Supply-chain Attacks

How one country is pwning us all, silently and effectively

whoami

REAQTA

www.reaqta.com

Alberto Pelliccione – CEO @ ReaQta

https://linkedin.com/in/albertopelliccione

Starting with a question

How to:

Compromise millions of devices
While remaining undetected
Without using a single exploit

A simple answer: Supply-chain. Or abusing the trust chain between a provider and its customers.

Understanding the motivations

Supply-chain attacks are a growing trend:

- Highly effective strategy
- Very hard to detect
- Can be used for both targeted and mass attacks

3 main reasons:

- Opportunistic targeting at scale
- Mass targeted espionage
- 4th party intelligence/data collection

Opportunistic Targeting at Scale

HACK IN BO®
Winter 2019 Edition
13ª EDIZIONE

Nice to meet you WINNTI

Nice to meet you WINNTI

2010 a new Threat Actor is born, later dubbed Winnti Umbrella

- Mainly targets Gaming Companies
- Steals digital certificates to reuse in further attacks
- Steals source codes and mines in-game gold currency to monetize

2011 Valve and Gameforge are breached

- 35M records stolen from Valve, undisclosed from GameForge
- 100k+ computers of Gamers become infected with a trojan
- Other 35 gaming companies worldwide are targeted by the group

The mistake: WINNTI was targeting the company but their trojan ends up being served as an update to an undisclosed “widely popular online game”

WINNTI Sudden Realization Moment

WHAT IF INSTEAD OF TARGETING THE COMPANY

WE TARGET THEIR CUSTOMERS

WINNTI Refocus

In 2014 WINNTI appears to refocus, what looked like a criminal gang changes strategy and aligns with different types of interests. Gaming remains an industry of interest but pharmaceuticals starts to be targeted more and more:

Bayer, BASF, Henkel, Roche are attacked by the same group

2018-2019 WINNTI keeps targeting some gaming companies

In Asia they repeat the same scheme as in 2011… 3 times

Garena, Electronics Extreme, Zepetto

Compromised games make 100k+ victims

One constant remains: the WINNTI backdoor keeps evolving over time, increasing in sophistication.

Putting the puzzle together

Mass Targeted Espionage

Target the masses, catch a few

Step 1) Acquire minimal information from a very large pool
Step 2) Identify key figures in key organizations
Step 3) Use the victims as a **bridge** for **targeted** attacks

