OPERATION SOFT CELL

Amit Serper, Mor Levi and
Assaf Dahan

$WHOAMI - A BUNCH OF 🇮🇱 THREATS 😉

Amit Serper

@0xAmit

- Head of Security research at Cybereason Nocturnus
- Former actor at a nation state 🇮🇱 acting agency 🙃
- Security research, exploits, & reverse engineering

Assaf Dahan 🇬🇧

Assaf Dahan

- Head of Threat Research at Cybereason
- Ex 8200, Offensive Cyber Ops
- Malware analysis, Reverse engineering, Threat hunting, Threat intel

Mor Levi

Mor Levi

- VP of Global Security Practices at Cybereason
- Security research, IR and Hunting

cybereason

Agenda

1. What is Operation Soft Cell?
2. Attack Breakdown
3. Threat Intel Work
4. Closing Remarks
5. Questions

cybereason

What is Operation Soft Cell?

1. An “access operation” - espionage campaign, meant to generate actionable intelligence about people of interest through cellular network metadata.

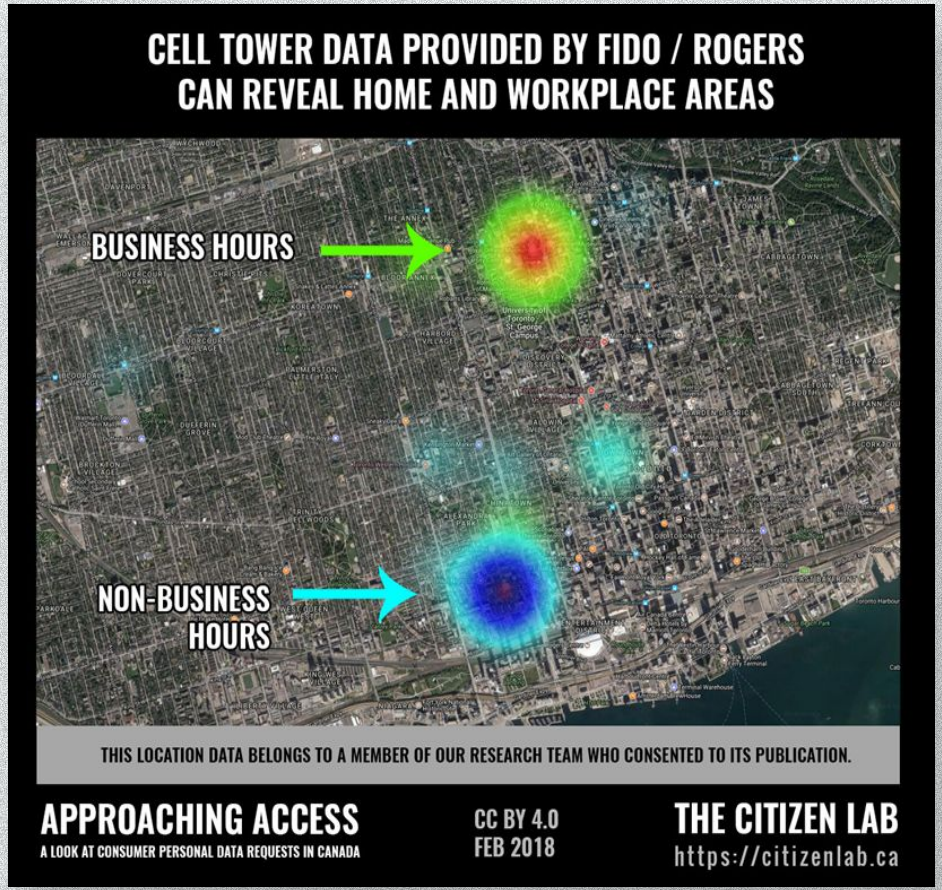
2. Multi-year, multiple-waved attack with TTPs that point to a Chinese nation-state threat group

3. Harnessing the presence of the threat actor in a mobile operator’s network as a platform for operations against other operators

Target of Attack:

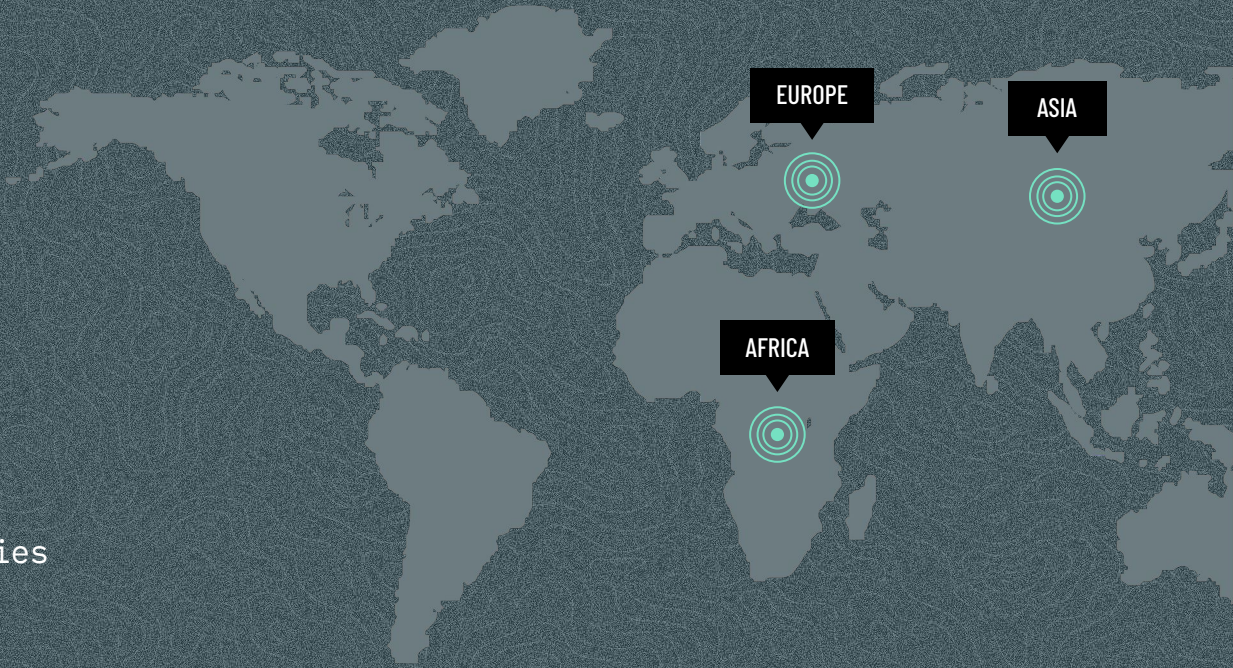
Call Detail Records

- **Date of call**
- Time of call
- Call duration
- **Originating number**
- **Terminating number**
- IMEI
  (International Mobile Equipment Identity)
- **Ci** (Cell Site Identity Number)



Impact

1. Business disruption
2. Operational cost to fix infrastructure
3. Foreign control of critical infrastructure
4. Access for
    a. Persons of interests for intelligence agencies
    b. Espionage
    c. Targeted operations



cybereason

ATTACK BREAKDOWN

Low & Slow

2018-2019

ATTACK TIMELINE

Attackers were in the system at least one year before Cybereason was deployed.

2 MONTHS

1ST WAVE

- WebShell Activity
- Credential Stealing
- Containment Actions

3 MONTHS

2ND WAVE

- A modified version of the original WebShell
- Attempted Credentials Stealing (Blocked)
- Reconnaissance
- Data Exfil
- Containment Actions

1 MONTH

3RD WAVE

- New Webshell
- User Enumeration
- Lateral Movement
- hTran
- Data Exfil
- Containment Actions

4TH WAVE

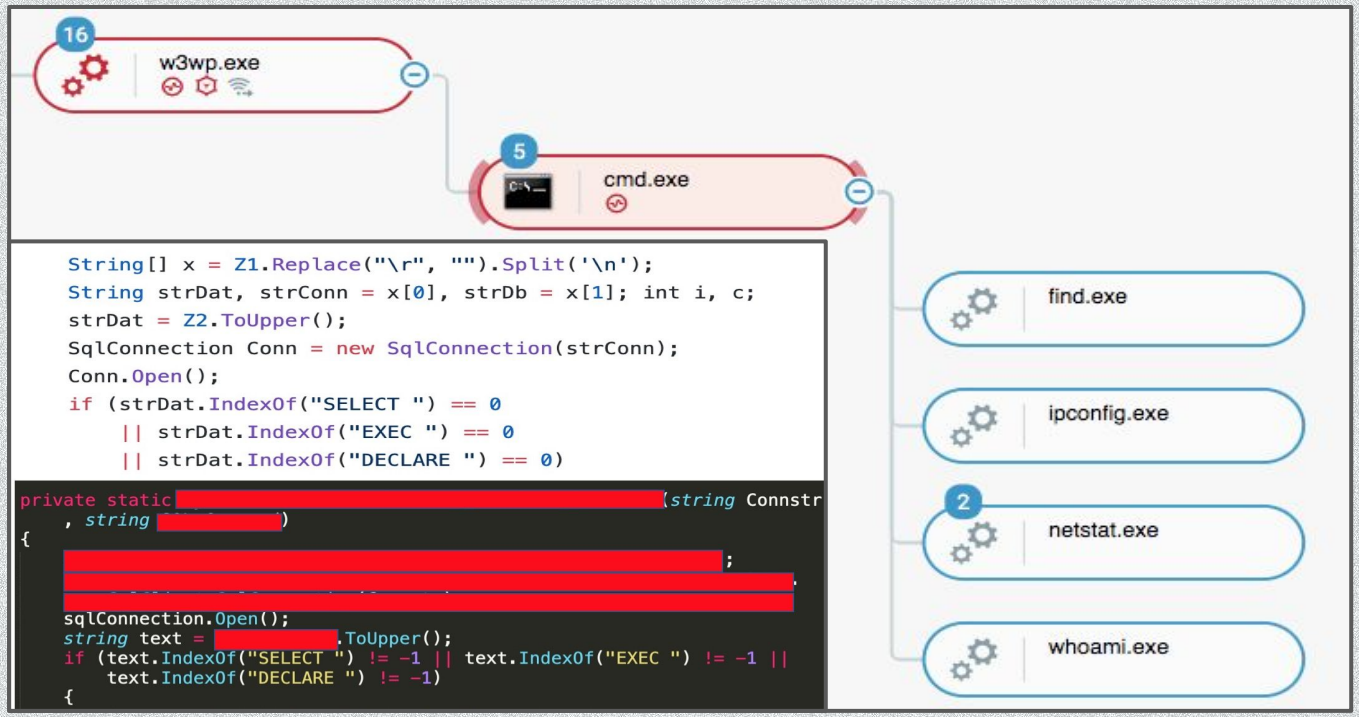
- Same tools, different IOCs
- Attackers create VPN access
- AD Enumerations

