cisco The bridge to possible

6 Years of Supply Chain Attacks

Martin LEE, EMEA Lead, Cisco Talos
@mlee_security

cisco Live!

BRKSEC-2727

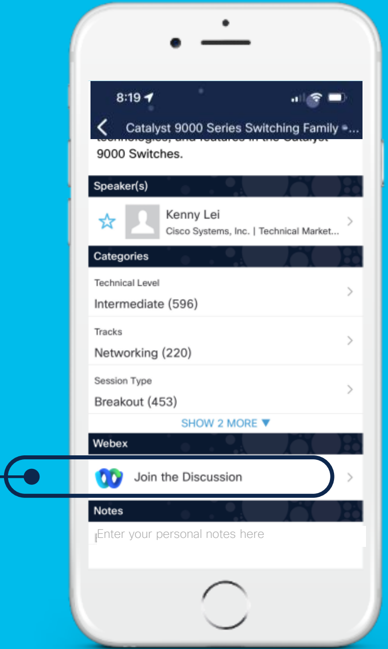
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Webex spaces will be moderated
until February 24, 2023.

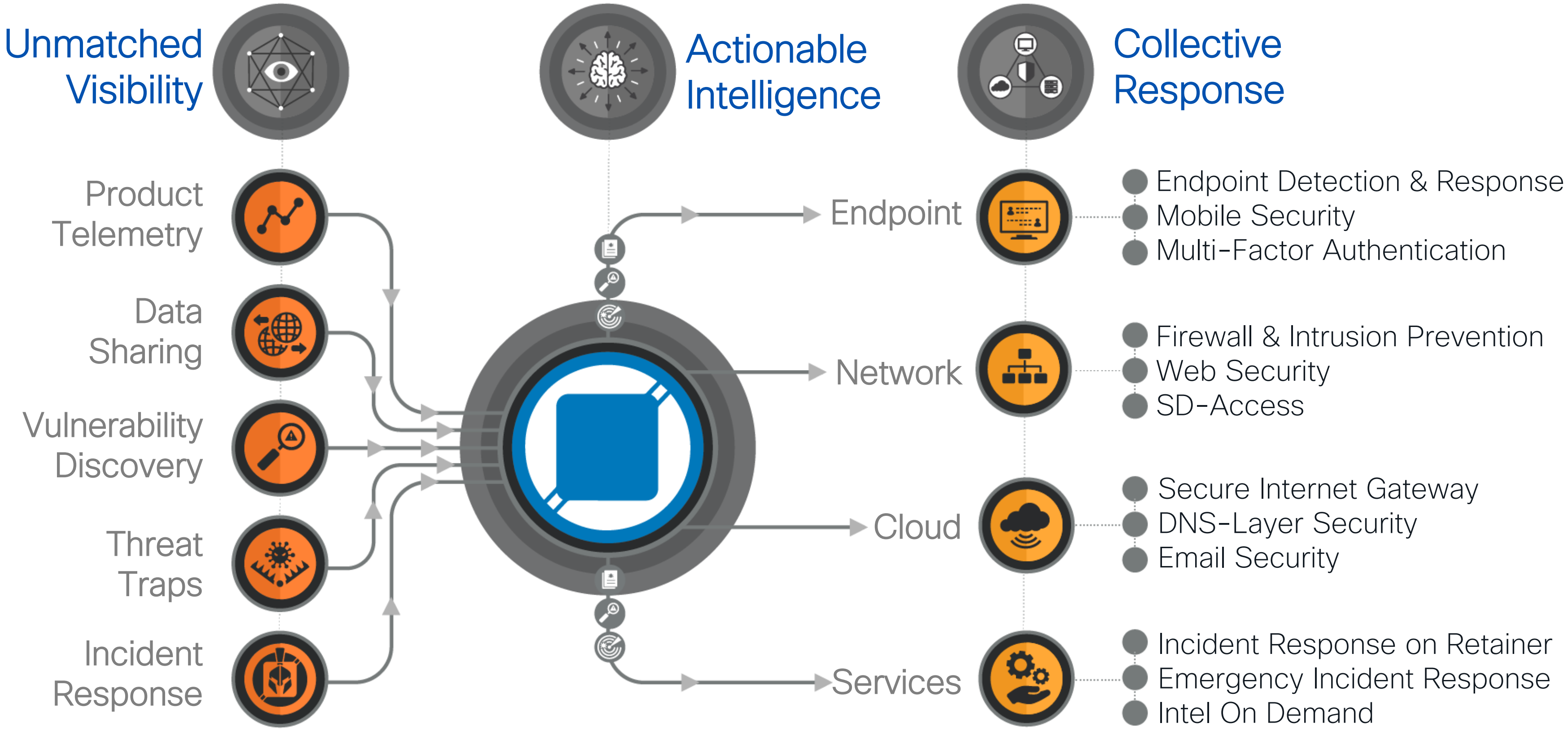
Who am I?

- Recycled human viral geneticist
- 27 years IT experience
- 20 years cyber security
- Chartered Engineer & CISSP

- Keen (if not very good) runner

How do you know if someone has run a marathon?

Cisco Talos – From Unknown to Understood



Unmatched Visibility

- Product Telemetry
- Data Sharing
- Vulnerability Discovery
- Threat Traps
- Incident Response

Actionable Intelligence

Collective Response

- Endpoint
  - Endpoint Detection & Response
  - Mobile Security
  - Multi-Factor Authentication
- Network
  - Firewall & Intrusion Prevention
  - Web Security
  - SD-Access
- Cloud
  - Secure Internet Gateway
  - DNS-Layer Security
  - Email Security
- Services
  - Incident Response on Retainer
  - Emergency Incident Response
  - Intel On Demand

What is a **Supply Chain Attack?**

“Intentional introduction of malicious functionality via a trusted third-party.”

