The SolarWinds Supply Chain Compromise

Erik Hjelmvik (Netresec, Sweden)

@netresec

Erik Hjelmvik

@netresec

- Founder of Netresec AB
- Developer
- Former Incident Responder
- Former ICS / SCADA geek
- Crazy about PCAPs

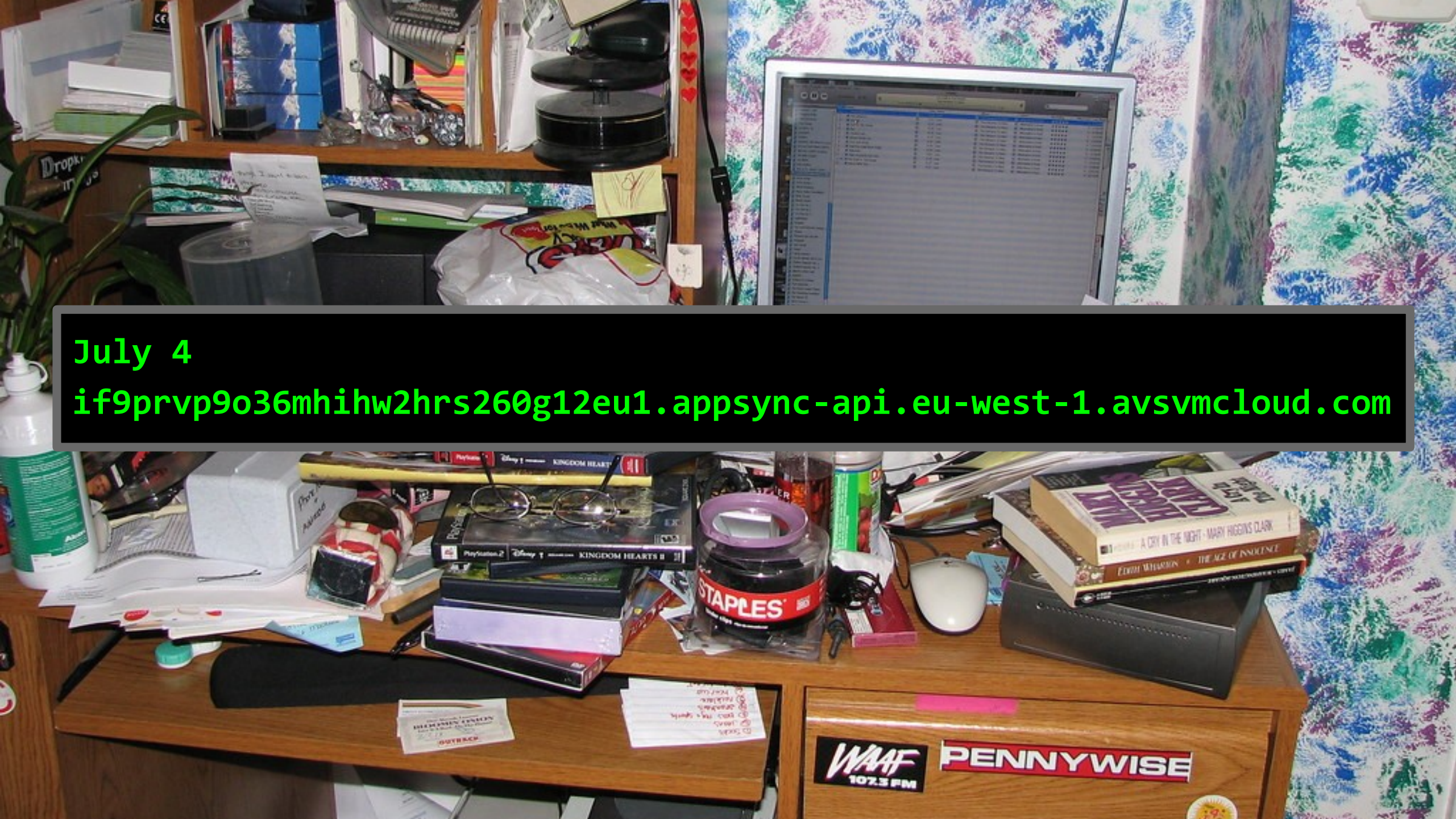
NetworkMiner

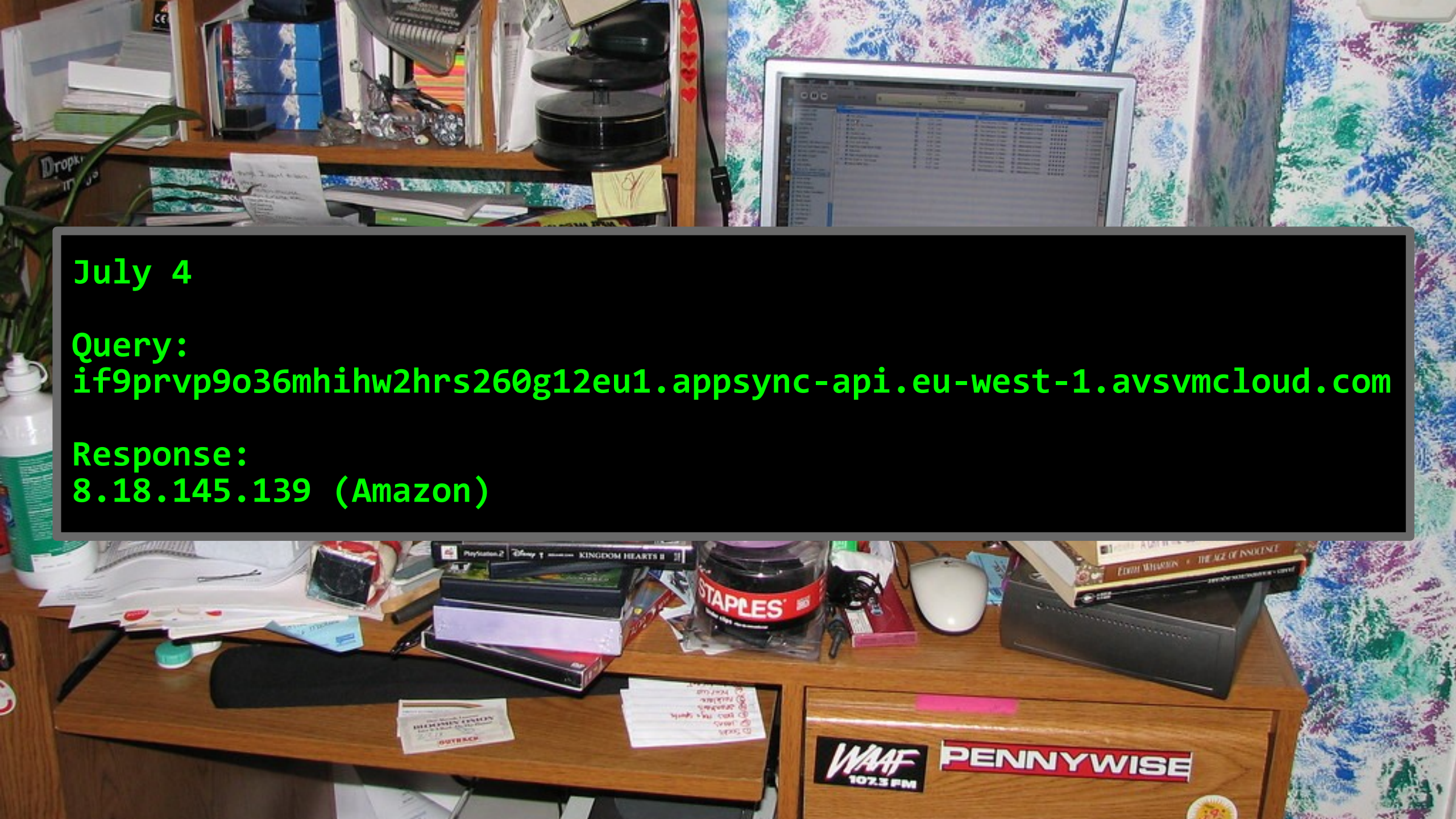
CapLoader

PolarProxy

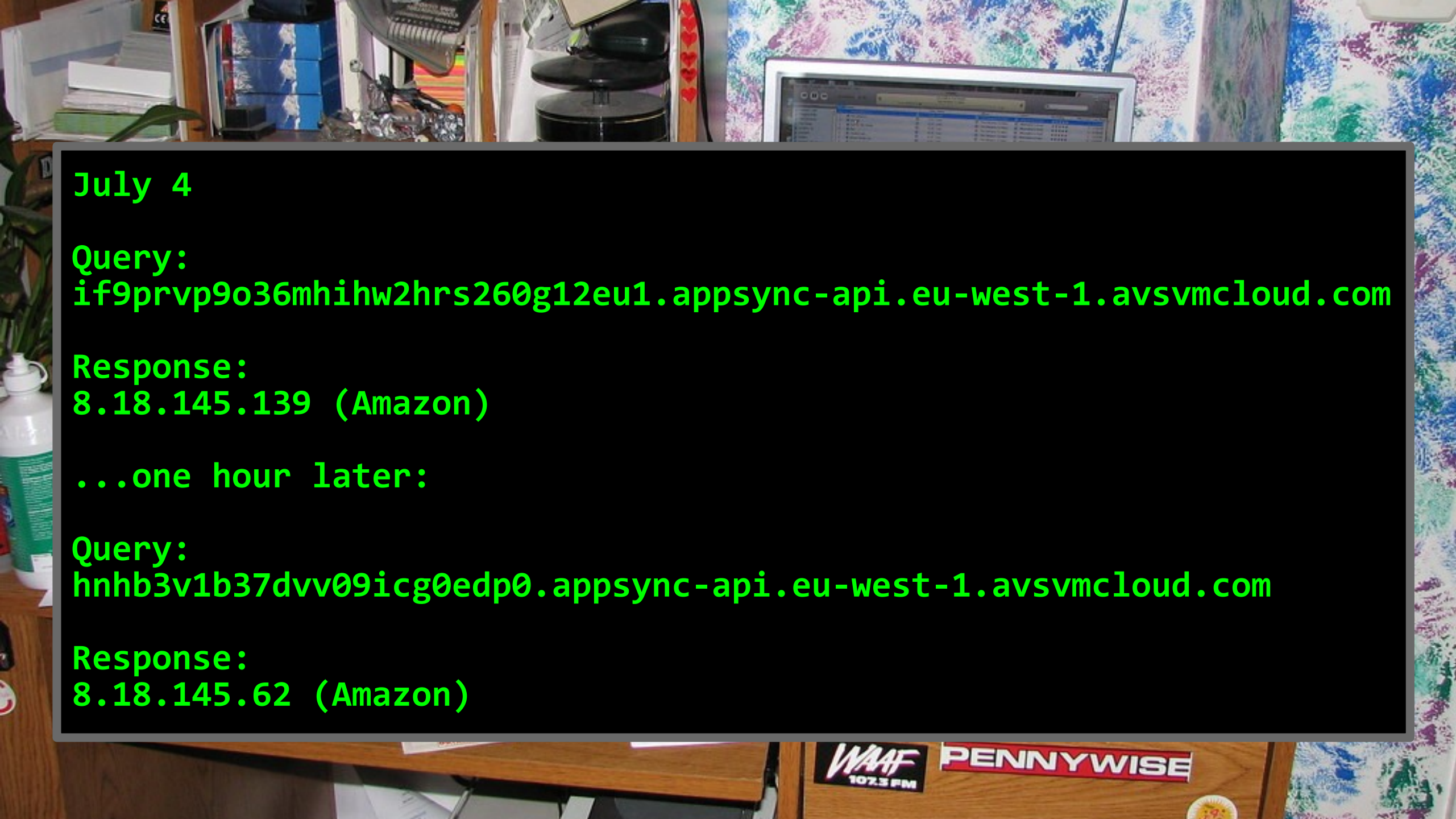
BACK AT THE OFFICE…


BACK AT THE OFFICE...
KINGDOM HEARTS II
STAPLES
WAAF
107.3 FM
PENNYWISE


July 4
if9prvp9o36mhihw2hrs260g12eu1.appsync-api.eu-west-1.avsvmcloud.com
KINGDOM HEARTS II
STAPLES
WAAF
107.3 FM
PENNYWISE


