Actors, threats and incidents today, and how to survive them

Jess García
@j3ssgarcia - jess.garcia@one-esecurity.com
Founder and CEO of One eSecurity
Senior SANS Instructor
www.ds4n6.io - Project leader

WhoAmI

Jess García

jess.garcia@one-esecurity.com

@j3ssgarcia

- Founder and CEO of One eSecurity
  25+ years of experience in CybSec / DFIR
- Global DFIR company for over 17+ years
  www.one-esecurity.com
- DS4N6 Project Leader
  www.ds4n6.io
- Senior Instructor at SANS Institute
  22+ years (10+ courses)

Index

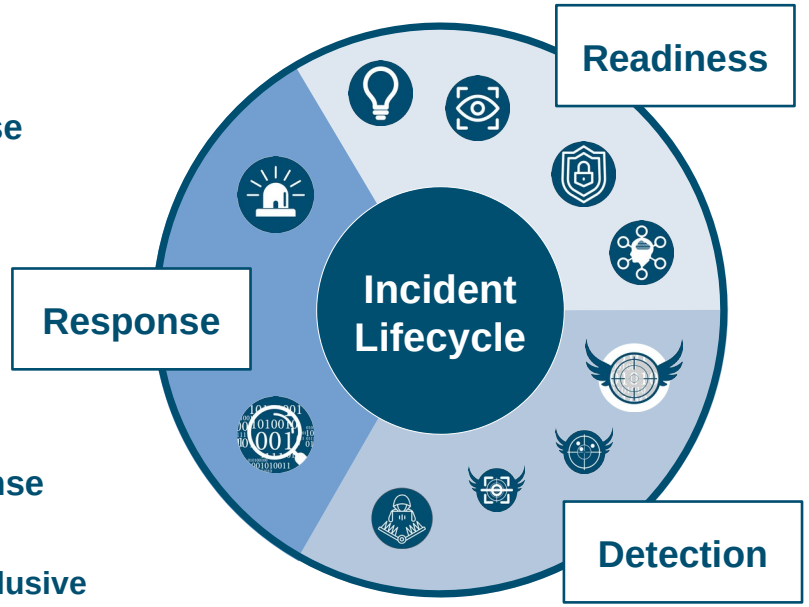
- Intro
- Roadmap to Detection & Response Maturity
- Case Studies
- How Can We Help?

Who Are We?

"We assist organizations in the preparation for and management of incidents"

*Market leading **DFIR** specialized **Global Service Provider**, fighting the most aggressive cyberadversaries **from the trenches** since **2007***

- ✓ **Flexibility**
- ✓ **Deep Expertise**
- ✓ **Adaptability**
- ✓ **Forensic Vision**
- ✓ **Rapid Response**



SANS exclusive partners in Spain

*Our **main clients** are **multinational** companies with **global** presence to which we provide different services, including:*

Global **Fortune 500**	**International** Institutions	**European** Agencies	Clients in **100+ Countries**

Large companies of numerous **sectors** (Finance, Energy, Telecom, Construction, Security and Defense, etc.)

40+ Forensics GIAC Certified DFIR Professionals working as **One global integrated team** ready to be deployed within hours

Before We Start…
Models Models Models

Roadmap to Detection & Response Maturity

Detection & Response Maturity

Depth

Incident Response RETAINER

Technology	People &Talent	Monitoring	DFIR Assessment + Cyber Threat Intelligence	Cyber Exercises	Proactive Detection & Response	Purple Team
SIEM	Talent Recruitment	SOC	Threat Landscape (TL)	Workshops	Compromise Assessment (CA)	Adversary Emulation (AE)
EDR	Training & Knowledge Management (KM): 1. Fundamentals 2. Advanced	Correlation	Incident Response Plan (IRP)	Cyber Exercises: 1. Tabletop 2. Top-bottom tabletop 3. Real interaction 4. Real offensive 5. Detectable activity 6. Real attacks	Threat Hunting (TH): 1. Intelligence based 2. Hypothesis based 3. Anomaly based	Deception
XDR	Knowledge Updates & Challenges	Use Cases	Data Source Analysis (DSA)		Managed Detection & Response (MDR)	
SOAR	Talent Retention Strategy	Cyber Threat Intelligence (CTI)	Playbooks			
		Artificial Intelligence (AI)	IRMM Gap Analysis			

Case Studies

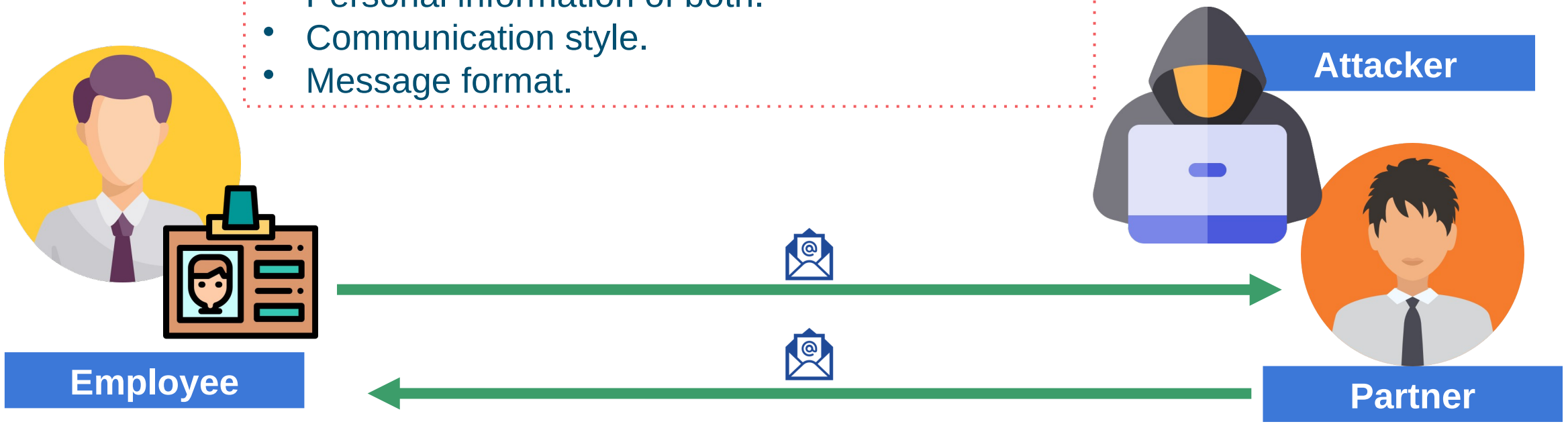
Identity theft case

What happened?

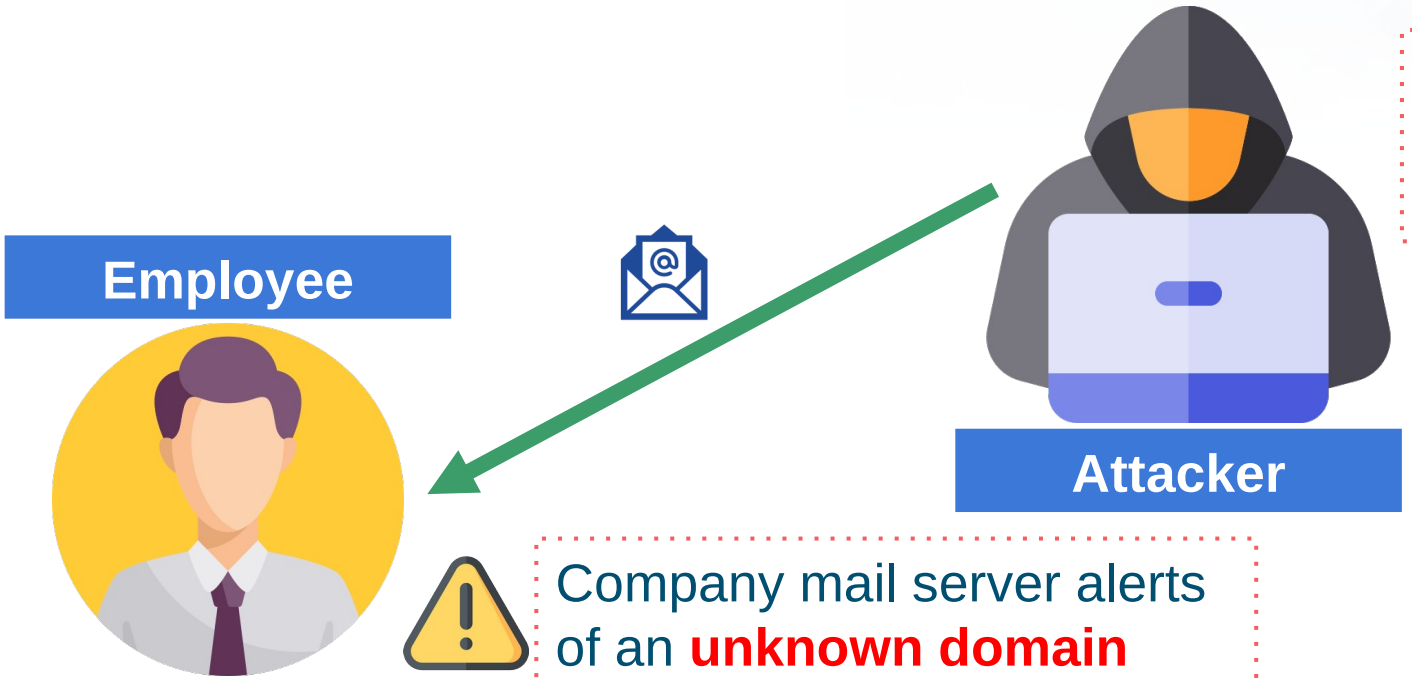
What happened?

Attacker has access to the content of all e-mails exchanged between employee and partner.

- Personal information of both.
- Communication style.
- Message format.



What happened?



