 56 |
| PROFINET | 34963 | 53 |
| PROFINET | 34964 | 53 |
| PROFINET | 34962 | 50 |
| FL-net | 55003 | 48 |
| EtherCAT | 34980 | 43 |
| OPC UA Discovery Server | 4840 | 41 |

SecurityScorecard

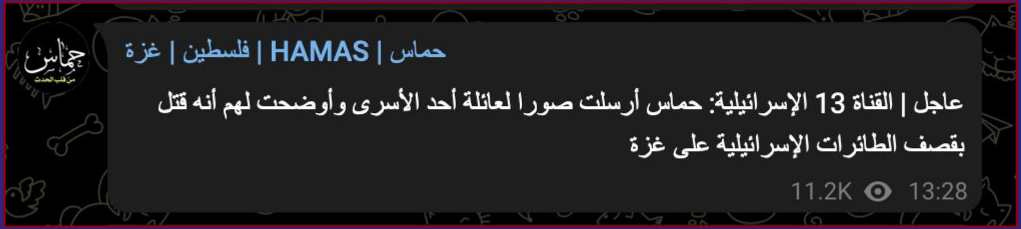
# Analyzing DDW Chatter

## Broader Physical Security Trend

- Assignment of culpability for civilian casualties
- Reports of Hamas rocket attacks

## SSC Analytical Enrichment

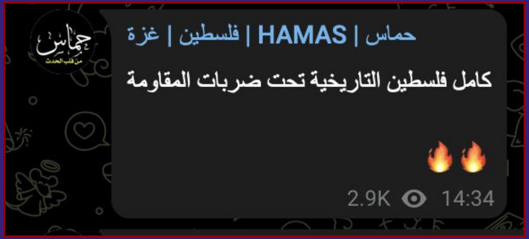
- Attention to DDW collections reveals priorities in Hamas messaging about events in question
  - Wording of claims suggests attempts to undermine claims about Israel's defensive capabilities



حماس | HAMAS | فلسطين | غزة

عاجل | القناة 13 الإسرائيلية: حماس أرسلت صورا لعائلة أحد الأسرى وأوضحت لهم أنه قتل
بقصف الطائرات الإسرائيلية على غزة

11.2K 👁 13:28



حماس | HAMAS | فلسطين | غزة

كامل فلسطين التاريخية تحت ضربات المقاومة

🔥🔥

2.9K 👁 14:34

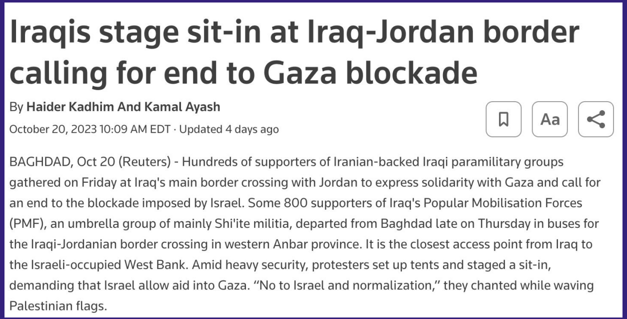
# Analyzing DDW Chatter

## Broader Physical Security Trend

- Possible regional escalation
  - Fears of Iranian involvement

## SSC Analytical Enrichment

- Collections suggest Hamas' awareness of international audience and possibilities of regional escalation



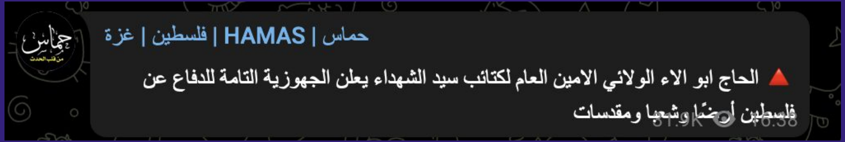
### Iraqis stage sit-in at Iraq-Jordan border calling for end to Gaza blockade

By **Haider Kadhim And Kamal Ayash**

October 20, 2023 10:09 AM EDT · Updated 4 days ago

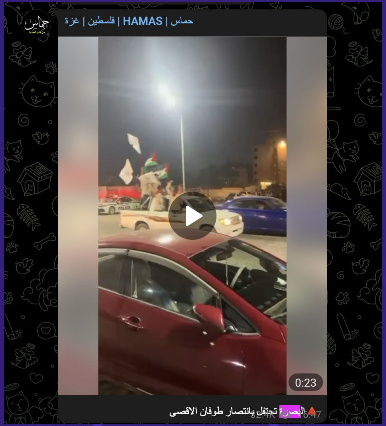
BAGHDAD, Oct 20 (Reuters) - Hundreds of supporters of Iranian-backed Iraqi paramilitary groups gathered on Friday at Iraq's main border crossing with Jordan to express solidarity with Gaza and call for an end to the blockade imposed by Israel. Some 800 supporters of Iraq's Popular Mobilisation Forces (PMF), an umbrella group of mainly Shi'ite militia, departed from Baghdad late on Thursday in buses for the Iraqi-Jordanian border crossing in western Anbar province. It is the closest access point from Iraq to the Israeli-occupied West Bank. Amid heavy security, protesters set up tents and staged a sit-in, demanding that Israel allow aid into Gaza. "No to Israel and normalization," they chanted while waving Palestinian flags.