July 4
Query:
if9prvp9o36mhihw2hrs260g12eu1.appsync-api.eu-west-1.avsvmcloud.com
Response:
8.18.145.139 (Amazon)
KINGDOM HEARTS II
STAPLES
WAAF
107.3 FM
PENNYWISE


if9prvp9o36mhihw2hrs260g12eu1
.appsync-api.eu-west-1
.avsvmcloud.com
3nevdwj3yrgc5h2feeynqo627y
.appsync-api.eu-west-1
.amazonaws.com


July 4
Query:
if9prvp9o36mhihw2hrs260g12eu1.appsync-api.eu-west-1.avsvmcloud.com
Response:
8.18.145.139 (Amazon)
...one hour later:
Query:
hnhb3v1b37dvv09icg0edp0.appsync-api.eu-west-1.avsvmcloud.com
Response:
8.18.145.62 (Amazon)
WAAF
107.3 FM
PENNYWISE

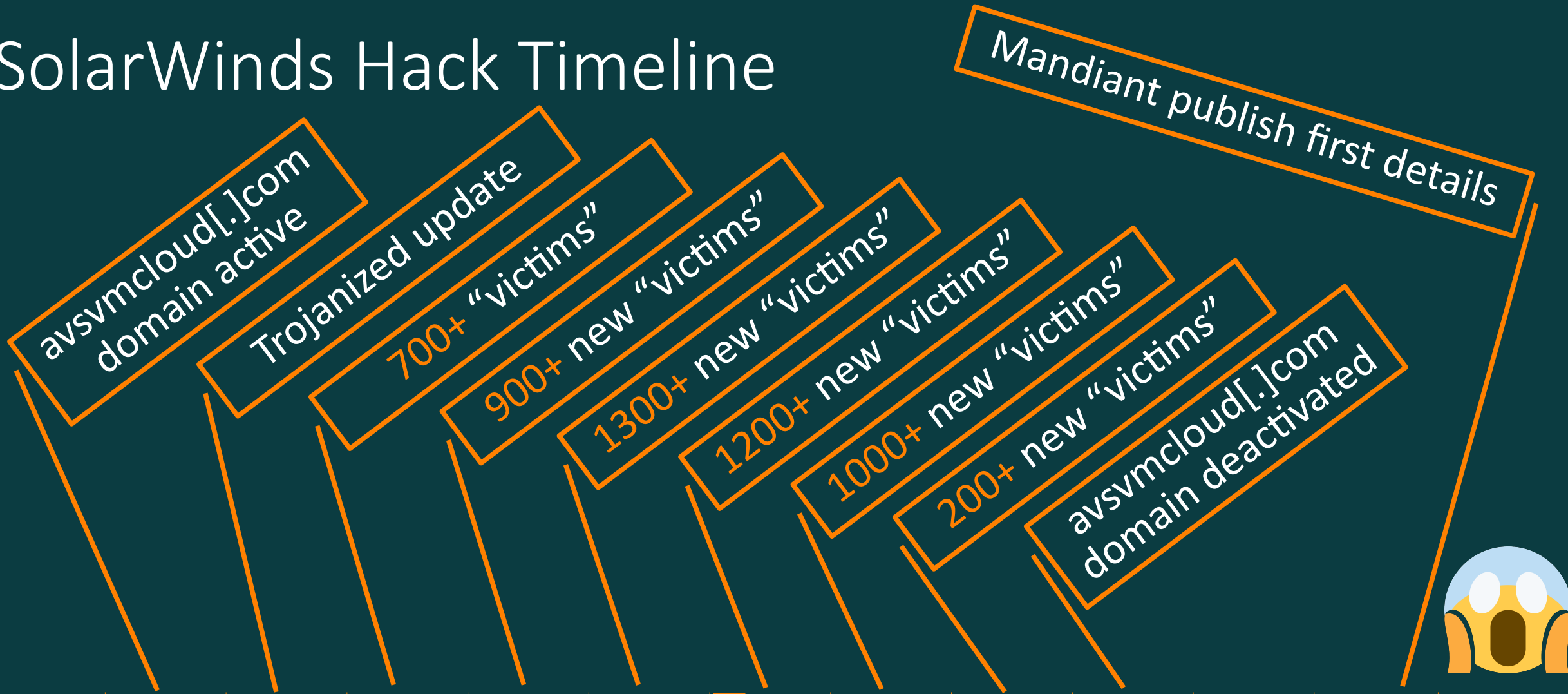
July 4
Q: if9prvp9o36mhihw2hrs260g12eu1.appsync-api.eu-west-1.avsvmcloud.com
R: 8.18.145.139 (Amazon)
Q: hnhb3v1b37dvv09icg0edp0.appsync-api.eu-west-1.avsvmcloud.com
R: 8.18.145.62 (Amazon)