Typosquatting: Attacker sends an email to the employee with the domain: **partner@domain_.com**

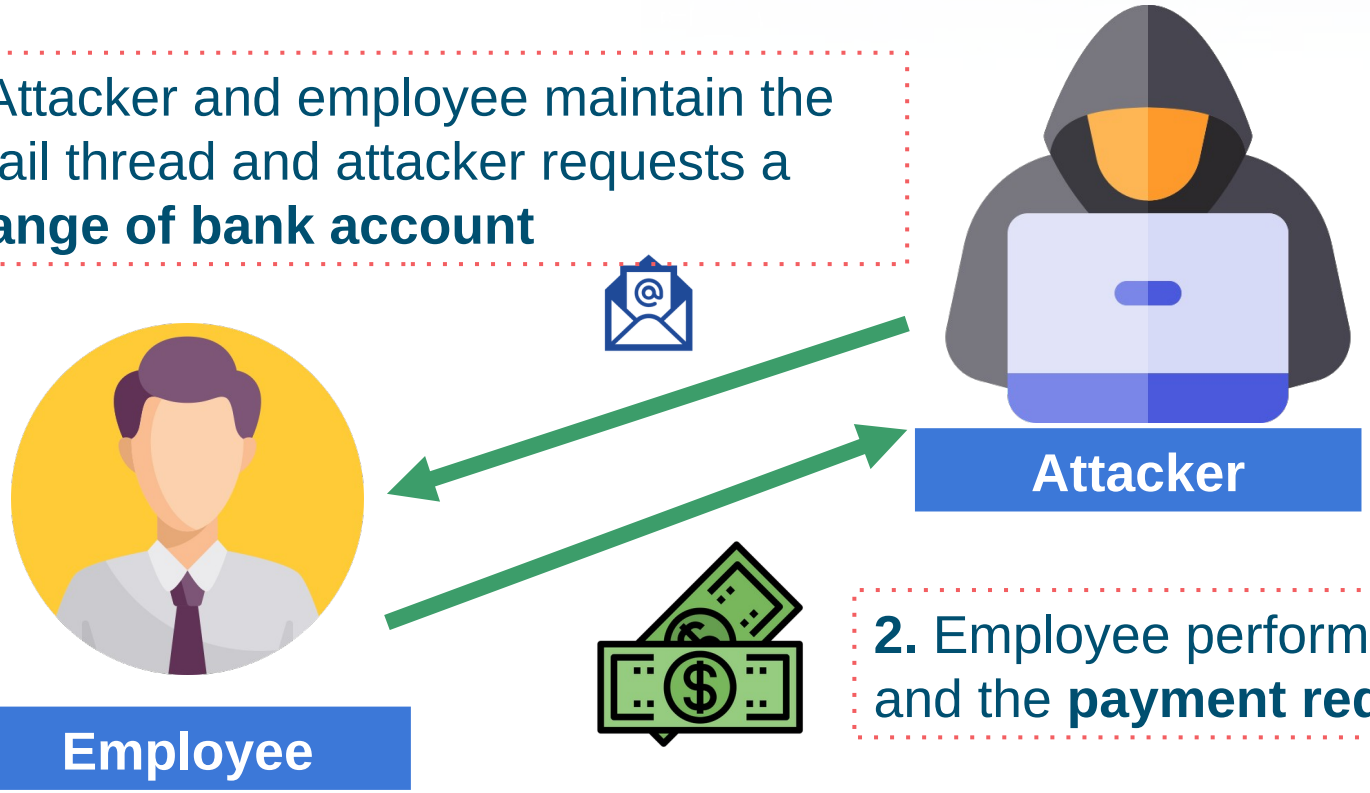
Company mail server alerts of an **unknown domain**

You don't usually receive emails from partner@domain_.com. Why is this important?

[CAUTION: EXTERNAL EMAIL- Careful with links and attachments.]

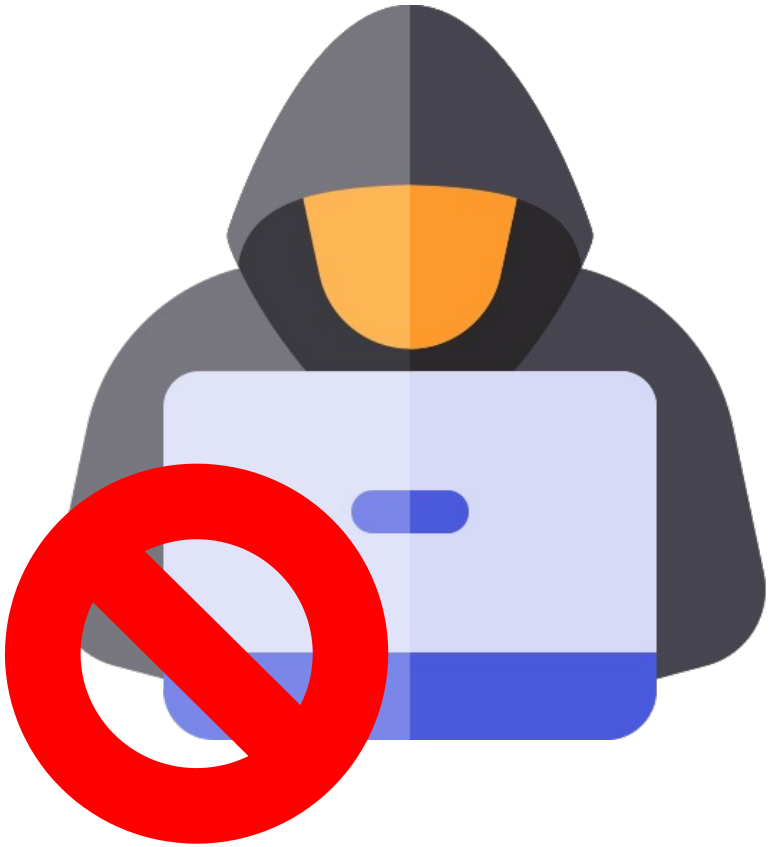
What happened?

1. Attacker and employee maintain the email thread and attacker requests a **change of bank account**



2. Employee performs the change of bank account and the **payment requested by the attacker**

To be improved



Security Awareness:

- Pay attention to warnings/alerts about cybersecurity risks.
- Do not share personal/private information.

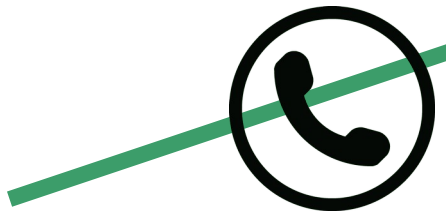
Procedures:

- Verify any change that may be a cause for fraud.

Attack on the supply chain case

What happened?

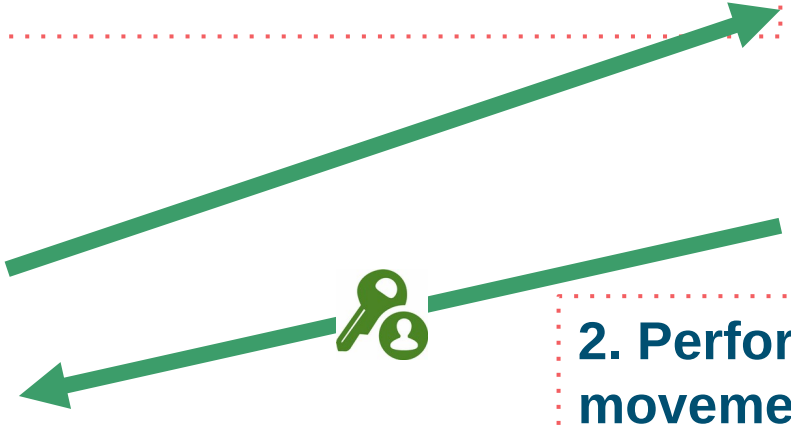
1. Company has a Call Center as a supplier that has the data of a company's customers

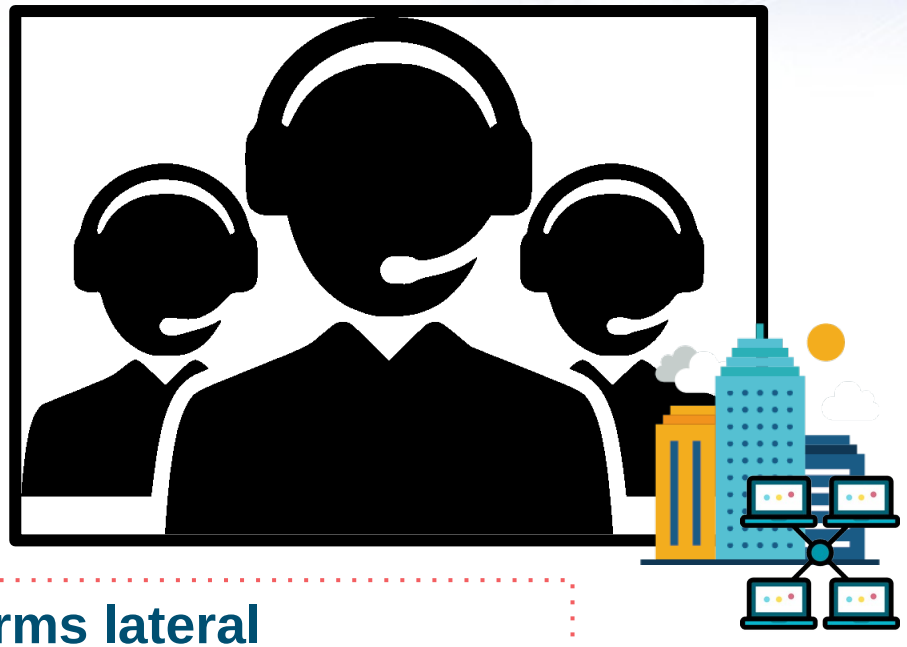


2. Attacker vishing Call Center employee posing as IT team member

What happened?

1. Attacker installs malware on employee's machine and gets employee's credentials
VPN access enabled





2. Performs lateral movements and password attacks
Credentials of several Call Center employees are obtained

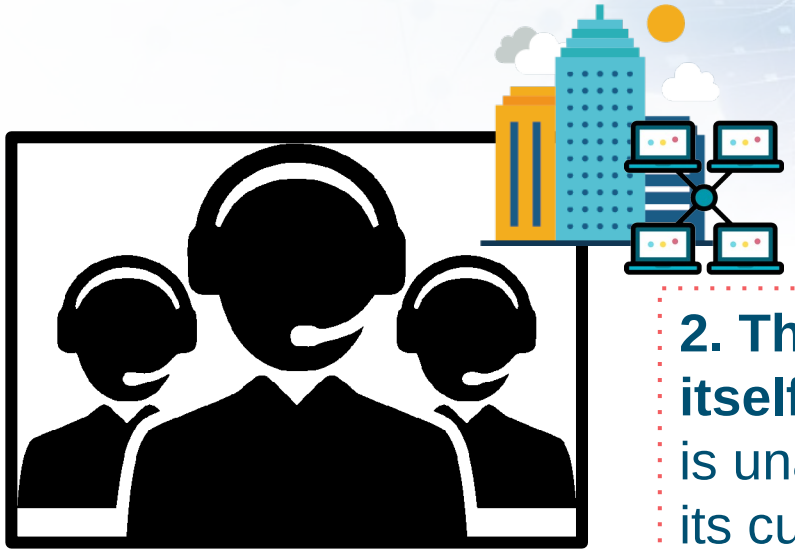
What happened?