cybereason

Initial Exploration & Staging

Github China Chopper Code

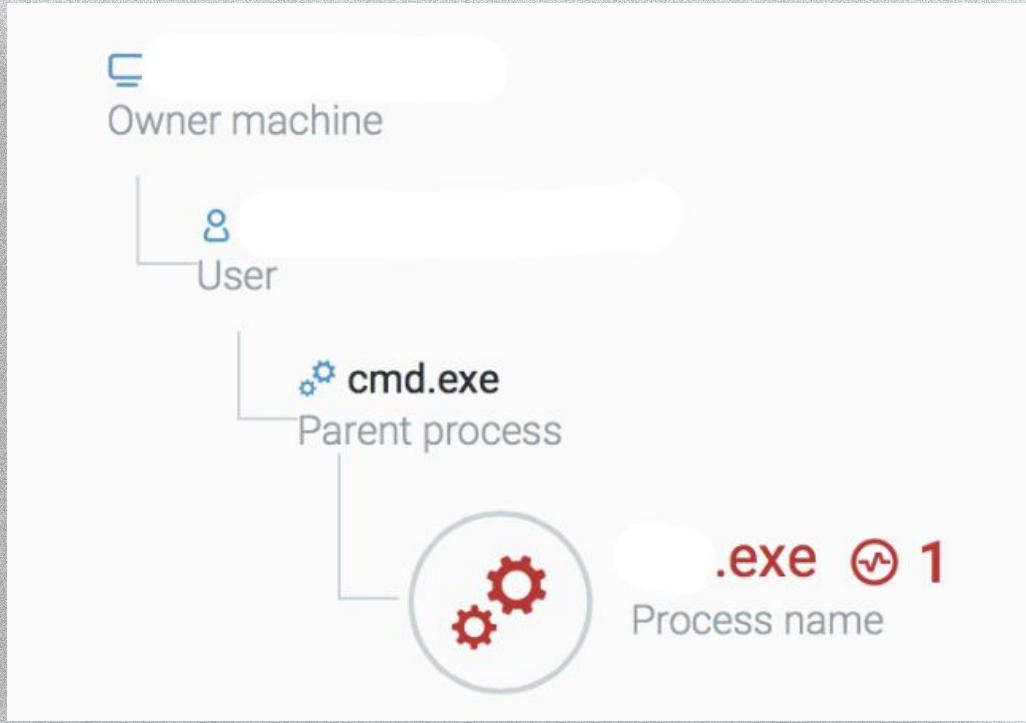
Modified China Chopper Code



cybereason

Modified NBTScan

- Threat Actor Used NBTScan
- Identifies NetBIOS Name Servers & System Information
- Previously Used by Chinese Threat Actors, including APT10, APT1, APT27...