Source: *Reuters*



حماس | HAMAS | فلسطين | غزة

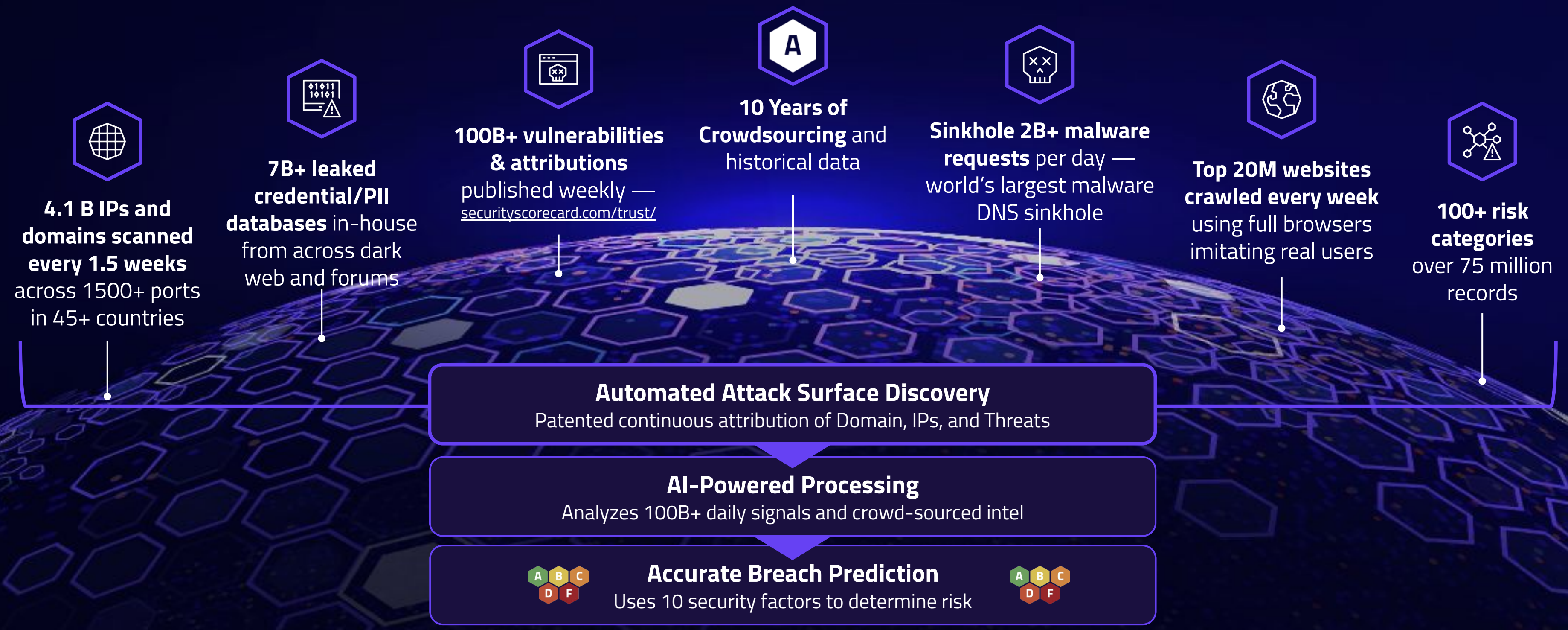
🔺 الحاج ابو الاء الولائي الامين العام لكتائب سيد الشهداء يعلن الجهوزية التامة للدفاع عن فلسطين أرضًا وشعبا ومقدسات



حماس | HAMAS | فلسطين | غزة

🔺البصرة تحتفل بانتصار طوفان الاقصى

# SecurityScorecard | SIGINT Network



**4.1 B IPs and domains scanned every 1.5 weeks** across 1500+ ports in 45+ countries

**7B+ leaked credential/PII databases** in-house from across dark web and forums

**100B+ vulnerabilities & attributions** published weekly — securityscorecard.com/trust/

**10 Years of Crowdsourcing** and historical data

**Sinkhole 2B+ malware requests** per day — world's largest malware DNS sinkhole

**Top 20M websites crawled every week** using full browsers imitating real users

**100+ risk categories** over 75 million records

### Automated Attack Surface Discovery

Patented continuous attribution of Domain, IPs, and Threats

### AI-Powered Processing

Analyzes 100B+ daily signals and crowd-sourced intel

### Accurate Breach Prediction

Uses 10 security factors to determine risk