1. Attacker modifies customer conditions of the company

2. Attacker tries to move laterally to the company's network

ALERT: Detected movement

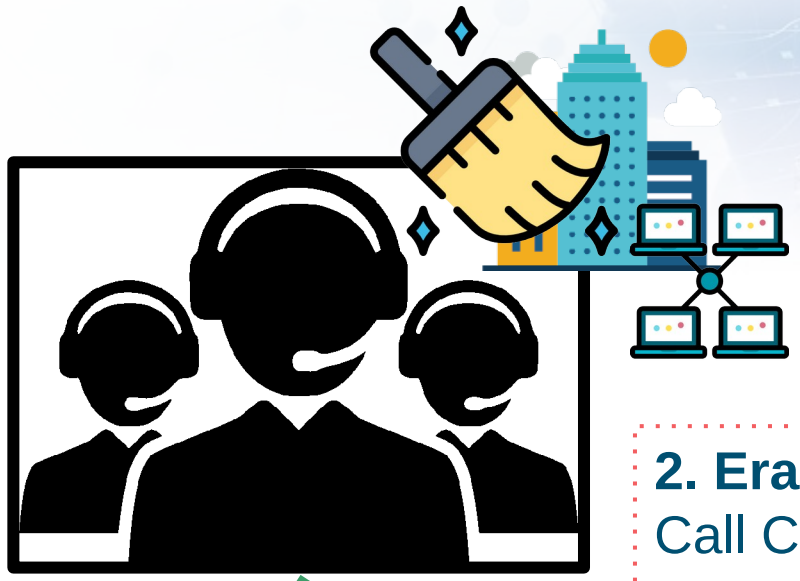
What happened?



1. The company disconnects from its Call Center
IR team is called in

2. The company isolates itself from its Call Center and is unable to provide service to its customers

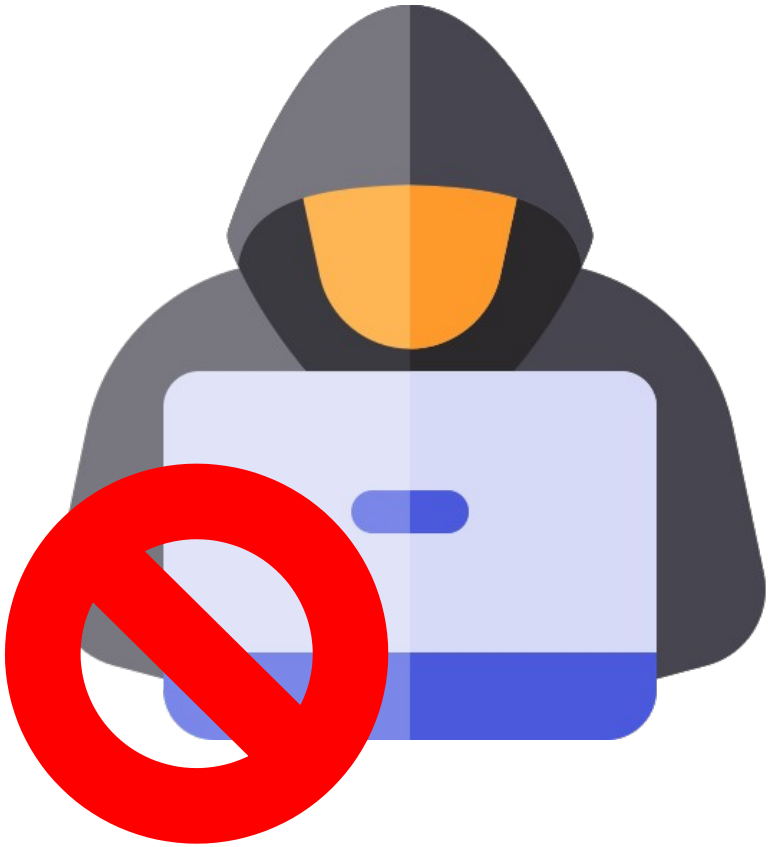
What happened?



1. Scope of the total equipment and correct eradication is **ensured**

2. Eradication completed: the Call Center is reconnected to the company

To be improved



Call center (supplier):

- VPN with 2FA.
- Monitoring and alerting.
- User training.
- AV with strong detection.

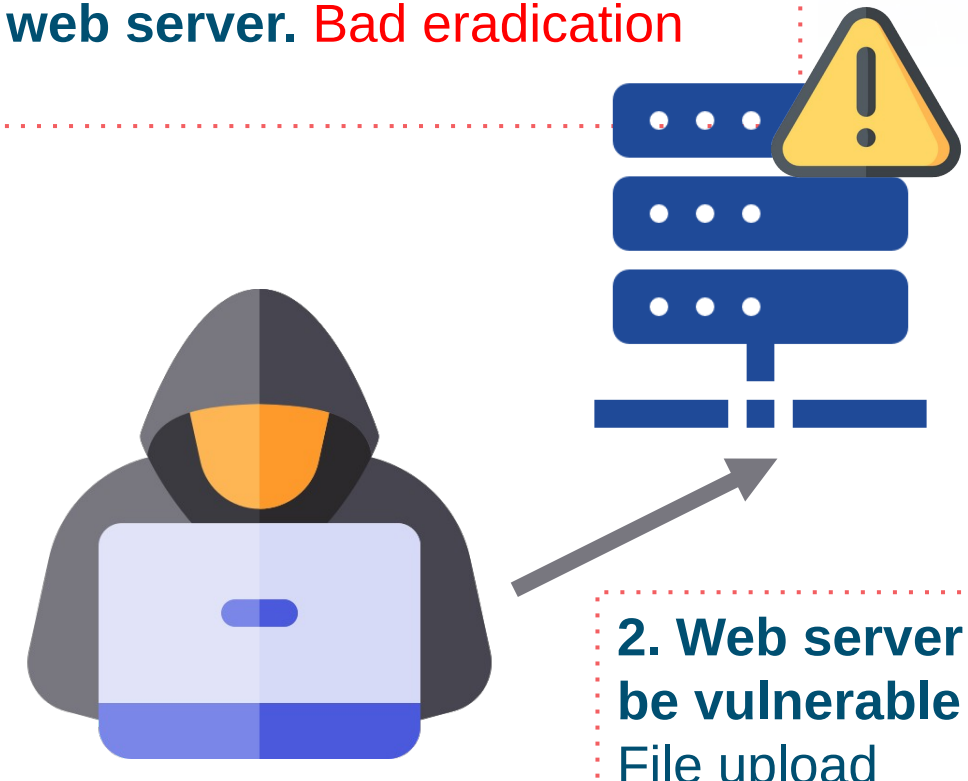
Company:

- Require good security practices from your vendors.

Fraud case: Fraudulent transactions as legitimate

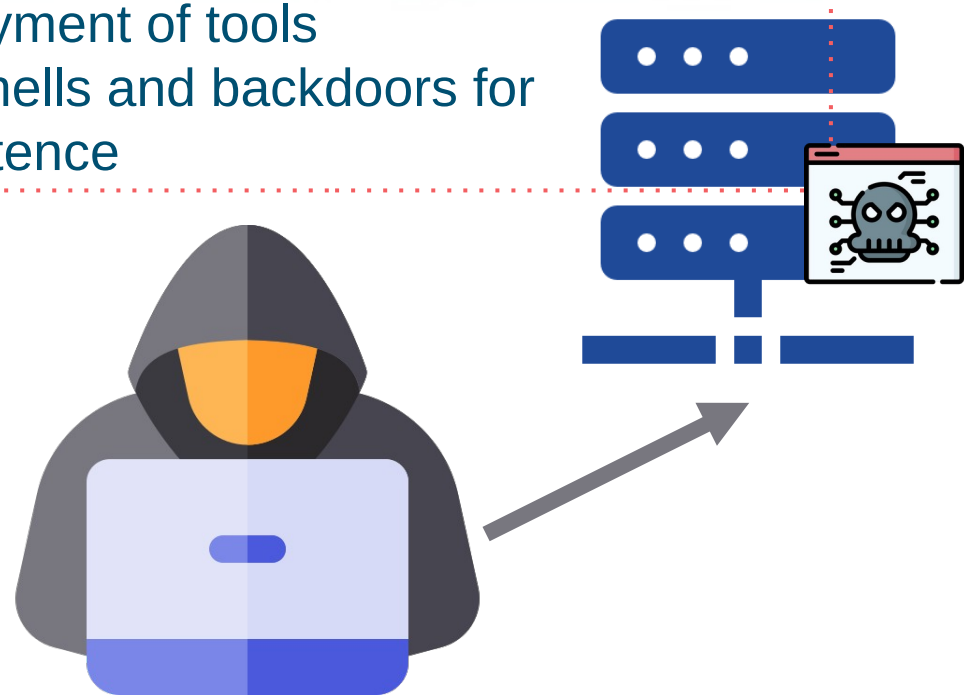
What happened?