May be via hardware or software.

(I’m only going to speak about software)

Why Supply Chain Attacks?

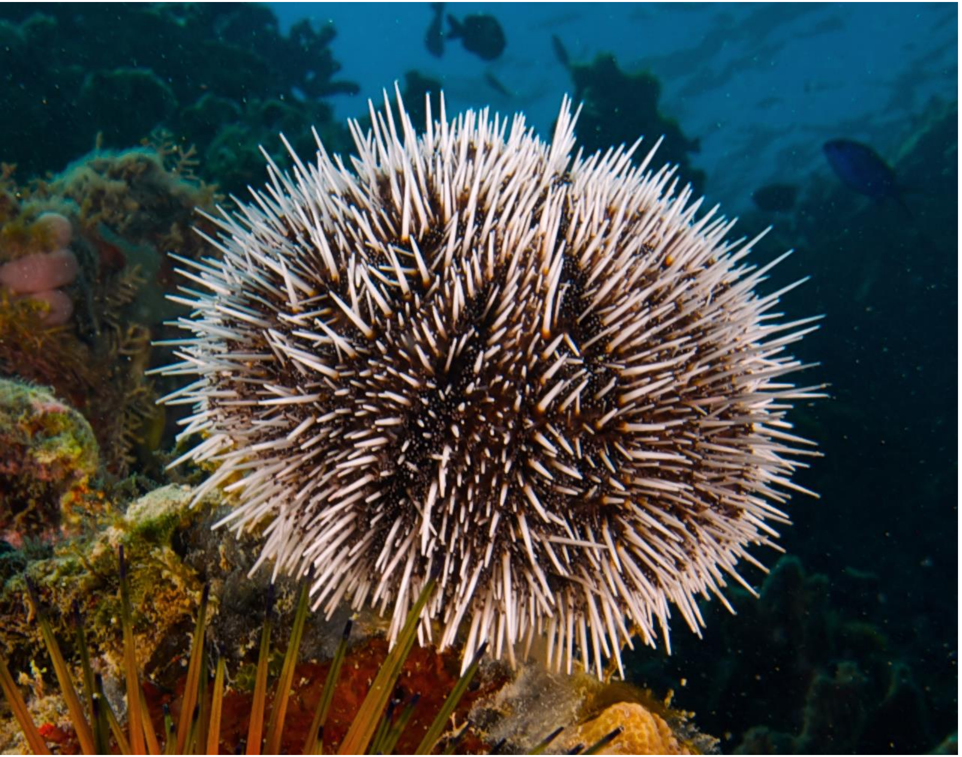


Image source: Nick Hobgood CC3.0 Wikipedia

Your organisation to an attacker.

- Traffic inspection.
- Email filtering.
- Fully patched.
- Two factor authentication.

Almost, but not quite.

☑ Intentional act

☑ Malicious functionality

✗ Supply chain

✗ Trusted third party

Wooden Horse of Troy

Almost, but not quite.

- ☑ Intentional act
- ✗ Malicious functionality
- ☑ Supply chain
- ✗ Trusted third party

Napoleon’s retreat from Moscow

cisco Live!

Early Software Supply Chain Attacks

Linux Kernel Modification 2003

Attempted Supply Chain Attack

Unauthorised code modification:

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
```

rapidly detected:

lack of approval audit trail

discrepancy between BitKeeper and CVS code repositories

RSA Hack 2011

Successful Supply Chain Attack

Seeds for 2-FA PIN numbers stolen.

Subsequently used to compromise defence contractors.

No new malicious functionality.

Exploitation of a systemic vulnerability?

Shamoon 2012

Supply Chain Attack (kind of)

Malicious wiper malware distributed via domain controller compromise.

30 000 computers wiped at major oil company.

Abuse of trust in updates pushed from internal domain controller.

2017

Malicious Insider or Compromise PyPi Repository

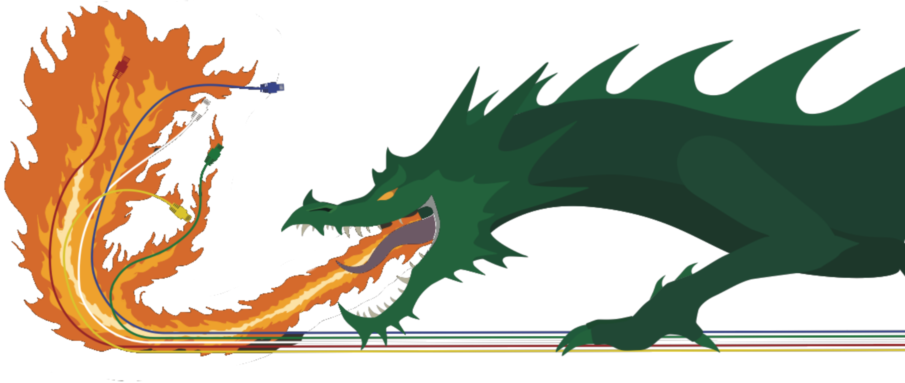
Anna Chapman
(malicious insider)

Long infiltration process.
Escalate privileges.
Risk of discovery.

pip install urllib-1.21.1.tar.gz
vs.
pip install urllib3-1.21.1.tar.gz

Rapid infiltration process.
Immediate privileges.
Discovery?

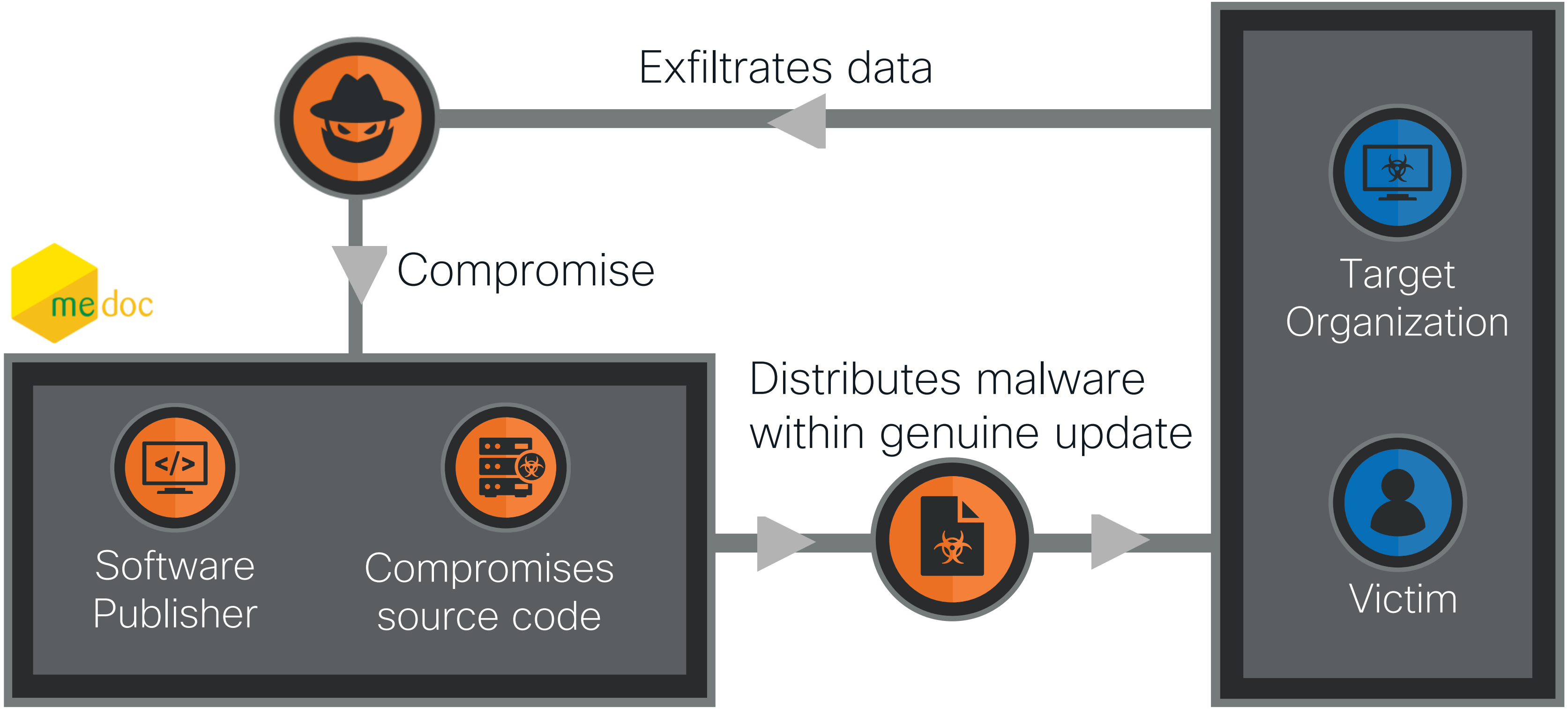