July 5
Q: ea99hr2sfen95nkjlc5g.appsync-api.eu-west-1.avsvmcloud.com
R: 8.18.144.150 (Amazon)

July 6
Q: 707gigk9vbc923hf27fe.appsync-api.eu-west-1.avsvmcloud.com
R: 8.18.145.151 (Amazon)

July 7
Q: 6eivqct649pcg0g16ol4.appsync-api.eu-west-1.avsvmcloud.com
R: 20.140.84.127 (Microsoft)

SolarWinds Hack Timeline




Had Mandiant not been targeted,
would we even know about
the SolarWinds backdoor?

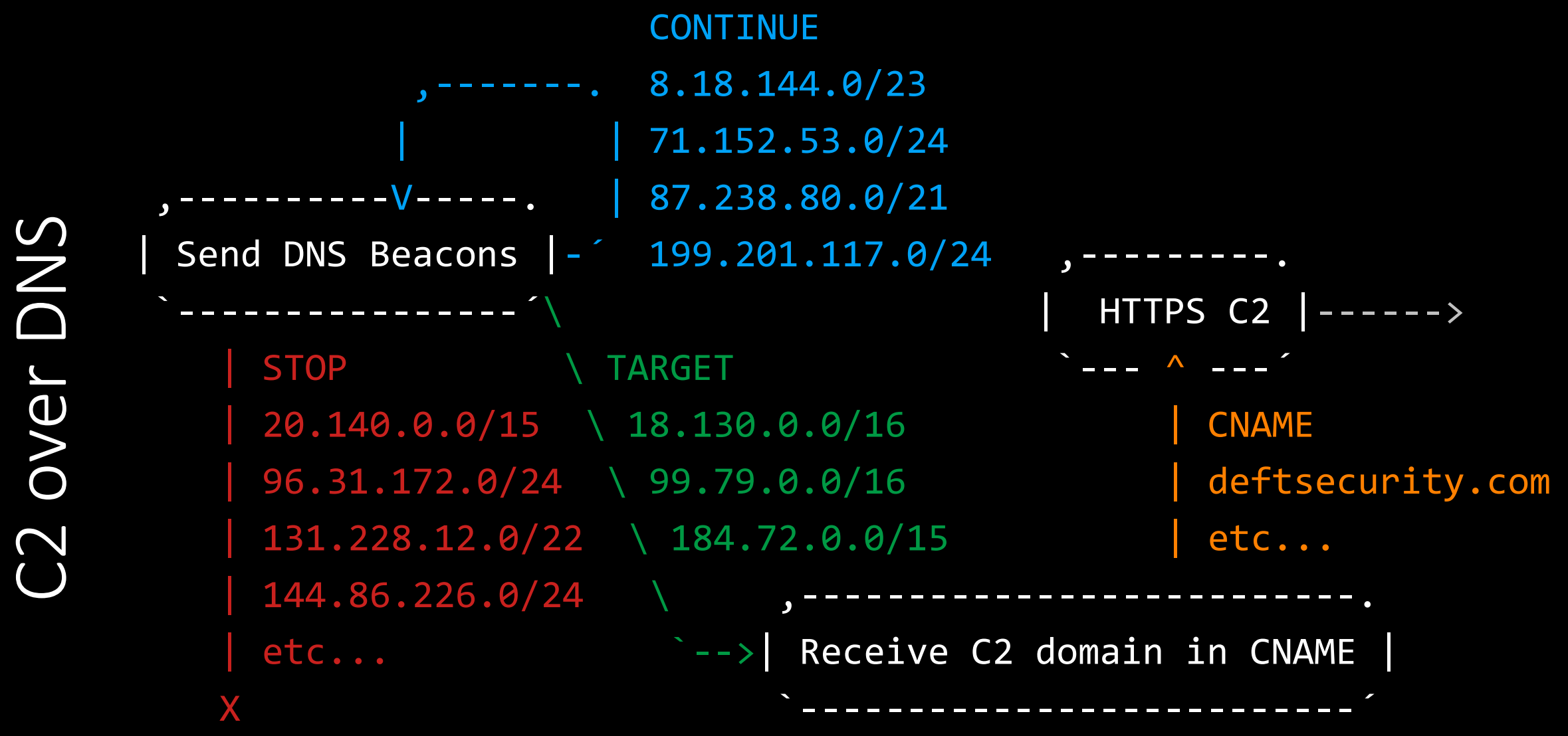
AD Name Transmitted over DNS

if9prvp9o36mhihw2hrs260g12eu1.appsync-api.eu-west-1.avsvmcloud.com