1. Previously compromised web server. Bad eradication

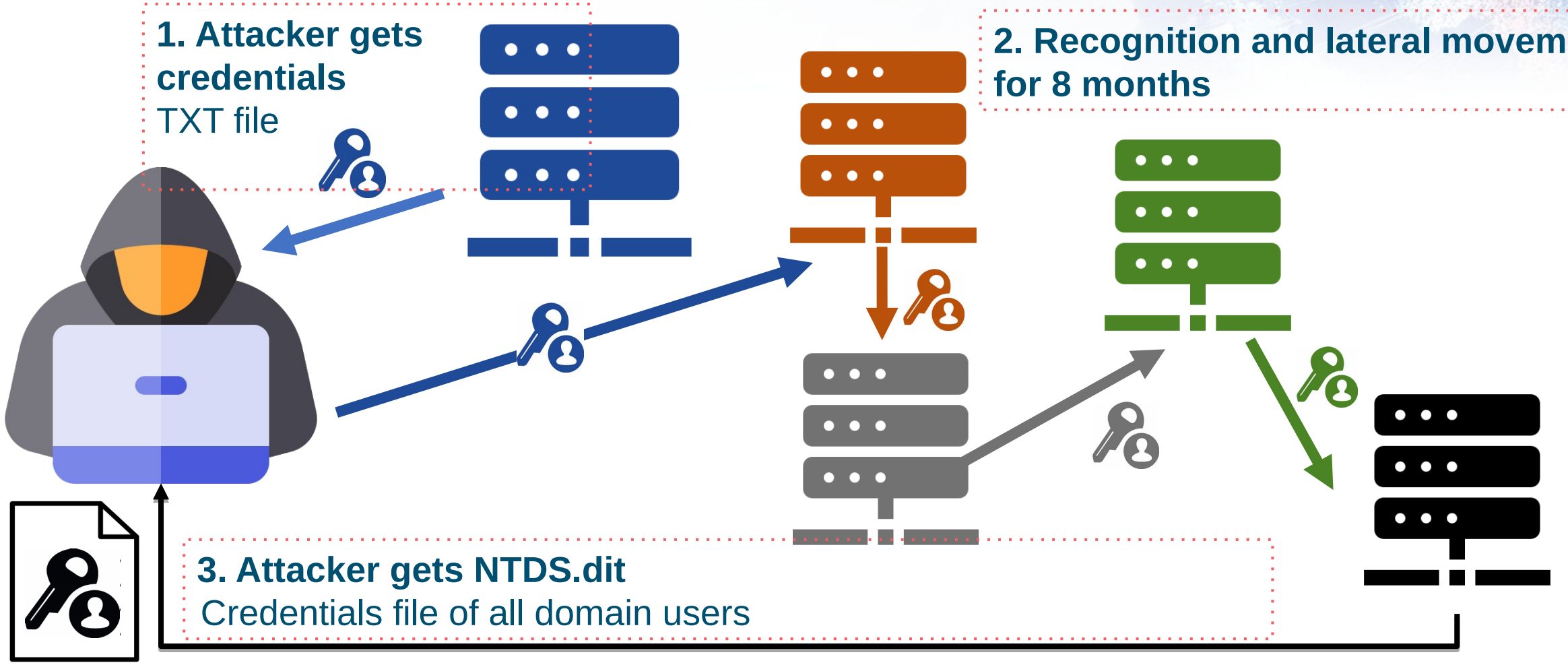


2. Web server continues to be vulnerable
File upload

3. Months later the attacker again exploits the same vulnerability.
Deployment of tools
Webshells and backdoors for persistence

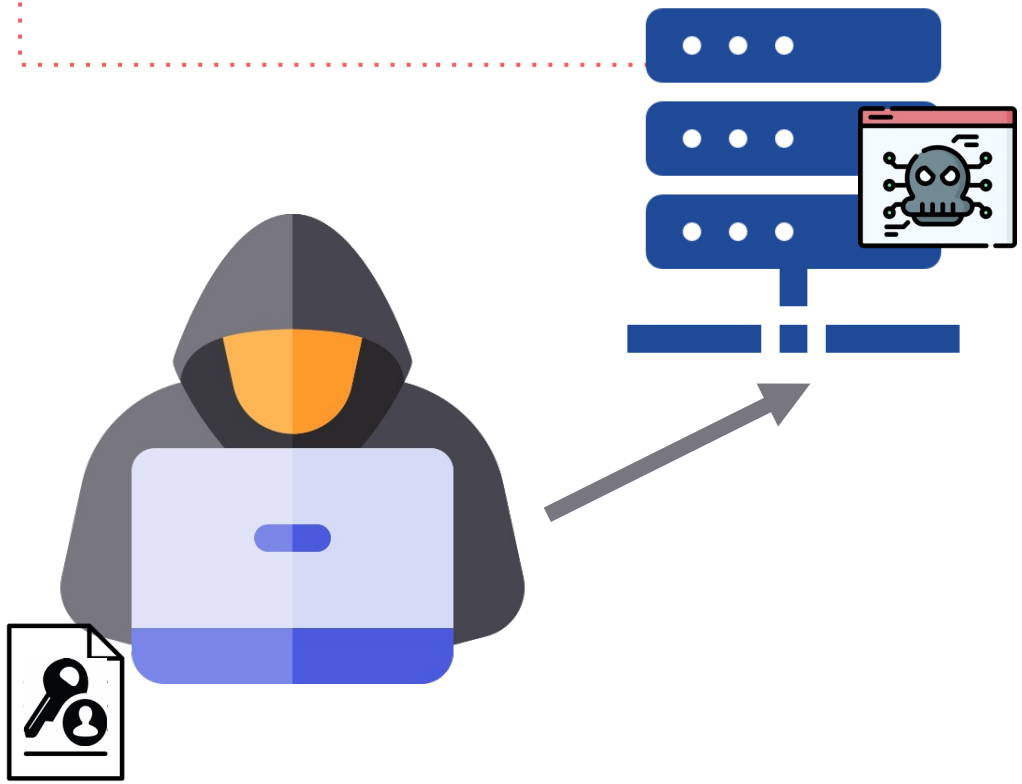


What happened?

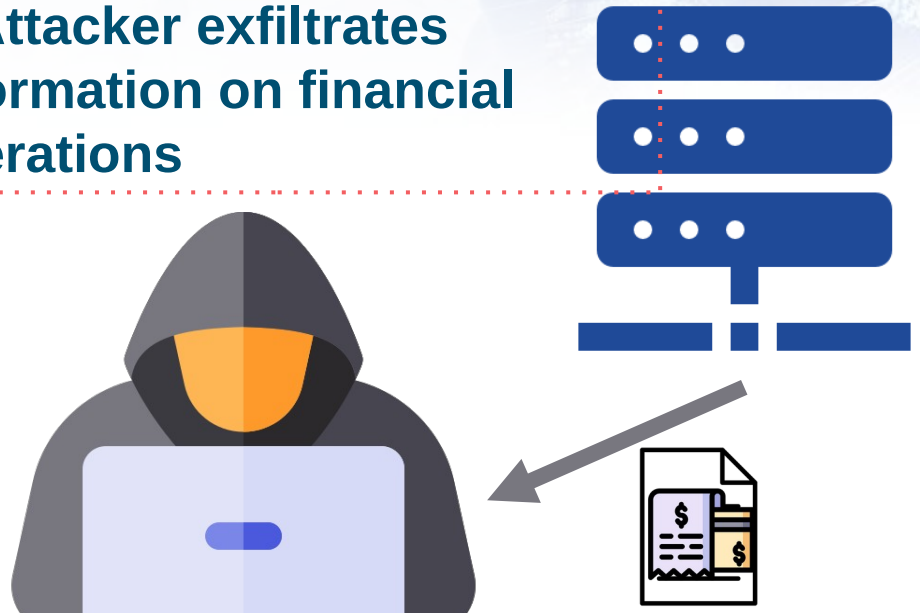


What happened?

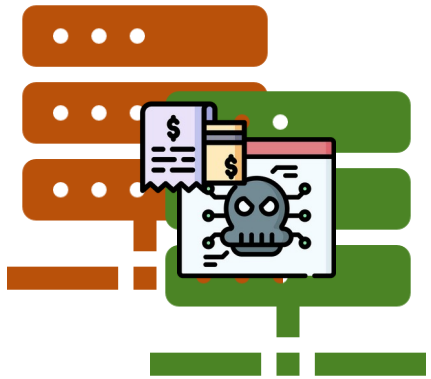
1. File server commitment



2. Attacker exfiltrates information on financial operations

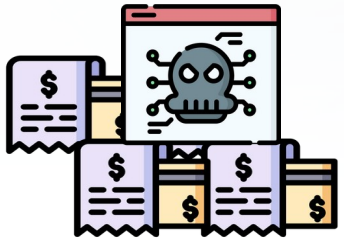


3. Commitment of SAP and transactional servers



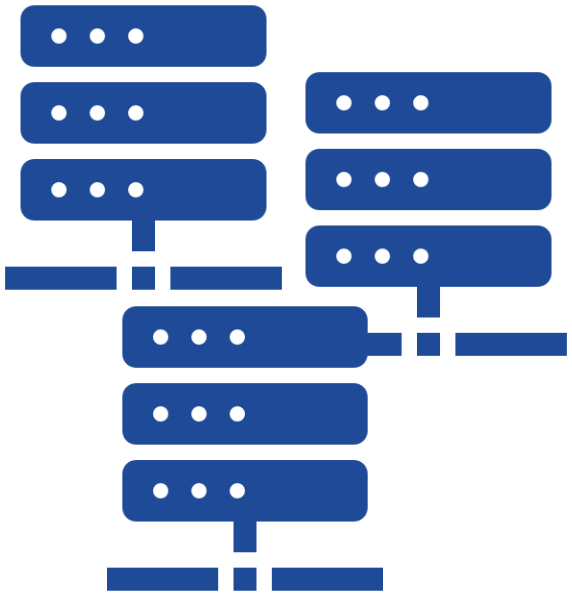
What happened?