NotPetya



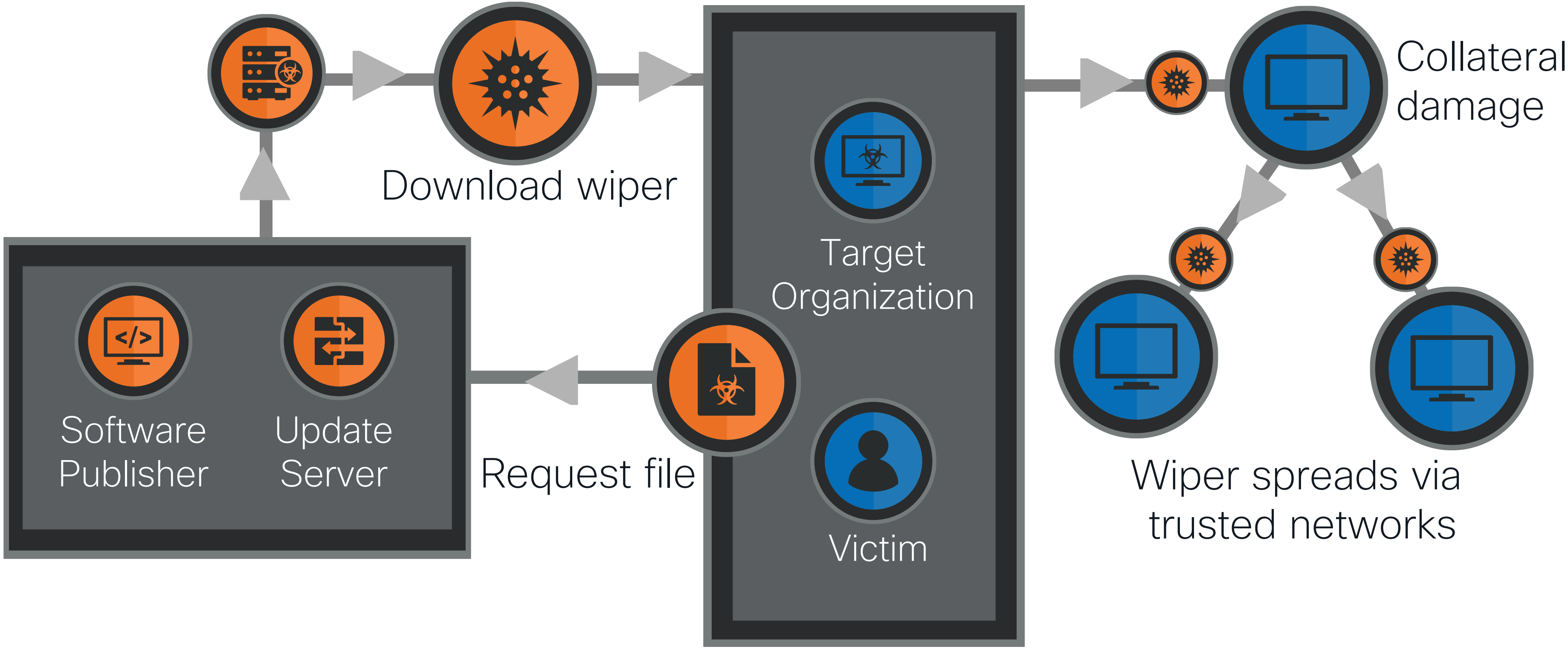
The world’s most destructive cyber attack.

A supply chain attack.

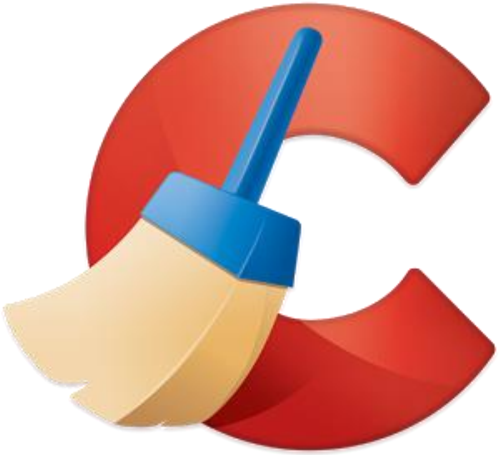
NotPetya (First Stage)



NotPetya (Second Stage)



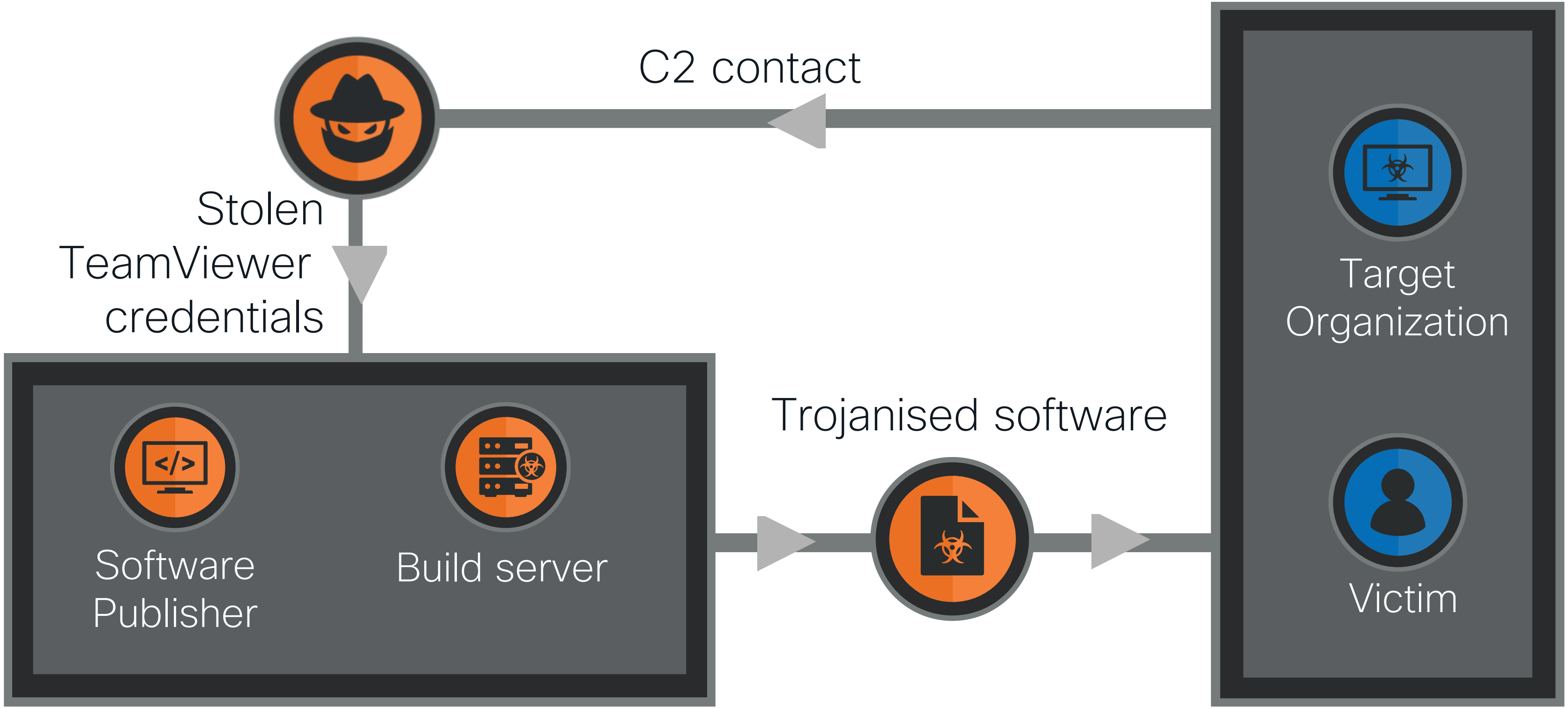
CCleaner



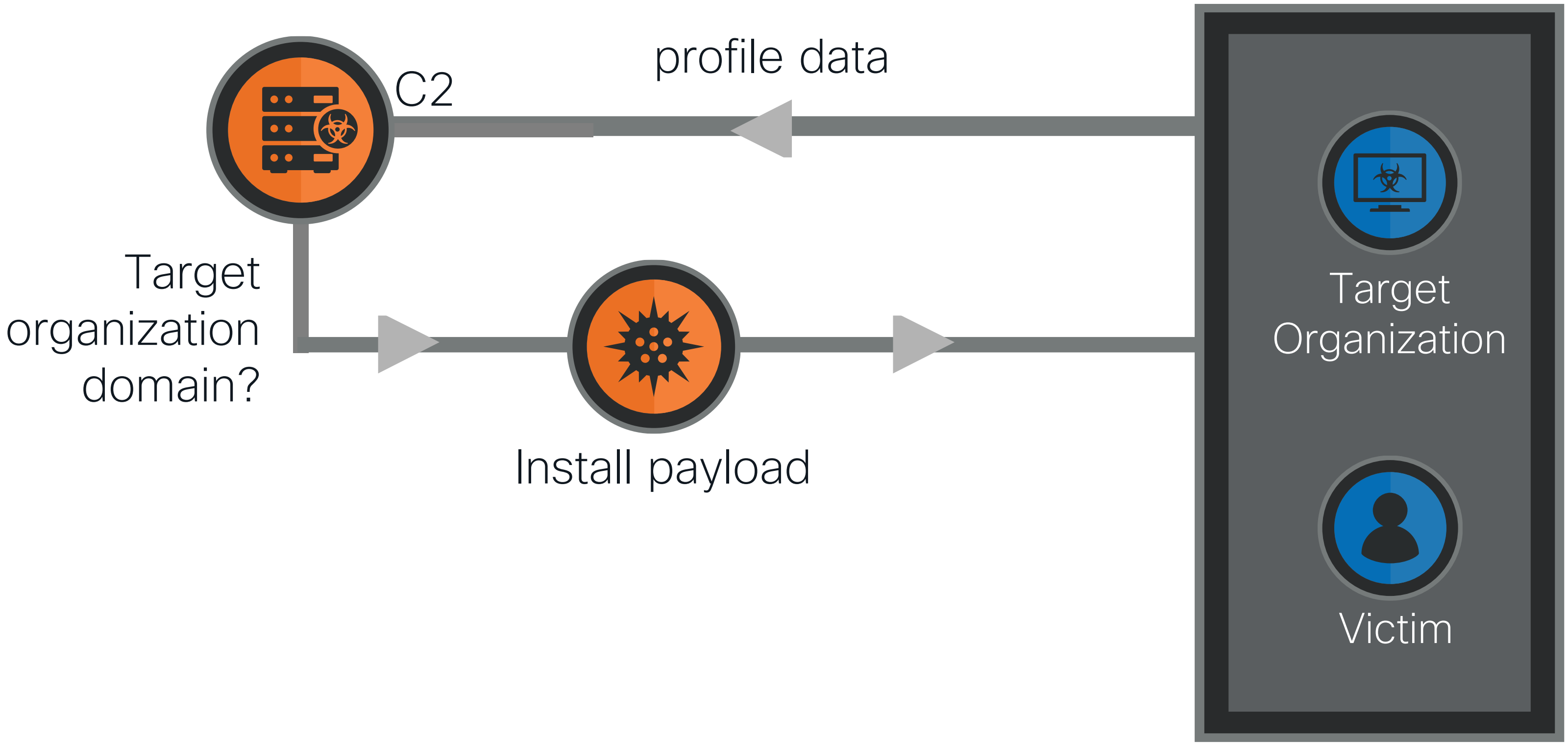
Mass compromise for targeted IP theft.

A supply chain attack.

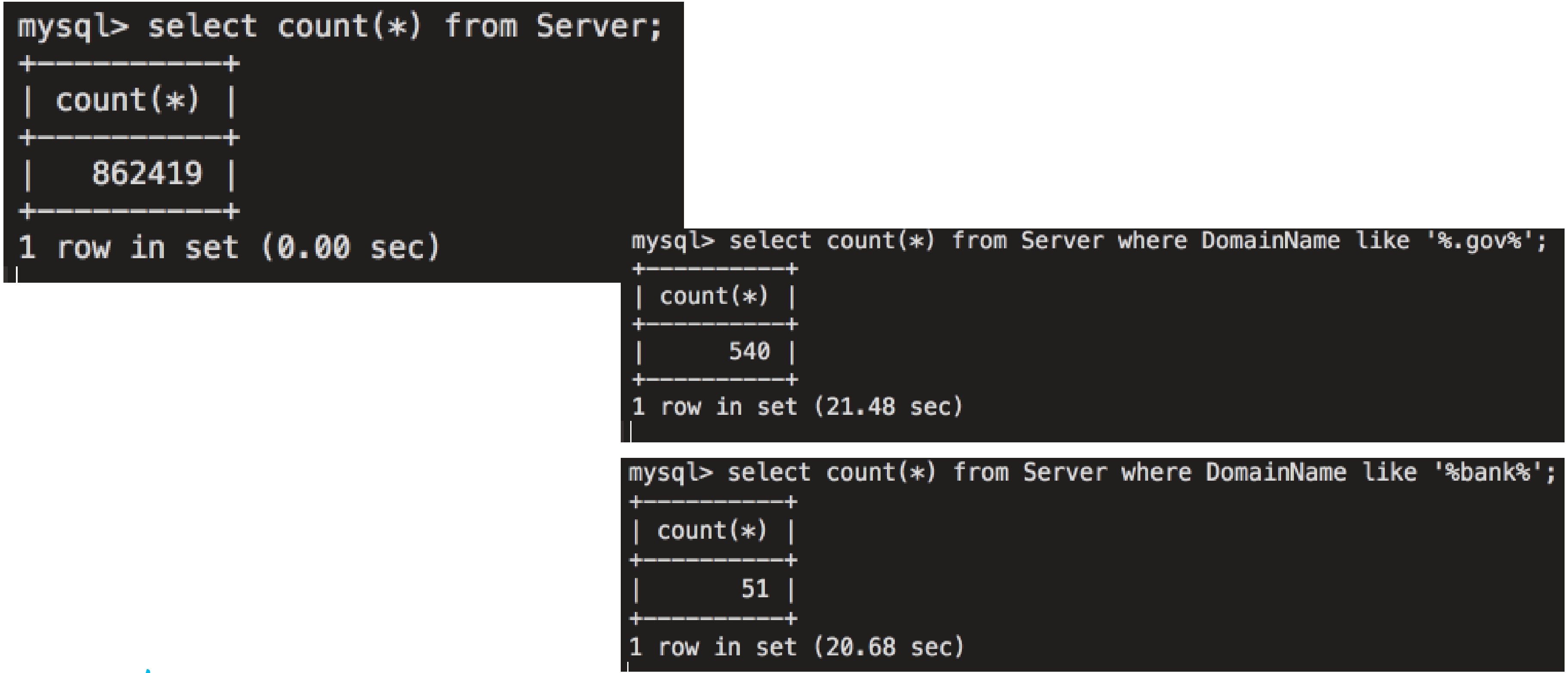
CCleaner (First Stage)



CCleaner (Second Stage)



CCleaner Effectiveness