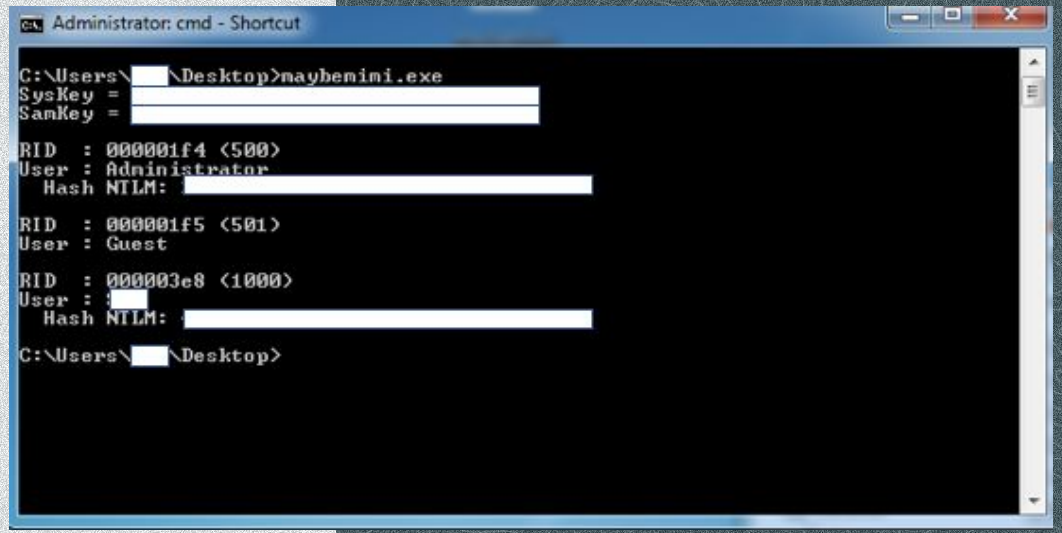


cybereason

cybereason

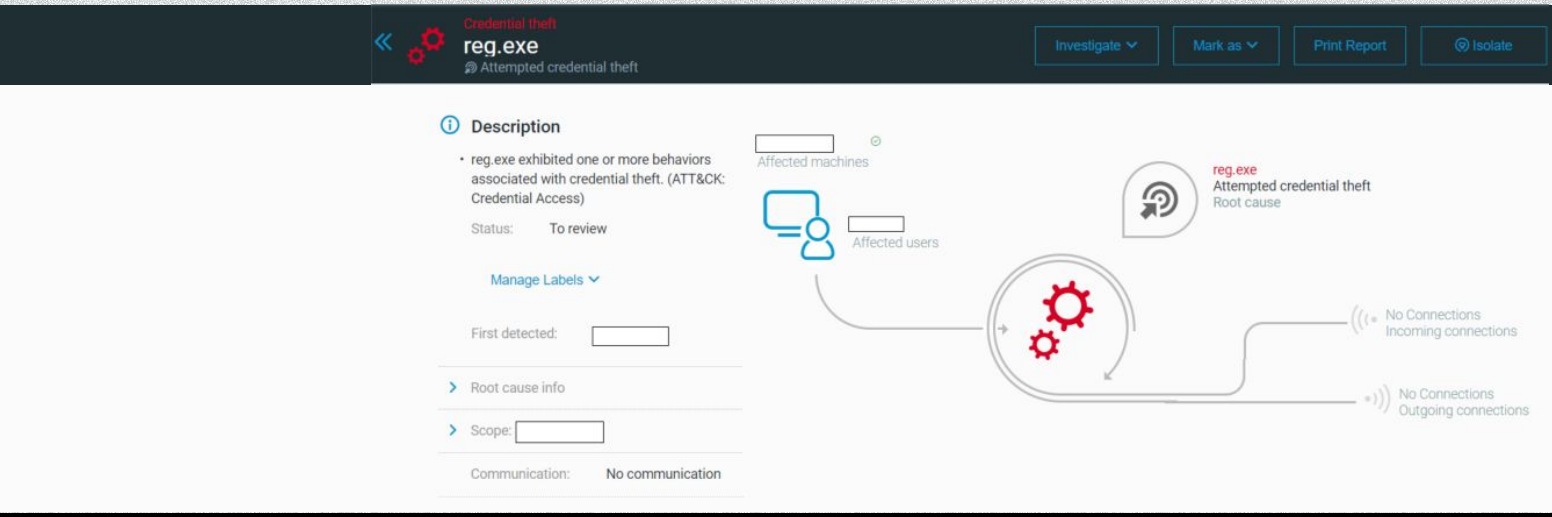
Modified Mimikatz

- Modified by Threat Actor
- No Command-line Arguments to Avoid Detection
- Dumps Credentials
- NTLM Hashes
- Additionally,PowerShell-based Mimikatz Used to Dump Credentials On Compromised Machines



Dumping Sam Hive From The Registry

- Threat Actor Dumped Specific Hives from the Windows Registry
- SAM Hive Contains Password Hashes



Lateral Movement

- Threat Actor Used WMI,PsExec
- Installed Tools Across Multiple Assets
- Compromised Critical Assets
  - Production Servers
  - Database Servers
  - Full Access of Domain Controller

```
/c cd /d "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\auth\"&wmic /node:[REDACTED] /user:"[REDACTED]" /password:"[REDACTED]" process call create a.bat&echo [S]&cd&echo [E]
```