1. Modification of legitimate transaction files



3. Execution of transactions with changes in the addressee

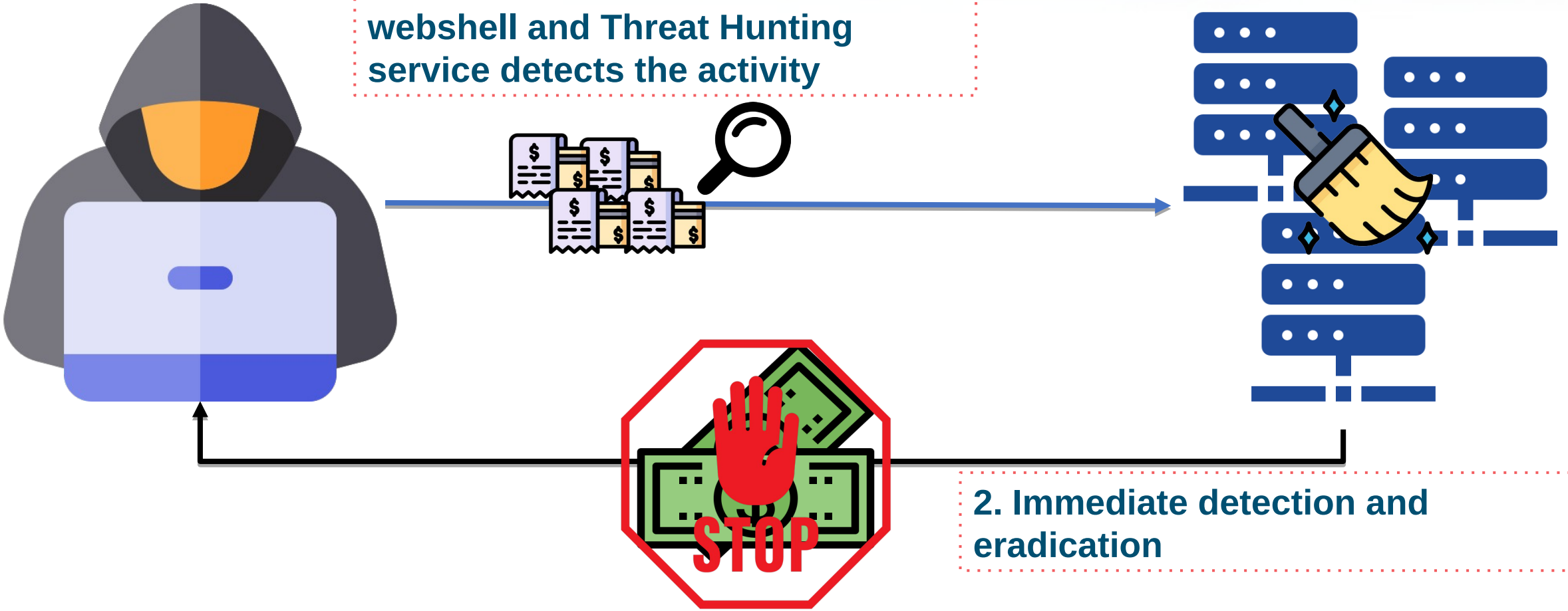
2. Encryption of fraudulent transactions with legitimate process



4. High amounts of money are obtained

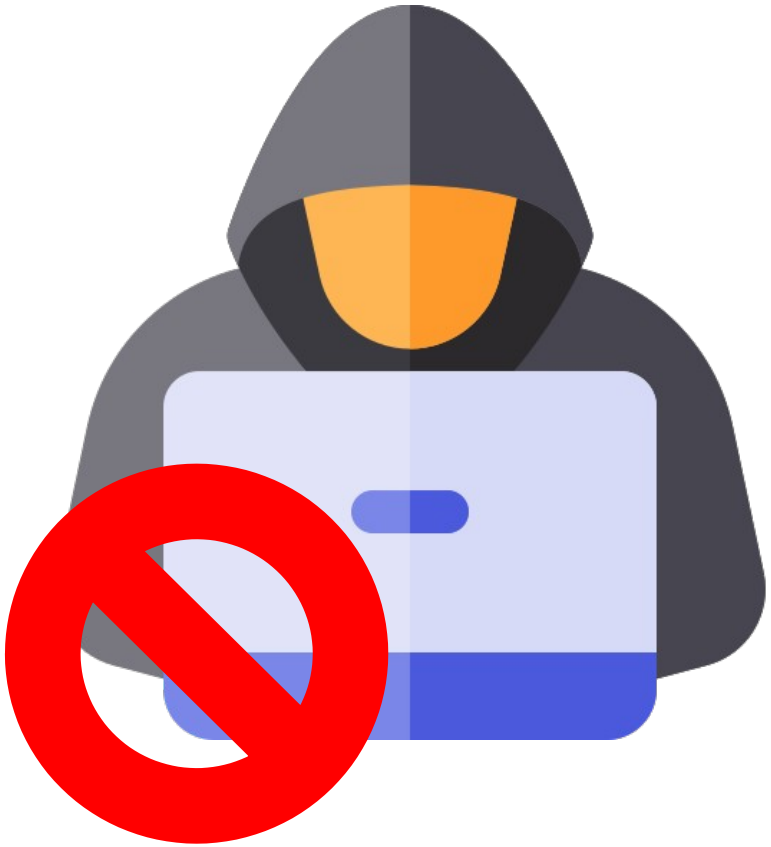
What happened?

1. Attacker accesses remnant webshell and Threat Hunting service detects the activity



2. Immediate detection and eradication

To be improved

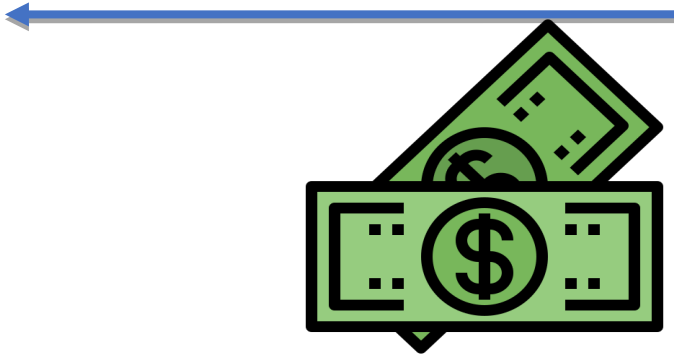


- Proper eradication of incidents.
- Transaction verification.
- Proper management of user permissions and passwords.
- Vulnerability detection.
- Monitoring and perimeter security.
- Segmentation and controls.
- Proper EDR configuration.
- Threat Hunting Service.

Jackpotting case
ATM robbery

What happened?

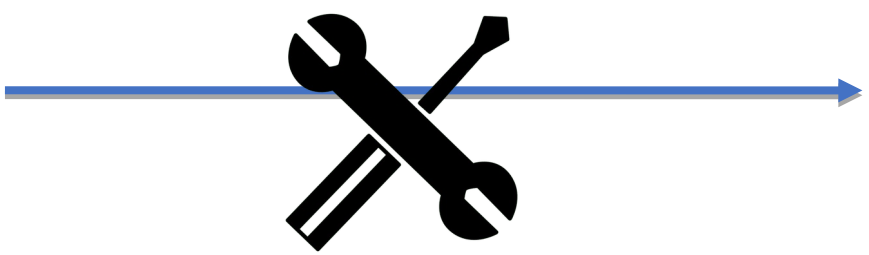
1. High cash withdrawals from ATMs were detected

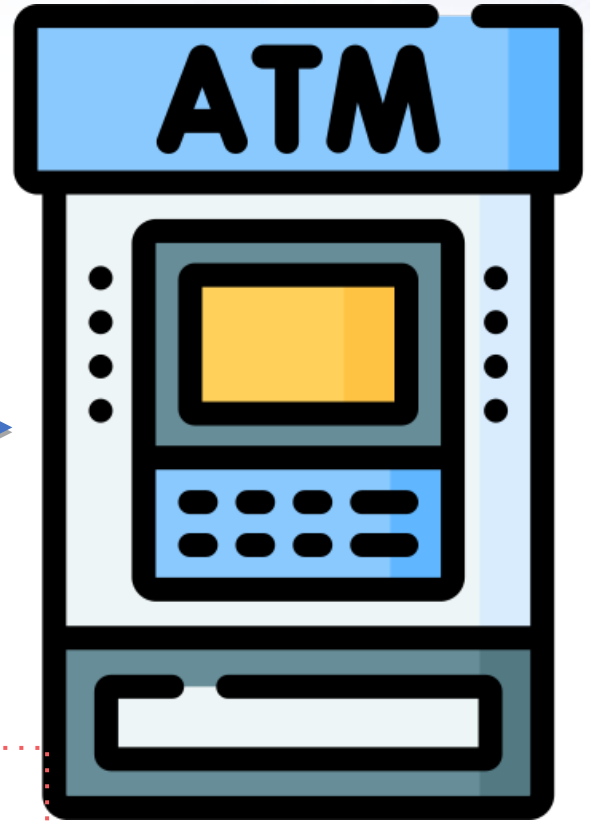


2. Vulnerable ATMs
Black-box attack

What happened?

1. Attacker repeatedly disassembles the same ATM to connect a Blackbox device that provides direct access to the ATM's SW.

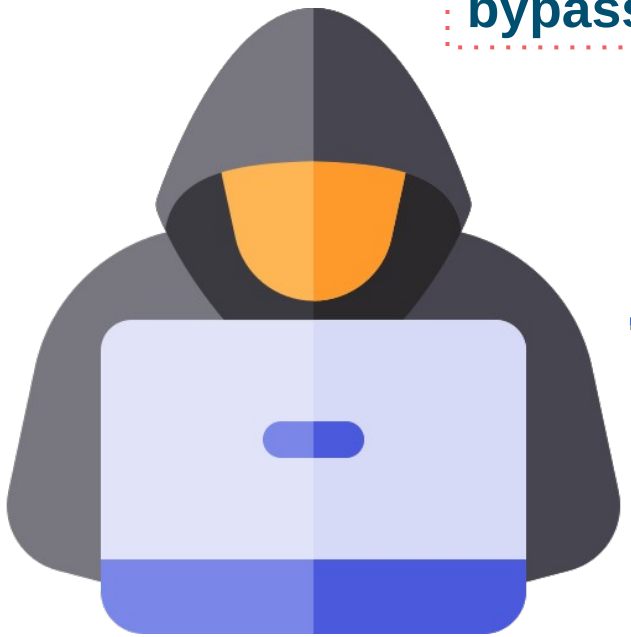


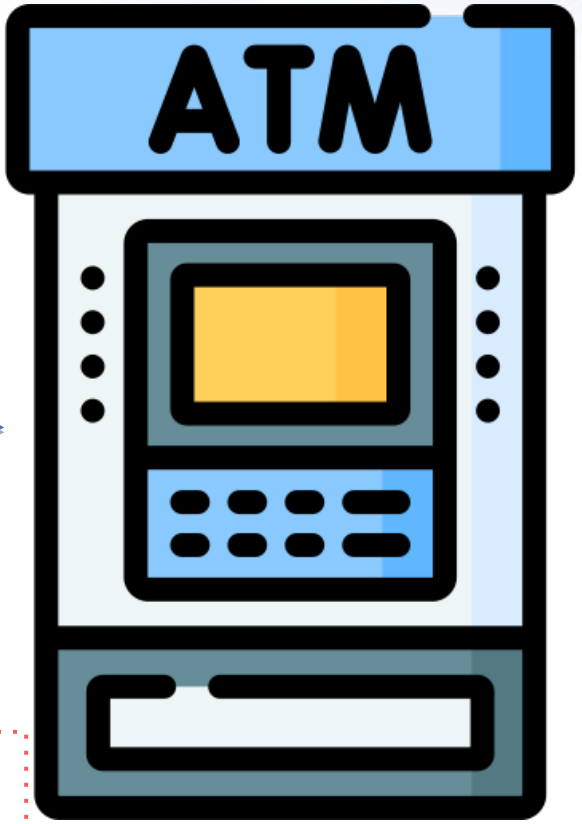


2. The malware is tested and tuned by connecting to the ATM in broad daylight several times.

What happened?