```
mysql> select count(*) from Server;
+----------+
| count(*) |
+----------+
|   862419 |
+----------+
1 row in set (0.00 sec)
```

```
mysql> select count(*) from Server where DomainName like '%.gov%';
+----------+
| count(*) |
+----------+
|      540 |
+----------+
1 row in set (21.48 sec)
```

```
mysql> select count(*) from Server where DomainName like '%bank%';
+----------+
| count(*) |
+----------+
|       51 |
+----------+
1 row in set (20.68 sec)
```

2019 & 2020

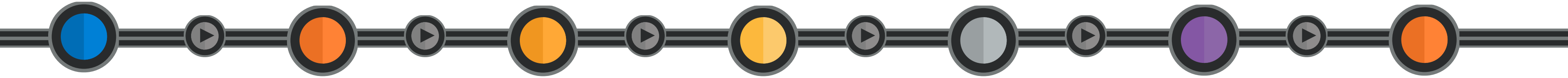
SolarWinds Orion

What - Back door integrated into SolarWinds Orion network management software

Who - Attributed to Russian state threat actors.

Impact – 18 000 customers potentially affected.

Timeline



Jan 2019
First evidence
of incursion

Aug 2019
C2 infrastructure
set up

12 Sep 2019
TA trial run
begins

4 Nov 2019
TA trial run
ends

20 Feb 2020
SUNBURST
back door deployed

4 Jun 2020
SUNBURST
removed

12/13 Dec 2020
Identification
& disclosure

Further Details

Privileges used to access the victim's global admin account and/or trusted SAML token signing certificate.

Forged SAML tokens used to bypass 2FA for services such as Office365 suite.

C2 server identified using a DGA, uses DNS for C2 traffic. Downloads second-stage payloads and exfiltrates data via C2.

Malicious network traffic appears as legitimate Orion protocols and the actors store information in legitimate plugin configuration files.

C2 IP addresses located in the same country as the victim.

2021

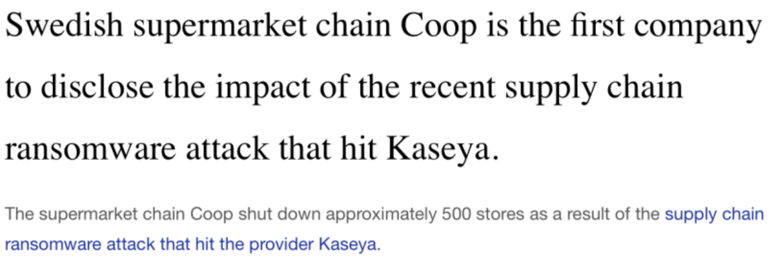
Kaseya VSA

Authentication bypass vulnerability in sys admin tool. Abused to distribute malware.

Who - Attributed to Revil criminal group.

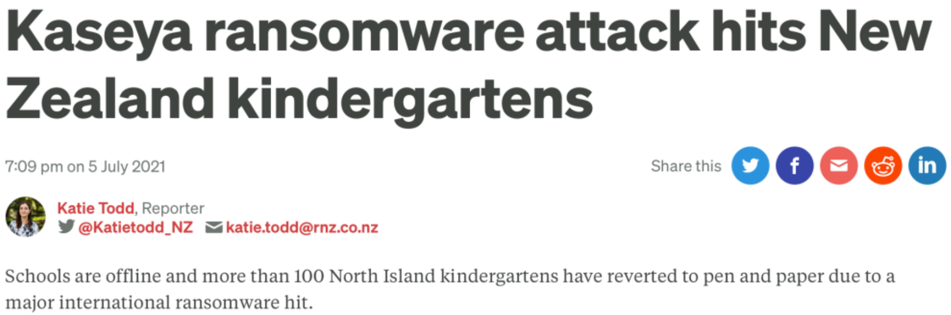
Impact – 800 to 1 500 customers of MSPs affected.

Kaseya VSA Breach Impact



Swedish supermarket chain Coop is the first company to disclose the impact of the recent supply chain ransomware attack that hit Kaseya.

The supermarket chain Coop shut down approximately 500 stores as a result of the supply chain ransomware attack that hit the provider Kaseya.

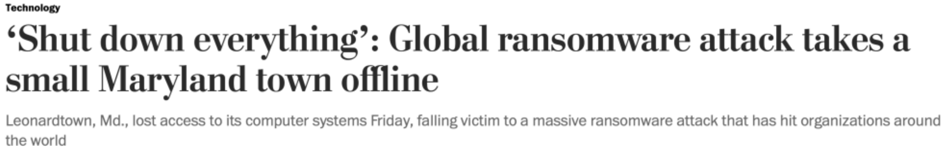


Kaseya ransomware attack hits New Zealand kindergartens

7:09 pm on 5 July 2021