Reasons

Possible lack of actionable intelligence on the intended target

More sophisticated or security-aware targets

Avoid alerting an entity that it is about to be targeted

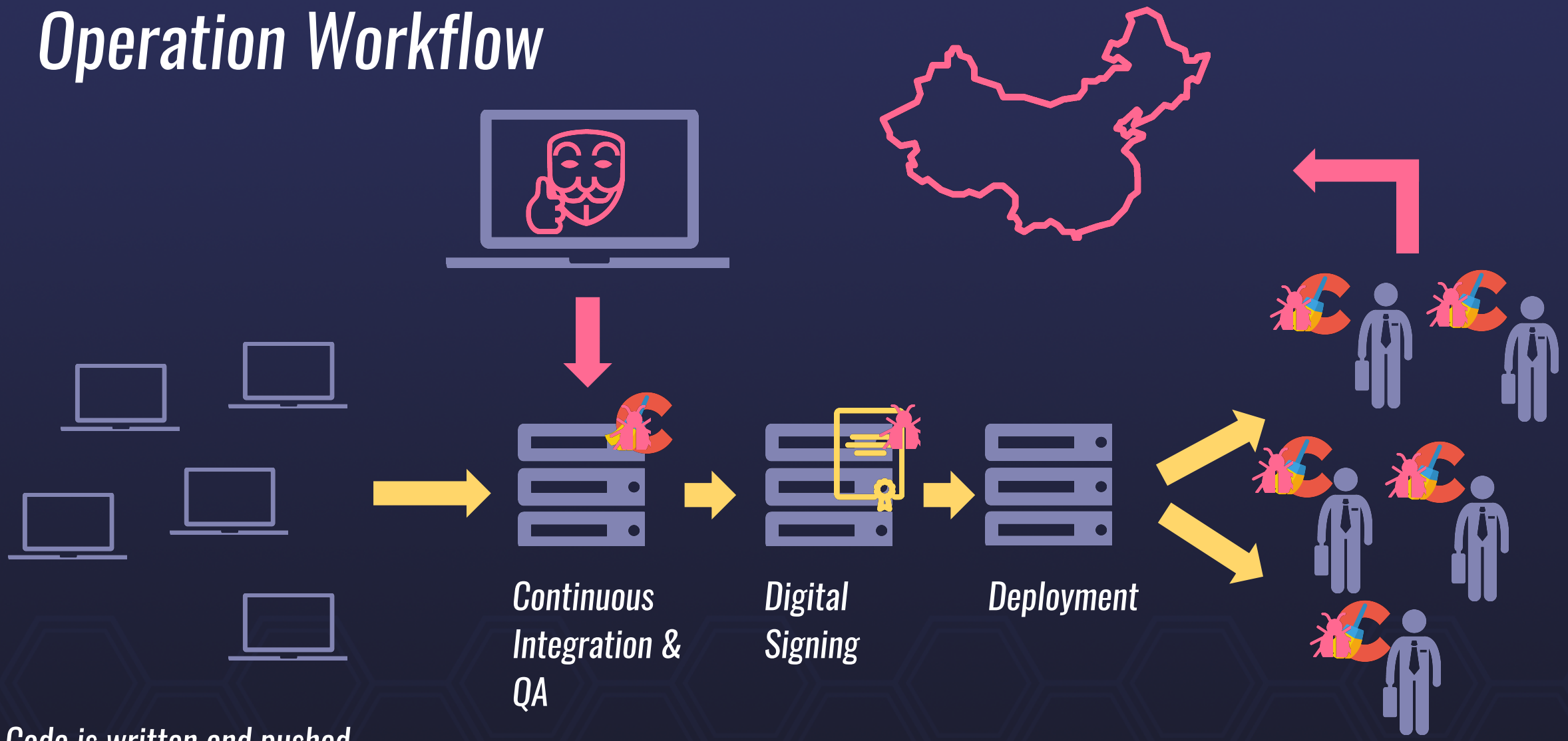
Nice to meet you BARIUM

March 2017 - CCleaner

Entrypoint

- Unattended workstation (TeamViewer) from one of Ccleaner's developers
- Barium installs first a VBS malware on the machine
- Then they deploy **ShadowPad** malware
- After that the supply-chain attack begins

Operation Workflow



March 2017 - CCleaner

Targets

2.27M devices with 1st stage backdoor

40 devices with 2nd stage backdoor

Akamai, Asus, Cisco, D-Link, Fujitsu, Google, HTC, Intel, Linksys, Microsoft, Samsung, Singtel, Sony, VMWare

June 2018 - ShadowHammer

Barium manages to sign a modified Asus binary from 2015 with an Asus certificate
The trojan is hosted on the Asus Update Server
It remains silent if the MAC address of the victim is not recognized
Around 100.000 infections, only 600 MAC addresses targeted

Linking the attacks

HACK IN BO Winter 2019 Edition
13ª EDIZIONE

4th Party Collection

4th Party Collection

Attack those with the keys to the Kingdom

- Effective against hard targets
- Potentially offers a privileged access to a well defended infrastructure
- Attacks are much harder to detect

Multiplication factor in effect if the targeted entity is a MSP

Hello APT10, welcome to the party!