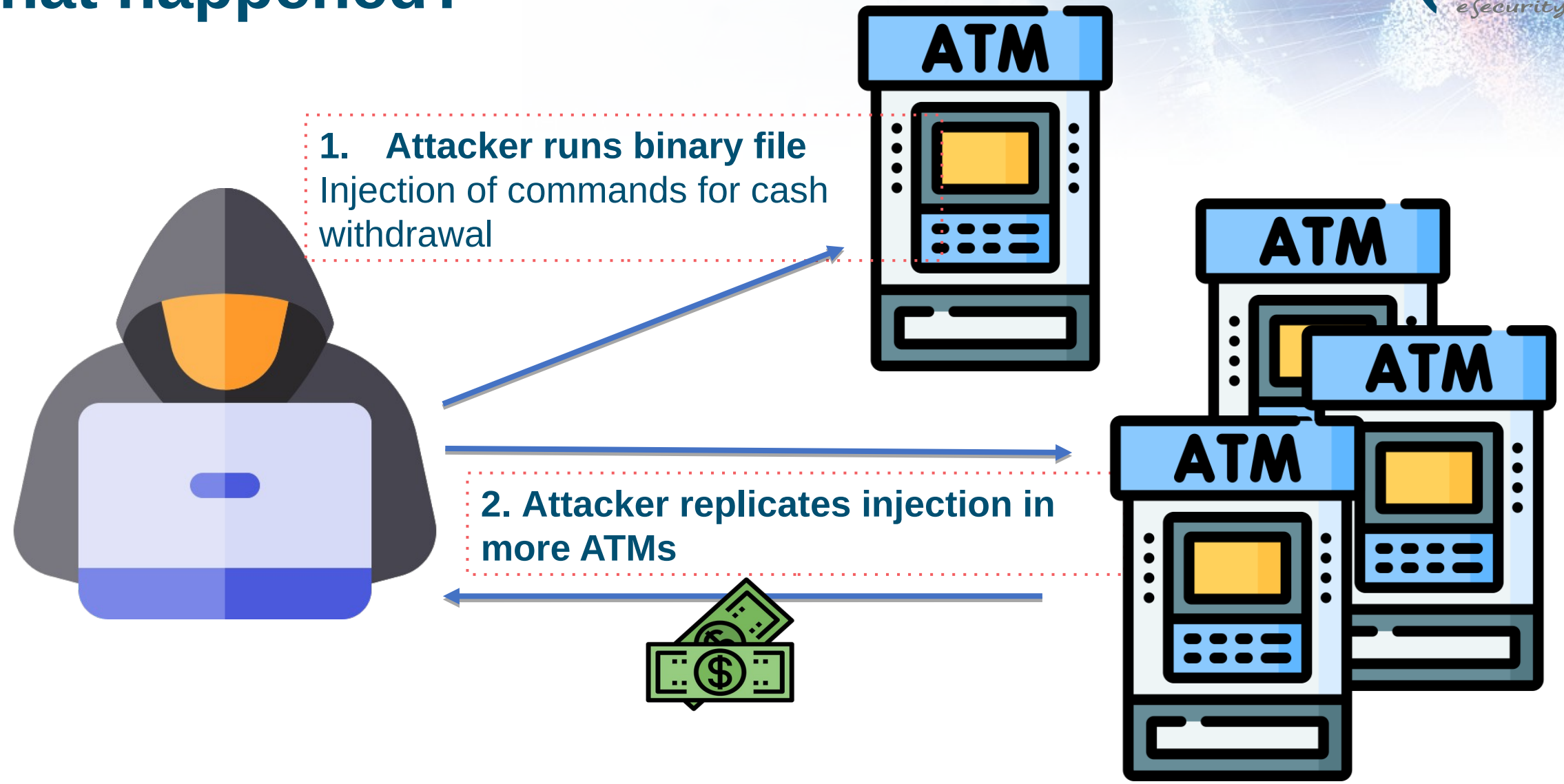
1. Attacker discovers ATM restrictions and how to bypass them



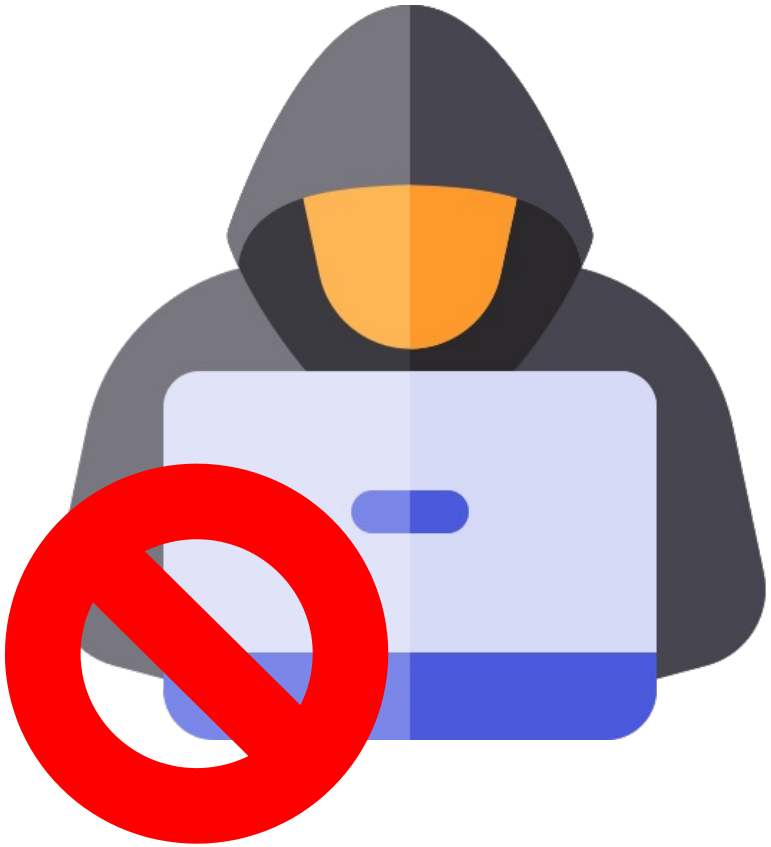


2. In order to run the binary file, the attacker includes it in the antivirus whitelist

What happened?



To be improved

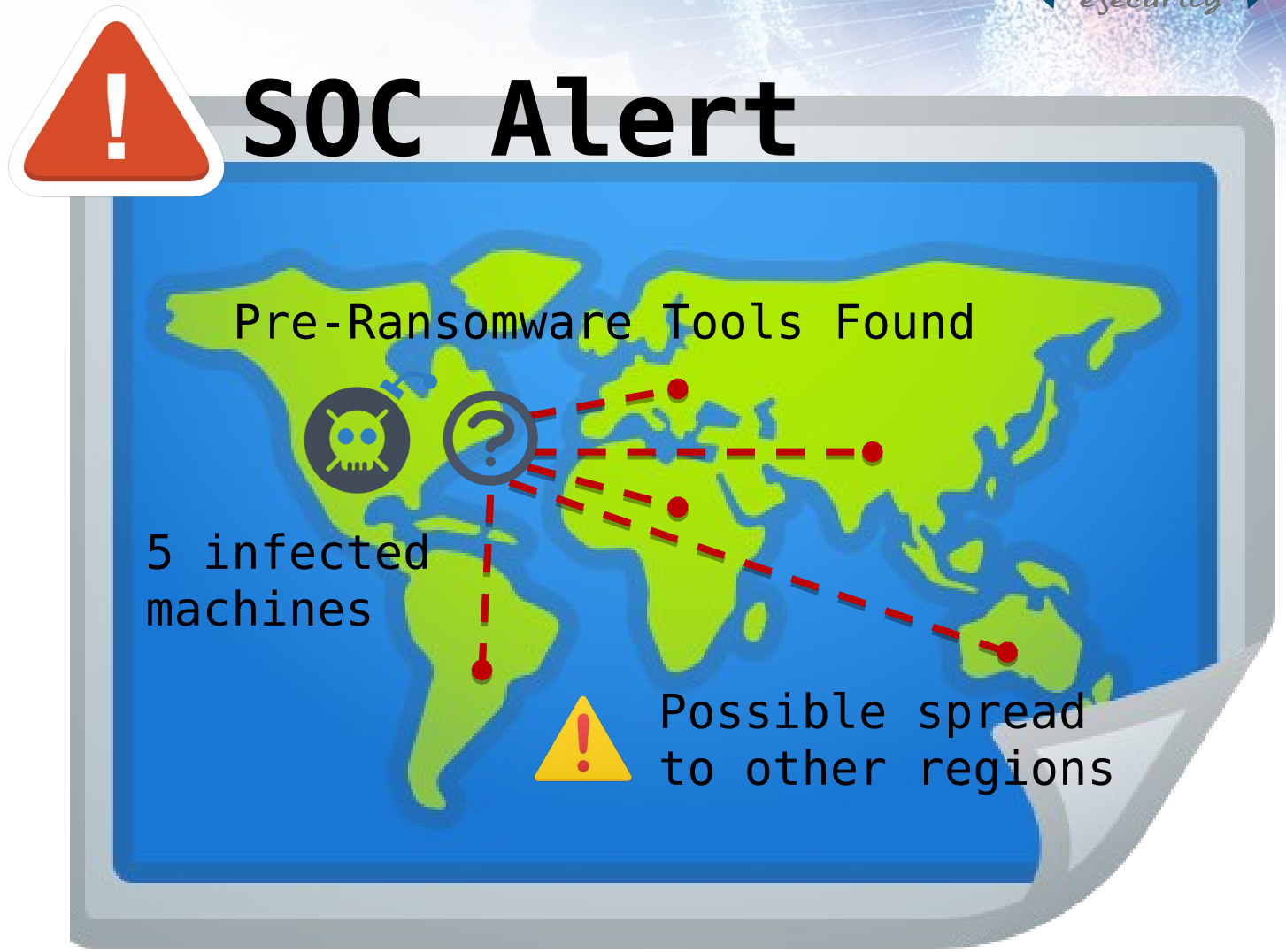


- Continuous software update.
- Vulnerability detection.
- Internet download control.
- Exhaustive control of access and management.
- Control of users and privileges.
- Monitoring and tracking.
- Reinforcement of physical surveillance of facilities.
- Monitoring and alert systems.