WMI Command to Move Laterally

cybereason

cybereason

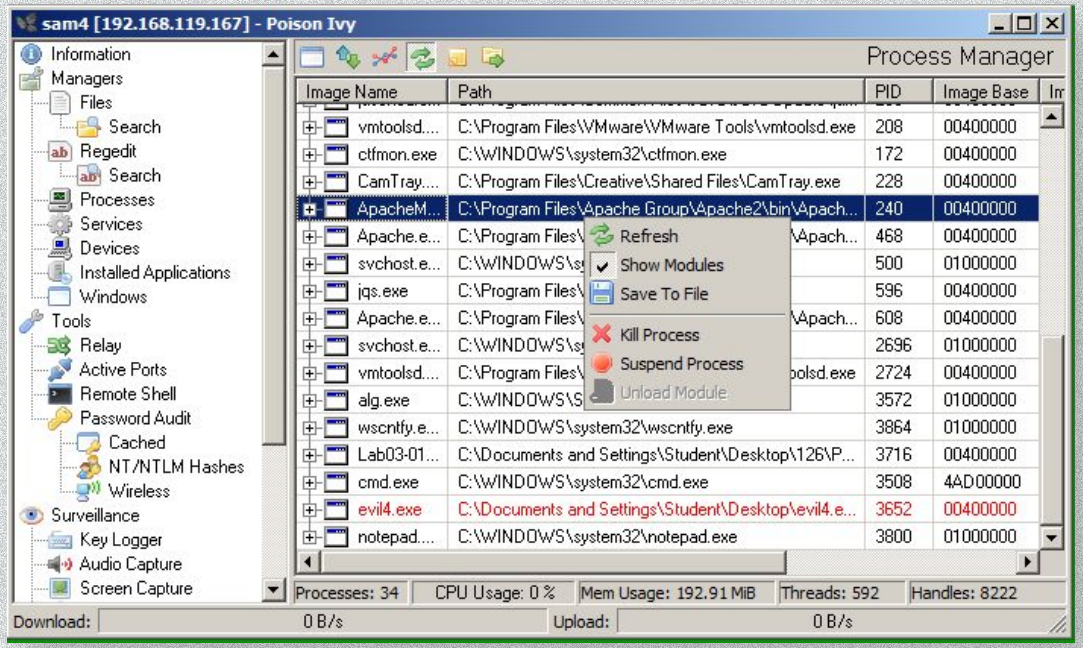
RAR

- Compressed & Password-protected Data
- Moved Data to Recycle Bin & Temp folders
- Stages Data in Multi-part Archives Before Exfiltration
- Understanding the motive - what information was stolen

```
rar.exe a -k -r -s -m1 -[password]
C:\[folder]\[file_name].rar "C:\[folder]\[DATE]_cdr.csv"
```

Long-Term Access - Modified Poison Ivy

1. Well known RAT, attributed to Chinese threat actors
2. Features endless possibilities for spying
3. New version - Proxy aware
4. Bundled with a signed Samsung installer and loads into memory via dll hijacking, known APT10 tactic.

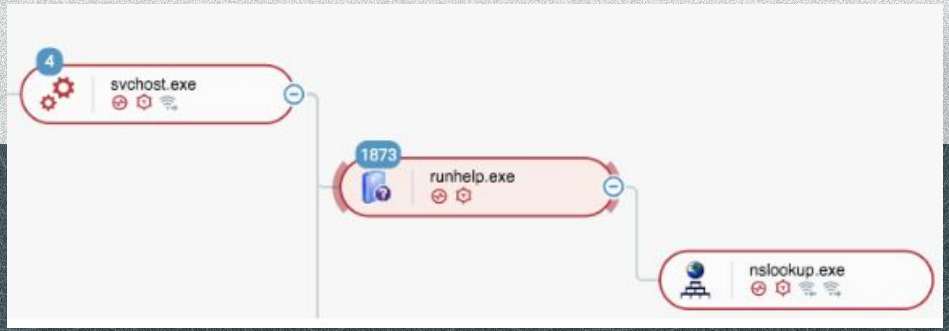


Poison Ivy

1. Application (runhelp.exe) runs the signed samsung application installer (NSIS installer)

2. ssMUIDLL.dll gets hijacked and injects the PoisionIVY stager to the memory of a preconfigured process - nslookup.exe