- **if9prvp9o36mhih** = XOR key 0xa4, Victim ID E0E48F2C425CBFEC
- **w** = Segment number 0 (first part)
- **2hrs26** = "o[redacted]"
- **0g12eu1** = ".local"

SunburstDomainDecoder

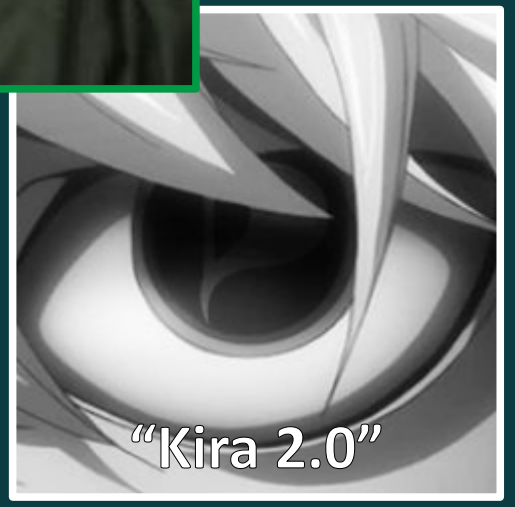
https://netresec.com/?b=20C0f71


C2 over DNS
CONTINUE
8.18.144.0/23
71.152.53.0/24
87.238.80.0/21
199.201.117.0/24
Send DNS Beacons
HTTPS C2
STOP
20.140.0.0/15
96.31.172.0/24
131.228.12.0/22
144.86.226.0/24
etc...
TARGET
18.130.0.0/16
99.79.0.0/16
184.72.0.0/15
CNAME
deftsecurity.com
etc...
Receive C2 domain in CNAME