Katie Todd, Reporter
@Katietodd_NZ katie.todd@rnz.co.nz

Schools are offline and more than 100 North Island kindergartens have reverted to pen and paper due to a major international ransomware hit.

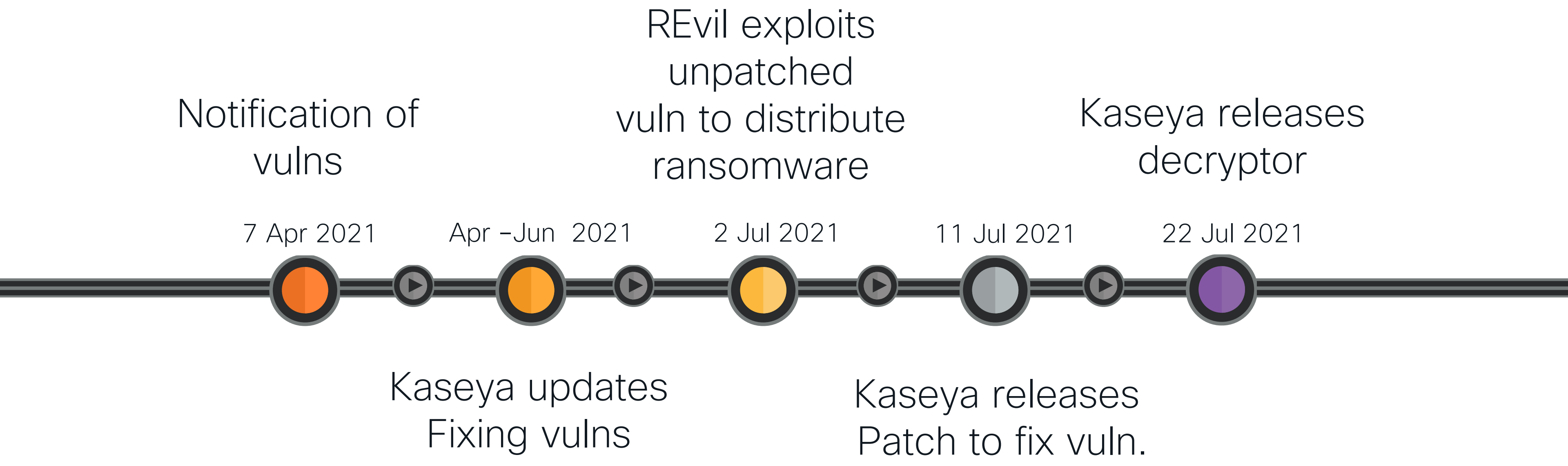


Technology

‘Shut down everything’: Global ransomware attack takes a small Maryland town offline

Leonardtown, Md., lost access to its computer systems Friday, falling victim to a massive ransomware attack that has hit organizations around the world

Timeline



7 Apr 2021

Notification of vulns

Apr -Jun 2021

Kaseya updates Fixing vulns

2 Jul 2021

REvil exploits unpatched vuln to distribute ransomware

11 Jul 2021

Kaseya releases Patch to fix vuln.

22 Jul 2021

Kaseya releases decryptor

2022

GoMet & unnamed software development company

What – Ukrainian software development company affected by GoMet backdoor.

Who – Likely Russian state-sponsored threat actors.

Impact – None. Attack detected and remediated.

Log4j

What – Easily exploitable vulnerability in widespread software package.

Who – Everyone!

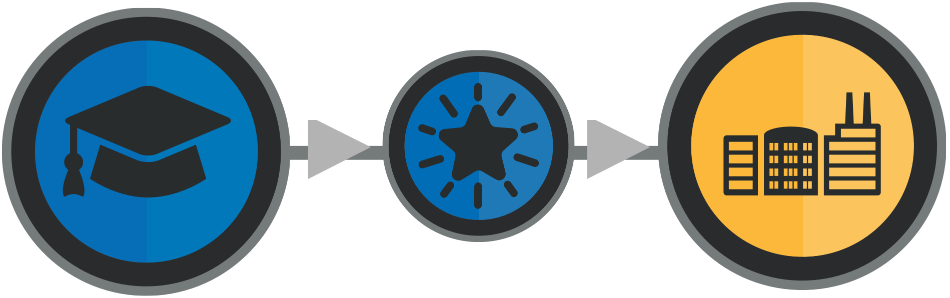
Impact – Widely used to distribute ransomware.

Protection

Provenance & Compliance

Is this the code expected?
Is there proof of provenance?

Does origin meet security requirements?
Clear manifest of bundled code?
(including external libraries)

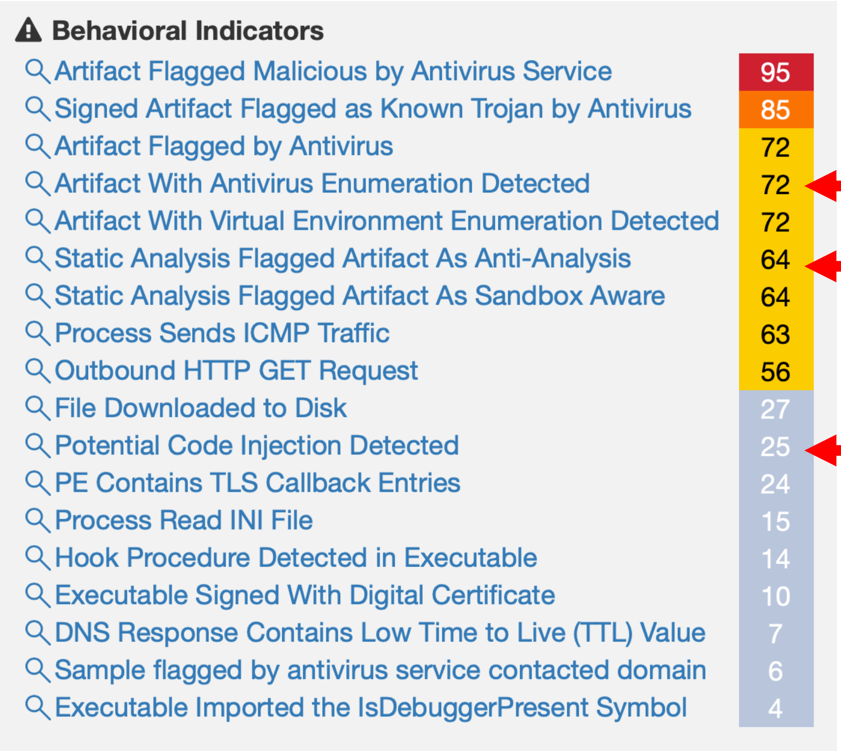


Secure Configuration

What are the minimum privileges necessary?
Does the code really need administrator privileges?

Restrict network access?
Segment networks to minimize risk exposure?

Verification – Code Analysis



⚠ **Behavioral Indicators**

Artifact Flagged Malicious by Antivirus Service	95
Signed Artifact Flagged as Known Trojan by Antivirus	85
Artifact Flagged by Antivirus	72
Artifact With Antivirus Enumeration Detected	72
Artifact With Virtual Environment Enumeration Detected	72
Static Analysis Flagged Artifact As Anti-Analysis	64
Static Analysis Flagged Artifact As Sandbox Aware	64
Process Sends ICMP Traffic	63
Outbound HTTP GET Request	56
File Downloaded to Disk	27
Potential Code Injection Detected	25
PE Contains TLS Callback Entries	24
Process Read INI File	15