3. Nslookup now hosts a malicious PoisonIVY thread.



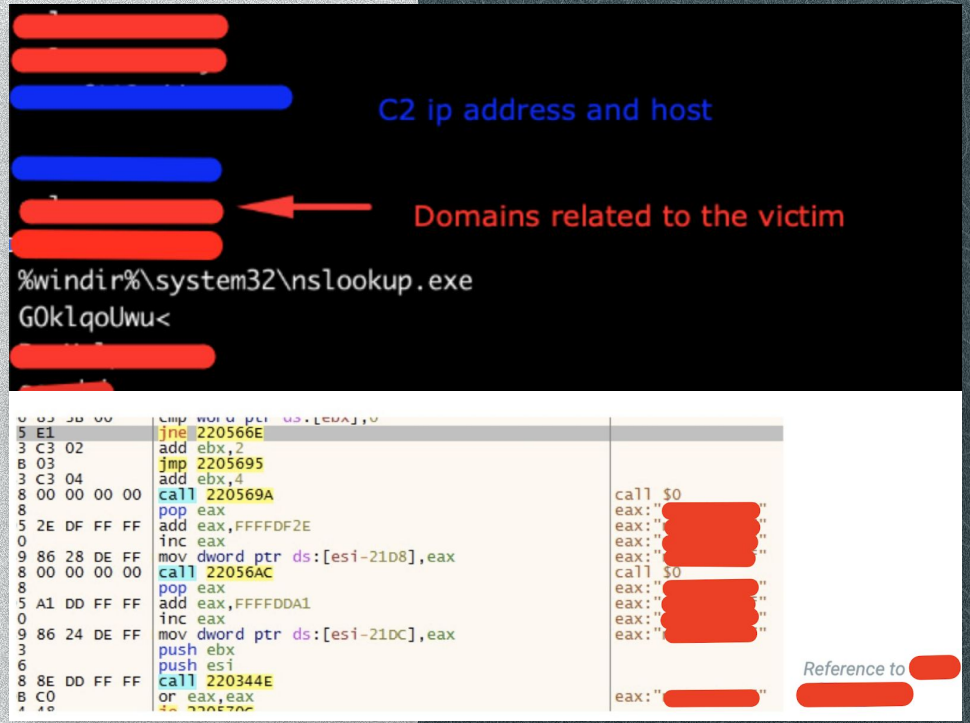
cybereason

Poison Ivy

1. The code gets unpacked and injected (hollowed) to nslookup.exe contains the configuration of the RAT itself

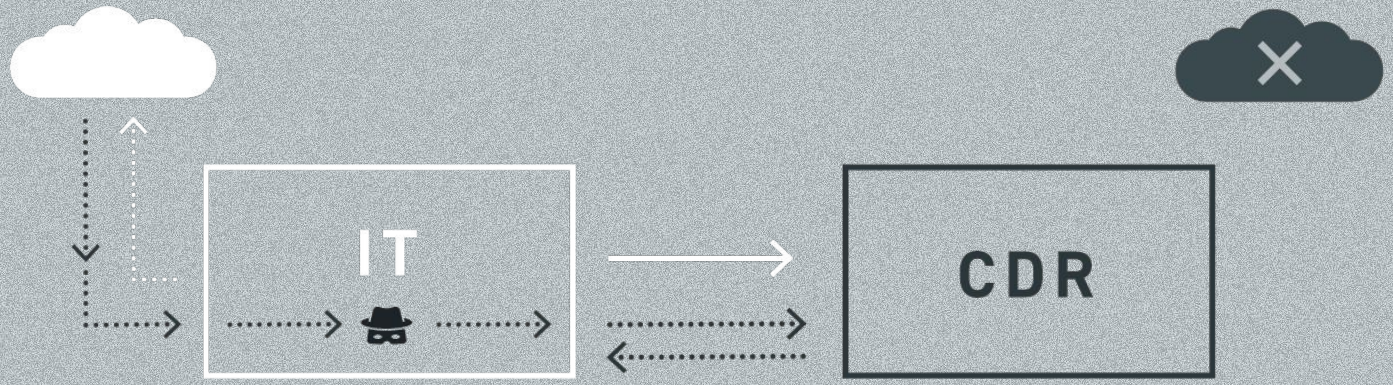
2. One of the values in the configuration contained the name of the victim and a few of their IP addresses

3. These details would come in handy in the future :)



hTran (HUC Packet Transmit Tool)

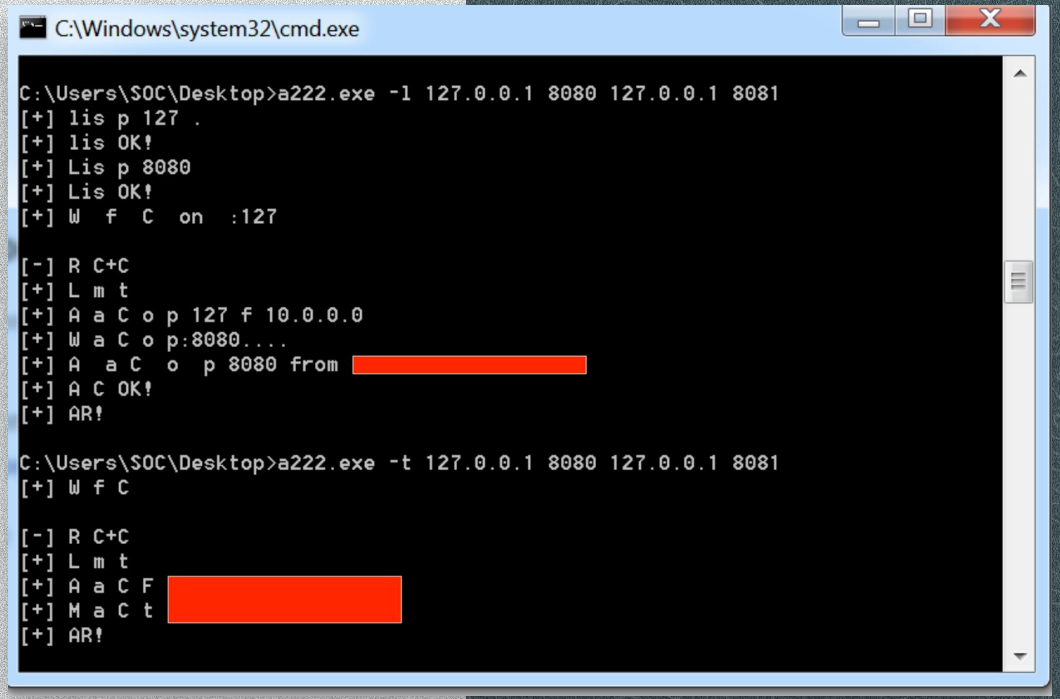
1. hTran is a client/server architecture based connection bouncer program written by Chinese hackers.
2. hTran is used by threat actors to mask their location by tunneling their traffic.
3. It can also be used to create a tunnel between two different networks



cybereason

hTran (HUC Packet Transmit Tool)

1. hTran is a client/server architecture based connection bouncer program written by Chinese hackers.
2. hTran is used by threat actors to mask their location by tunneling their traffic.
3. It can also be used to create a tunnel between two different networks