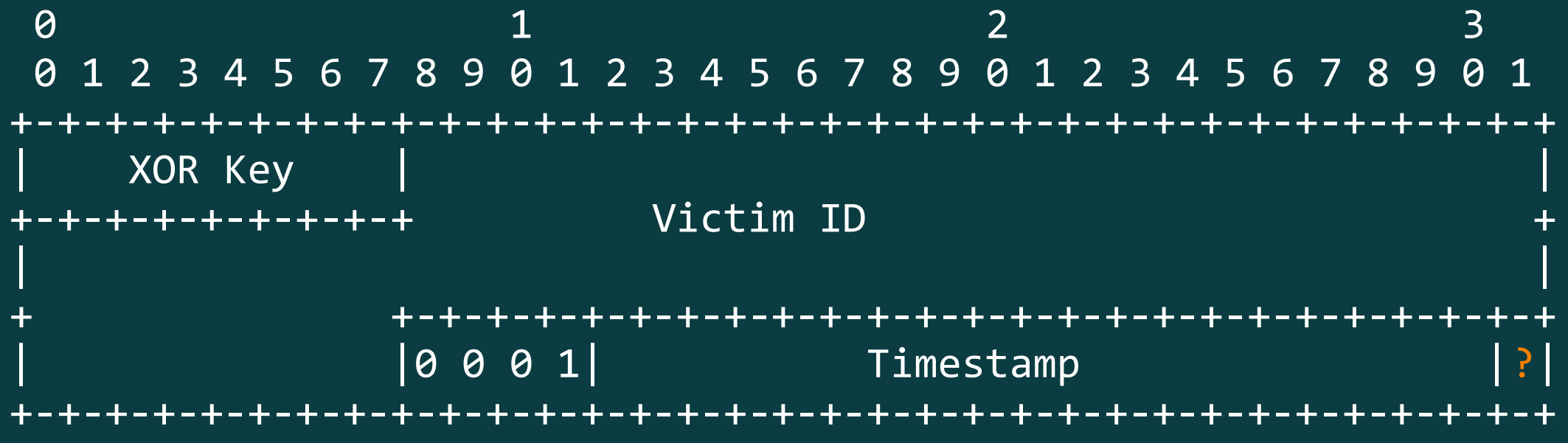
Victim Profiling over DNS

Query/Response	Decoded
if9prvp9o36mhihw2hrs260g12eu1 .appsync-api.eu-west-1.avsvmcloud[.]com	AD domain "o[redacted].local"
8.18.145.139	Sleep 1 hour, then Continue
hnhb3v1b37dvv09icg0edp0	EV/EDR: Carbon Black, 2020-07-04 01:00 UTC
8.18.145.62	Sleep 1 day, then Continue
ea99hr2sfen95nkjlc5g	PING, 2020-07-05 01:00 UTC
8.18.144.150	Sleep 1 day, then Continue
707gigk9vbc923hf27fe	PING, 2020-07-06 02:30 UTC
8.18.145.151	Sleep 1 day, then Continue
6eivqct649pcg0g16ol4	PING, 2020-07-07 03:30 UTC
20.140.84.127	Stop DNS beacon

Thanks to Everyone who Contributed with pDNS!