Apr 2017 – APT10 – Operation CloudHopper

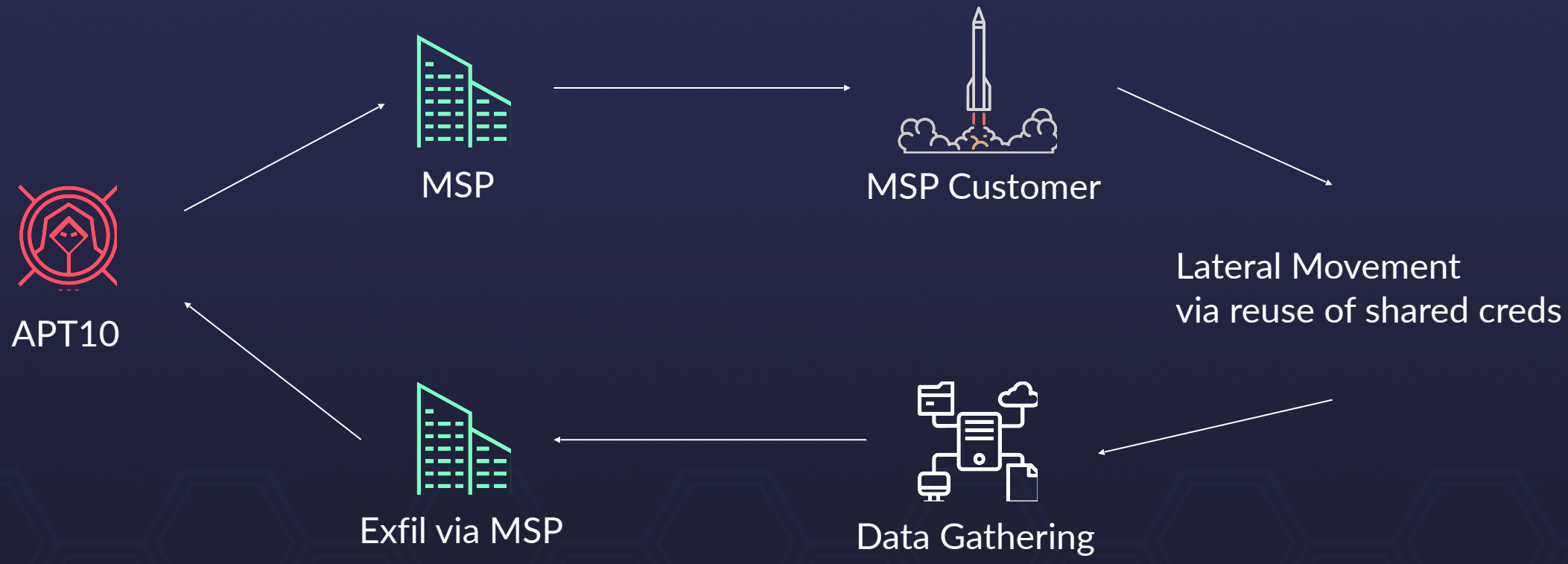
Entrypoint

MSP via carefully crafted Spear Phishing campaigns

Targets

Aligned with China's FYP: aerospace, new materials, robotics, next-gen IT…
MSP (Enterprise Services and Cloud Hosting) and their customers (IP theft)
High value system (for high level access) and low value (for persistence)
Remains persistent for very long time

Operation CloudHopper Workflow



HACK IN BO
Winter 2019 Edition
13ª EDIZIONE

September 2019 - Airbus

4 Airbus suppliers are breached

- Rolls Royce (engines)
- Expleo/Assystem (avionics)
- 2x undisclosed

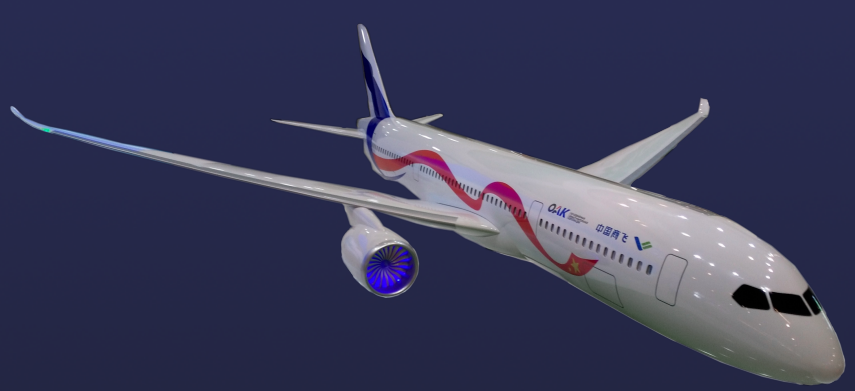
Target: certification process, engines for A400M and A350

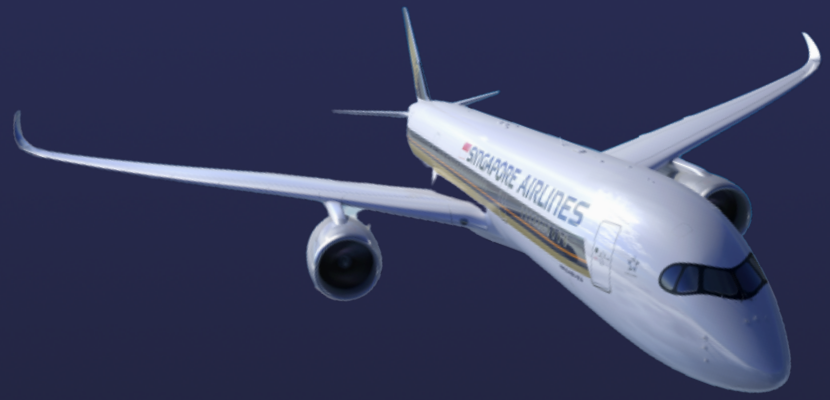
Enter COMAC – ARJ21

Development started: 2002
Maiden flight (planned): 2005
Maiden flight (effective): 2008
First commercial flight: 2016

Problems: avionics, wiring, wing cracks etc…

Enter COMAC – CR929





CR929
Engines: 2
Aisles: 2
Passengers: 250-290
Length: 64M
Thrust: 86000 lbf (Trent 1000?)
Range: 12000KM