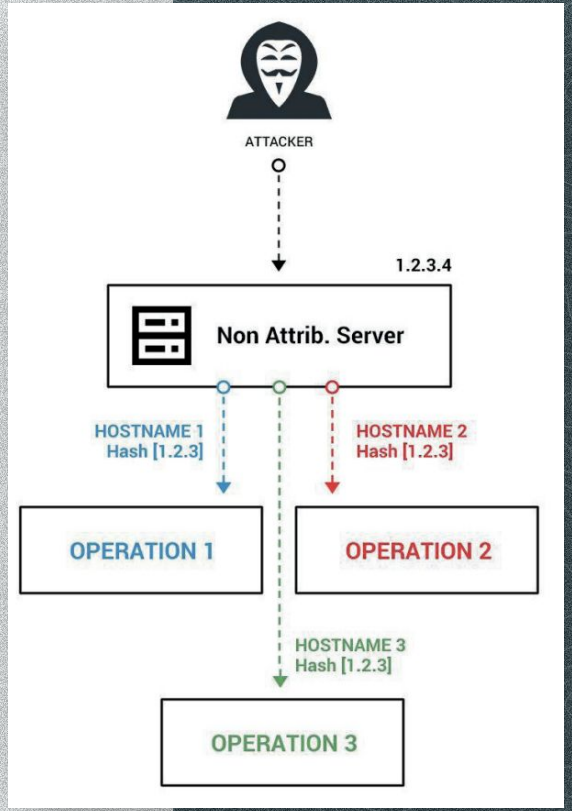


THREAT INTEL

Connecting the dots to a global campaign

From one Telco to Global Attack

- Threat intel research of the domains and IP -> other hostnames -> tied to the same IP address.
- The C2 infrastructure is Chinese affiliated territories \ countries
- Hostnames -> more related samples, which were identical to the original samples we found
- The samples contained information about other Telcos that were attacked by the same actor.
- Multiple samples targeting more than 10 different companies worldwide.
- Every company that we found was targeted received a full briefing from us and a dossier with the report and the relevant IoCs
- The evidence that we found proves that this operation was not new and was dating as far back as **2012.**



cybereason

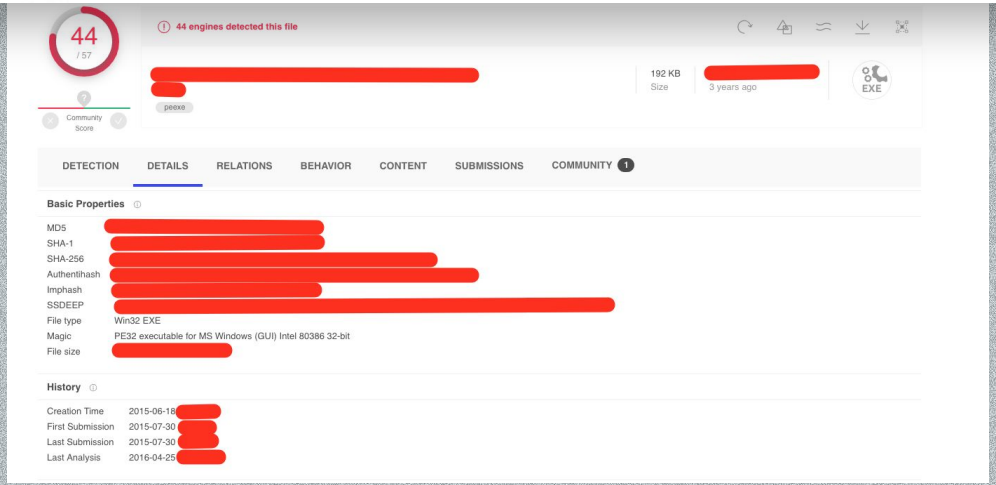
Infrastructure Overview

1. Command and control infrastructure was based in China or Chinese affiliated territories/countries:
    - China
    - Hong Kong
    - Taiwan

2. Multiple companies in different regions were targeted by the same infrastructure and malware.

Samples Data

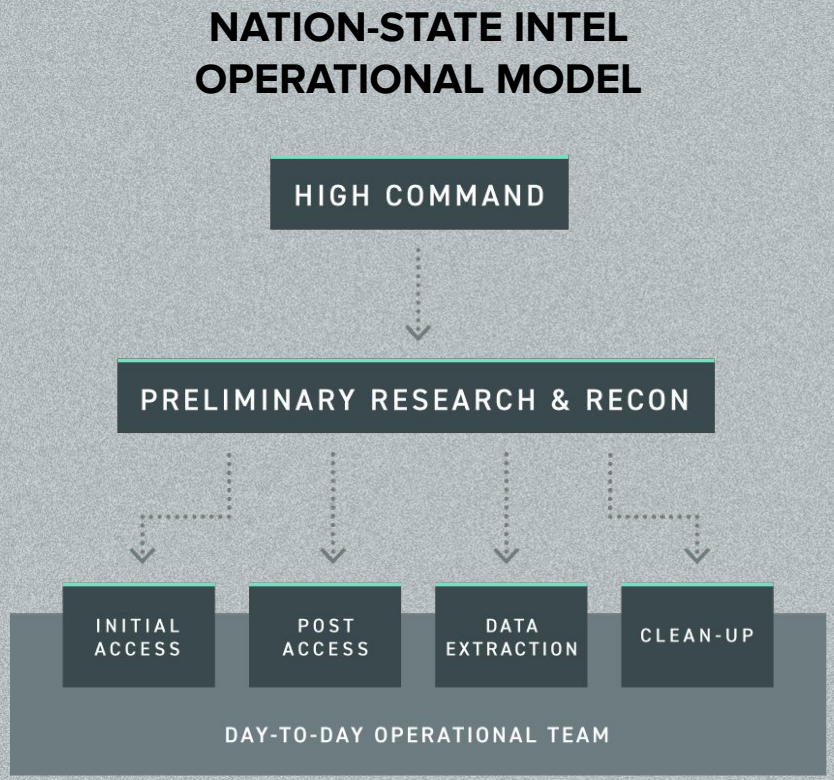
- 2019 — 3 Samples
- 2018 — 4 Samples
- 2017 — 3 Samples
- 2015 — 2 Samples
- 2012 — 1 Sample



cybereason

Single Team / Joint Effort?