Ransomware case: APT Attack

What happened?

- Global company on 5 continents
- Regional headquarters:
  - London / NY / Sydney
- US based SOC
- One eSecurity provides:
  - Threat Hunting Services in EMEA and LATAM
  - DFIR Retainer



What happened?

Attack scope

United States

Risk of global spread

Servers	5,000
DC	350
Workstations/laptops	12,000

What happened?

Day 1

Ransomware deployment is **imminent**

Aggressive measures to prevent massive encryption

Goals

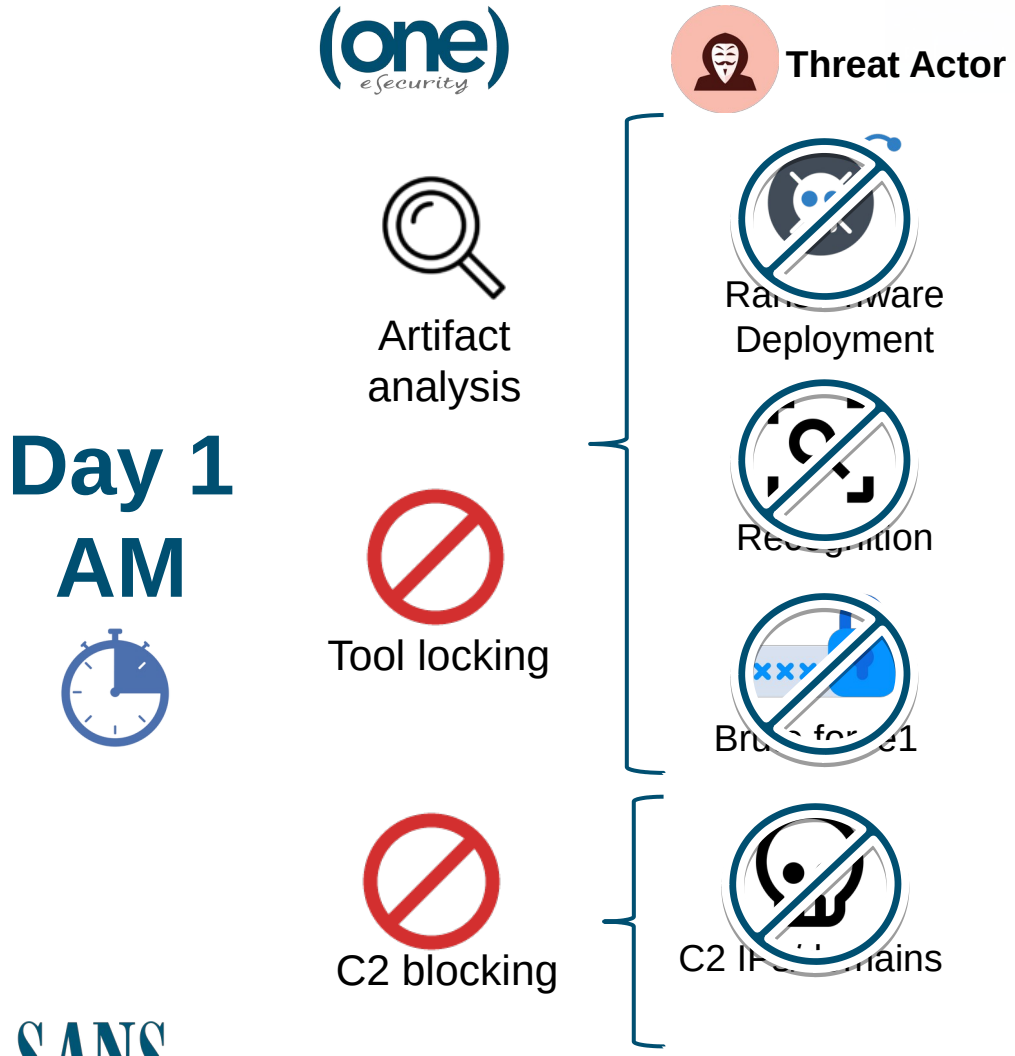
Containment

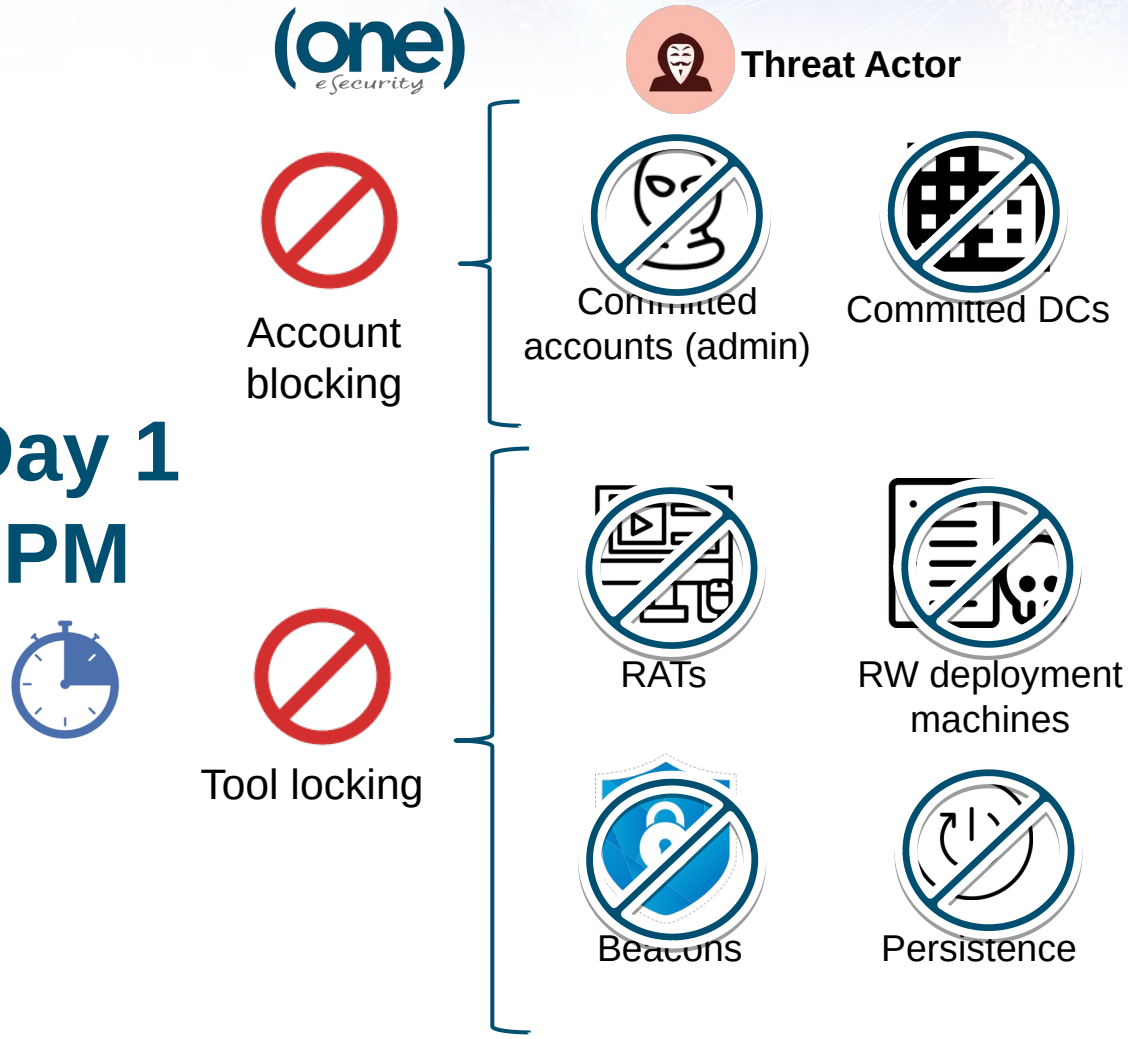
- Backups protection
- Network isolation
- DCs disconnection
- SOC high alert
- C-level support
- Business impact

Tarpitting

- Disabling compromised accounts
- Massive change of credentials
- Blocking malicious IPs/domains
- Firewalls/Proxies deployment
- Limit input options
- AV upgrade

What happened?





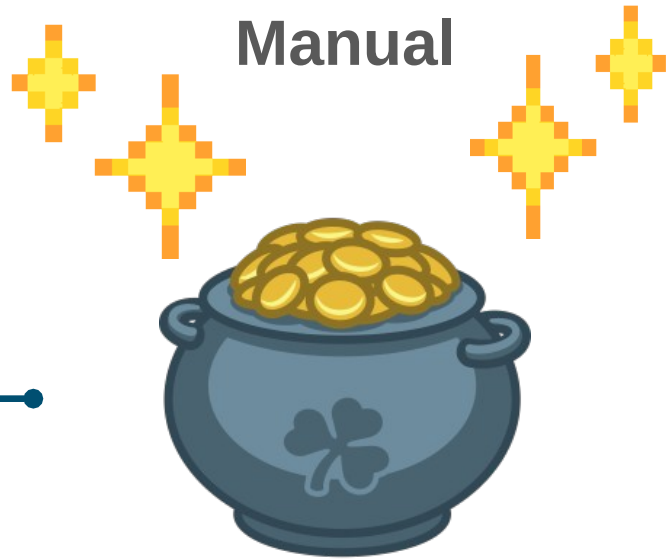
What happened?