A350-900
Engines: 2
Aisles: 2
Passengers: 315
Length: 66M
Thrust: 87000 lbf (Trent XWB)
Range: 15000KM

HACK IN BO®
Winter 2019 Edition
13ª EDIZIONE

Linking the attacks

HACK IN BO®
Winter 2019 Edition
13ª EDIZIONE

Increasing Sophistication

2019 – ICEFOG

Entrypoint

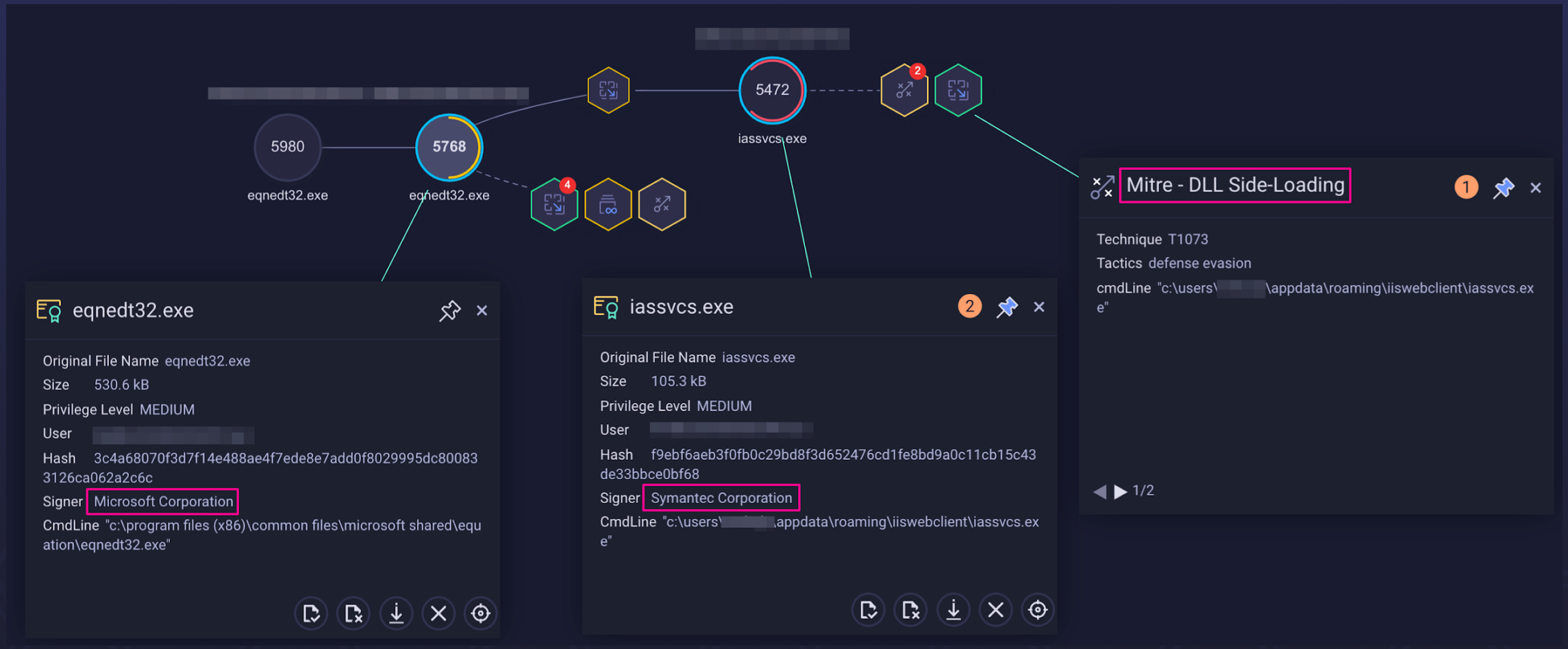
Supply-chain **defence** contractors

ICEFOG is shared among **many** groups (APT15, APT9, Roaming Tiger)

Targets

Defence, Governments, High-Tech

2019 – ICEFOG (file-less payload)



HACK IN BO Winter 2019 Edition 13ª EDIZIONE

Completing the Puzzle

The Final Picture

HACK IN BO® Winter 2019 Edition
13ª EDIZIONE

Conclusions

Supply-chain attacks are highly effective

1) to hunt for targets
2) to get into highly secured infrastructures

Hard to detect due to trust chain between suppliers and customers

1) Network monitoring and anomaly detection do help
2) Behavioral Analysis on the endpoint is effective