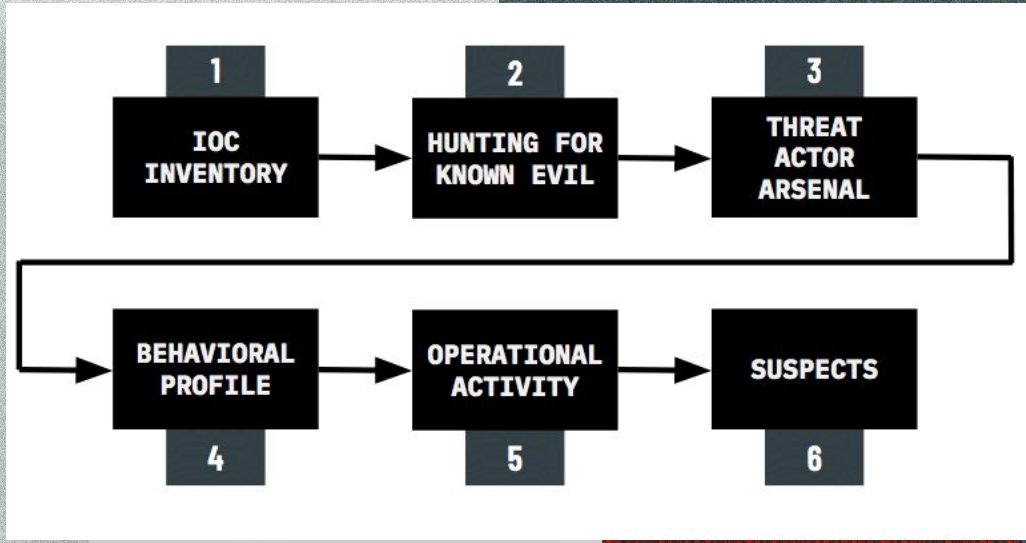
- Getting in is “easy” - what’s next?
- Reconnaissance and mapping of the network and relevant assets
- Maintaining foothold and day-to-day operations
- Getting the relevant data poses challenges:
  - Specific technical knowledge required (deep understanding of compromised systems & technology)
  - How to exfiltrate without getting caught?

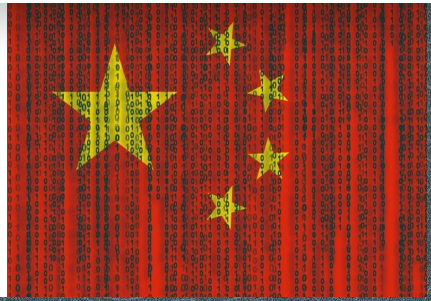


cybereason

Attribution

- The attribution model is based on a multi-facet model, that takes into consideration multiple aspects of the attack.
  - Tools and techniques
  - Infrastructure
  - Activity patterns (e.g GMT +8)
  - Motivation
- Possibility of “Copy Cat” operation, masquerading as another threat actor. Important to remember:
  - Publicly available tools that can be used by anyone
  - Psychological warfare
- In our reports we have mentioned possible Chinese state sponsored groups such as APT10, DragonOK and APT27.





China hacked Asian telcos to spy on Uighur travelers: sources

Jack Stubbs

REUTERS

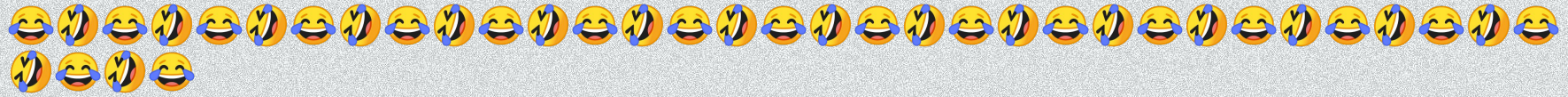
LONDON (Reuters) - Hackers working for the Chinese government have broken into telecoms networks to track Uighur travelers in Central and Southeast Asia, two intelligence officials and two security consultants who investigated the attacks told Reuters.

China actually responded! 🗣️🇨🇳

Alfred NG, CNET

A Chinese foreign ministry spokesperson said that China "firmly opposes" cyberattacks using the nation's infrastructure, and denied involvement with the hacks.

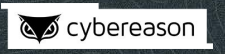
"Second, with the cyberspace being a highly virtual one filled with multiple actors whose behaviors are difficult to trace, one should present abundant evidence when investigating and determining the nature of a cyberspace activity," the Chinese embassy said in an email. "Making groundless accusations are neither professional nor responsible."



cybereason

Closing Remarks

QUESTIONS?



THANK YOU