Hook Procedure Detected in Executable	14
Executable Signed With Digital Certificate	10
DNS Response Contains Low Time to Live (TTL) Value	7
Sample flagged by antivirus service contacted domain	6
Executable Imported the IsDebuggerPresent Symbol	4

Indicator

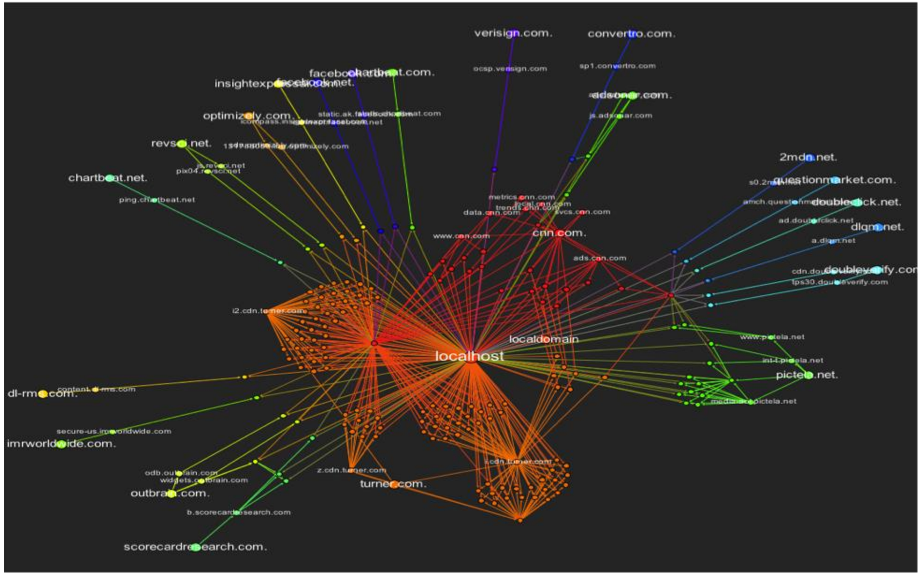
Indicator

Indicator

We can detect malicious code!

Needs investigation & response.
There will be false positives.

Verification – Network Traffic Analysis



We can detect malicious connections!

Needs investigation & response.
There will be false positives.

Conclusion

We are all reliant on the integrity of the supply chain.

- Identify your biggest exposure to 3rd party software.

(bad guys only need one install)

- Make security & compliance part of procurement.

(be realistic, vendors will wheedle out)

- Aggressively harden systems.
- Proactively hunt for incursion.
- Prepare & rehearse response.

Security Technologies

General Security Technologies

Learn about the different shades of cyber security in our daily lives and join us for a journey through various topics, from the depths of the darknet to the peak of crypto-analysis.

START

- Feb 7 | 08:30
  BRKSEC-2487
  Cat and Mouse - Defender's need better Mousetraps!
- Feb 7 | 10:00
  BRKSEC-2727
  6 Years of Supply Chain Attacks
- Feb 7 | 11:30
  BRKSEC-1240
  If you don't have a Security Reference Architecture, you must get one!
- Feb 7 | 11:30
  BRKSEC-2037
  Securing Starlink Internet Services
- Feb 7 | 12:20
  PSOSEC-1213
  The Evolution of Ransomware
- Feb 7 | 13:30
  BRKSEC-2354
  Automating Security: Just Because You Can, Doesn't Mean You Should
- Feb 7 | 14:00
  IBOSEC-3000
  Critical Requirements for Securing Government Networks
- Feb 7 | 15:00
  BRKSEC-2051
  The Evolution of DNS Security
- Feb 7 | 17:15
  IBOSEC-2012
  Ransomware Role-Playing: A Guided Tabletop Exercise with Talos Incident Response
- Feb 8 | 08:45
  BRKSEC-2227
  Evaluating and Improving Defenses With MITRE ATT&CK
- Feb 8 | 10:45
  BRKSEC-2172
  Peeling an Onion: A Short Travel into the Darknet

If you are unable to attend a live session, you can watch it On Demand after the event

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

ALL IN