SUNBURST PING over DNS



- 8+ US Tech/Telco Companies
- 7+ US Government Agencies
- 1+ EU Agency

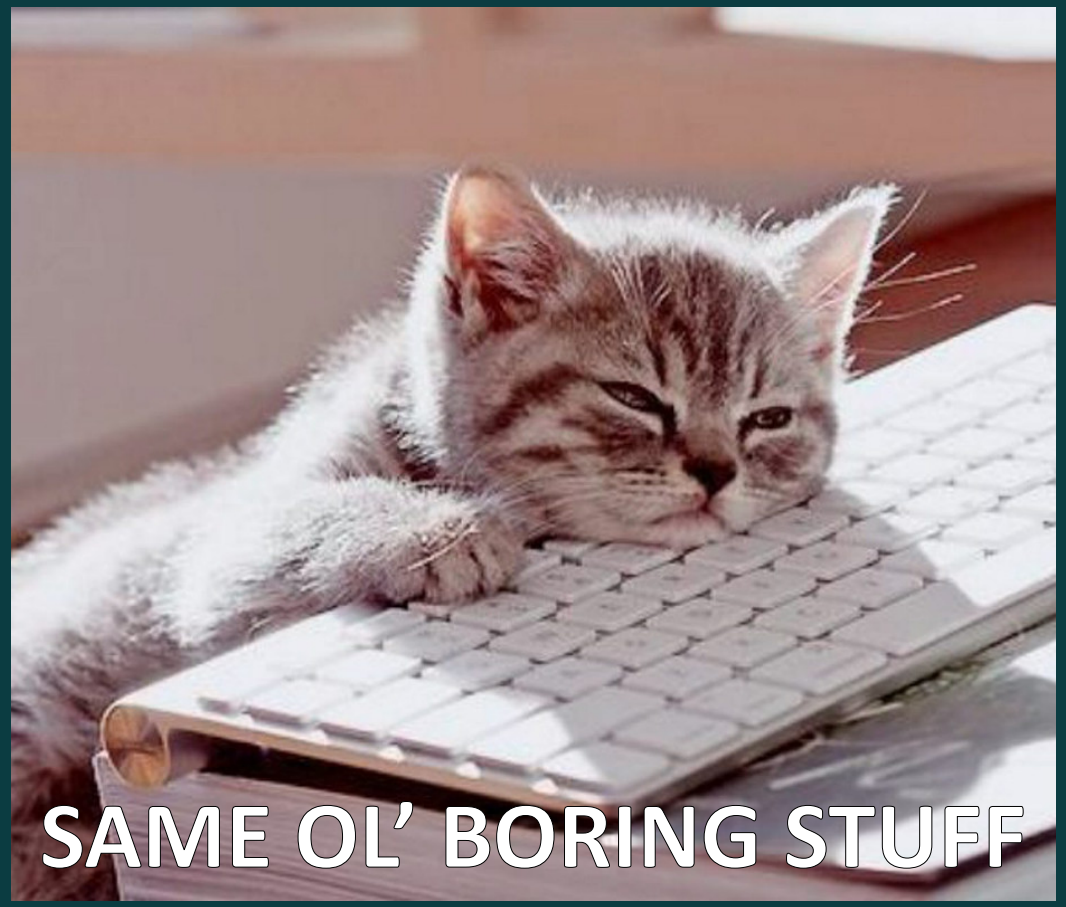
Timestamp in C2 Protocol

```
private static int GetStringHash(bool flag) {
    return ((int)((DateTime.UtcNow - new DateTime(2010, 1,
    1, 0, 0, 0, DateTimeKind.Utc)).TotalMinutes / 30.0)
    & 0x7ffff) << 1 | (flag ? 1 : 0);
}
```

Time resolution: 30 minutes
Min timestamp: January 1, 2010
Max timestamp: December 4, 2039

Protecting Against Supply Chain Attacks

- **Invest** in Security Operations (CERT/CSIRT/SOC)
- **Remove** unnecessary systems
- **Minimize** privileges
- **Enable** MFA
- **Segment** networks
- **Filter** egress traffic
- **Monitor** your environment




VENDOR ADVICE:
DON’T GET HACKED!!!


VENDOR ADVICE #2:
IN-N-OUT
EAT YOUR OWN DOG FOOD

VENDOR ADVICE #3:

STOP, COLLABORATE AND LISTEN

Protecting Vendors Against Supply Chain Attacks

1. **DON'T GET HACKED!!!**
- Same ol' boring stuff...

2. **Build Secure Products**
- Have a PSIRT
- SDLC/SDL/Security Engineering
- Test, Test, Verify and Test again
- Eat your own dog food

3. **Build Defensible Products**
- Listen to customer requests
- Declare required Internet resources
- Run with minimal privileges
- Enable integration with SIEM or EDR

Summary

- SolarWinds Orion backdoor used DNS based C2 protocol
- DNS traffic designed to blend in with normal traffic
- Threat actor hand-picked targets from a huge pool of “victims”
- Victims and targeted victims could be identified with pDNS
- Vendors: Don’t get hacked — eat your own dog food — stop, collaborate and listen to your customers!

https://netresec.com/?r=SolarWinds

6+ Blog posts on the SolarWinds hack