Day 1 - PM

The actor is identified:

CONTI

CONTI Filtered Manual



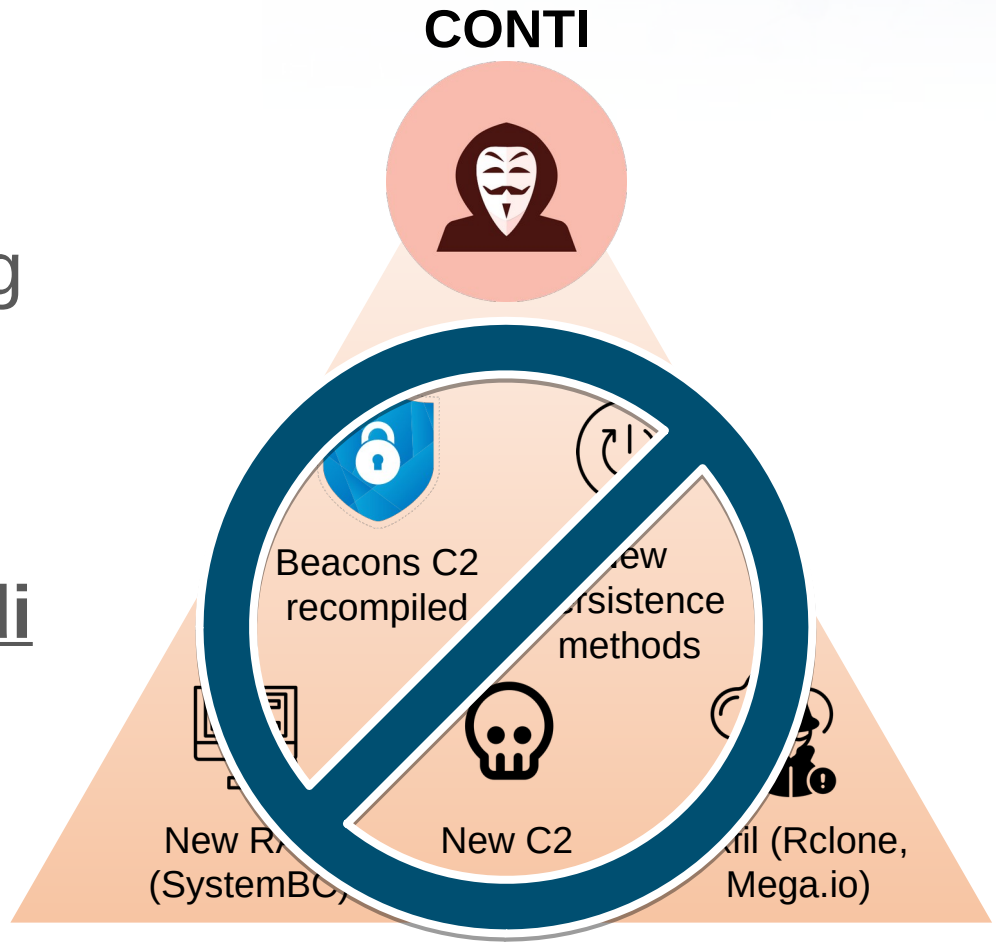
- Russian Actor
- **TOP Threat Actor**
- **Ransomware as a Service (RaaS)**
- Specialized in double extortion (Data Theft + Ransomware)

What happened?

Day 2

The attacker knows he's being restrained

<u>Changes his modus operandi</u>



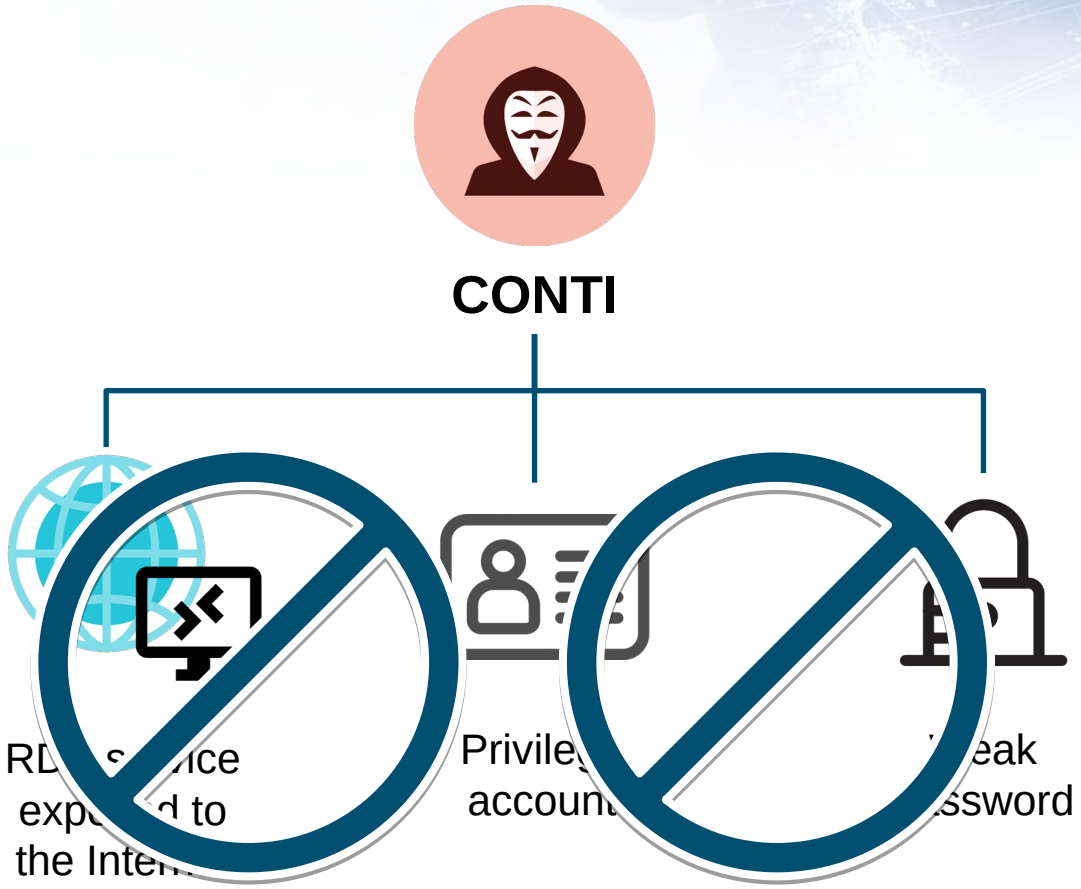
What happened?

Day 3

Entry point confirmed

Continued blocking of IOCs

Last day of actor activity



What happened?

Next 4 weeks

Committed DCs

Possibility to return

Next victim!

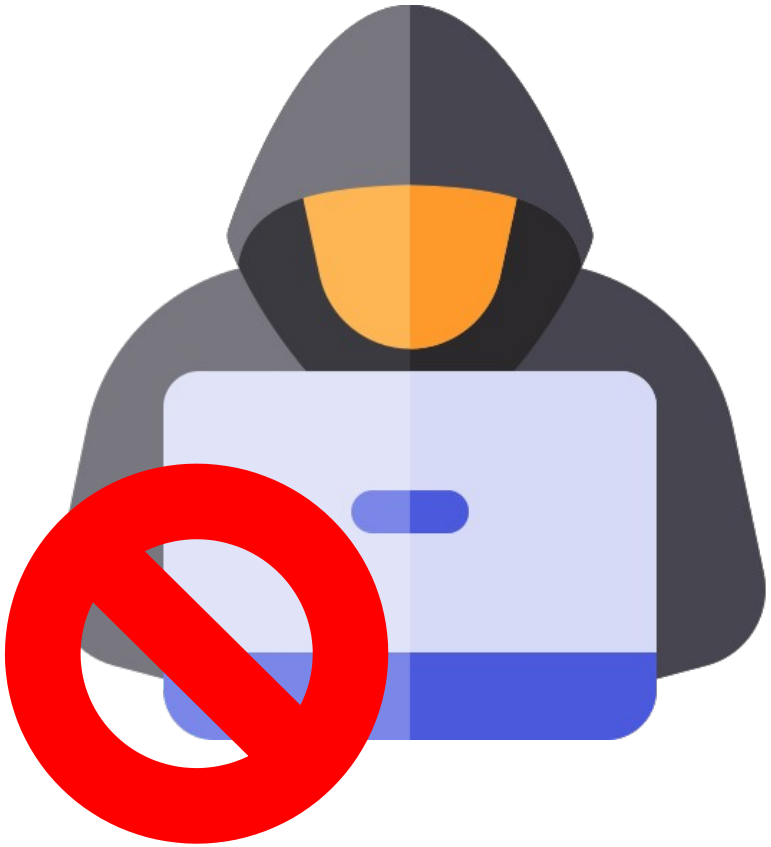
Continuous TH cycle 24x7

Cleanup and recovery continues

Security improvements

Make attacker's life a misery

To be improved



- Securing exposed/vulnerable remote access/VPNs
- Network segmentation
- Robust credential management
- Optimization of monitoring capabilities
- Security awareness
- Use of Cyber Intelligence
- Threat Hunting Service

Success Factors: Roadmap to Maturity

Objectives

- **Fast Detection**
- **Effective Response**

- **Preparation**

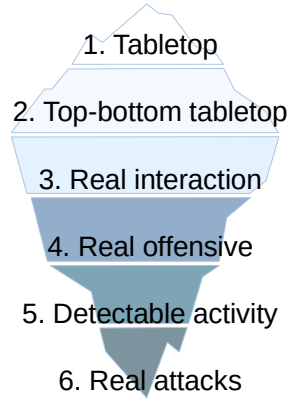
How Can We Help?

Roadmap to Detection & Response Maturity

Detection & Response Maturity

Depth

Incident Response RETAINER

Technology	People &Talent	Monitoring	Proactive Detection & Response	DFIR Assessment + Cyber Threat Intelligence	Cyber Exercises	Purple Team
SIEM	Talent Recruitment	SOC	Compromise Assessment (CA)	Threat Landscape (TL)	Workshops	Adversary Emulation (AE)
EDR	Training & Knowledge Management (KM): 1. Fundamentals 2. Advanced	Correlation	Threat Hunting (TH): 1. Intelligence based 2. Hypothesis based 3. Anomaly based	Incident Response Plan (IRP)	Cyber Exercises:  	Deception
XDR	Knowledge Updates & Challenges	Use Cases	Managed Detection & Response (MDR)	Data Source Analysis (DSA)		
SOAR	Talent Retention Strategy	Cyber Threat Intelligence (CTI)		Playbooks		
		Artificial Intelligence (AI)		IRMM Gap Analysis		

How Can We Help?
Today

- **Rapid Advanced Detection**
  - **Managed Threat Hunting | Detection & Response**
  - **Our experts operate your tools**
- **Fast & Efficient Response**

- **Retainer**

How Can We Help?
Preparation

Retainer Contract

During “peace” time…

Compromise Assessment

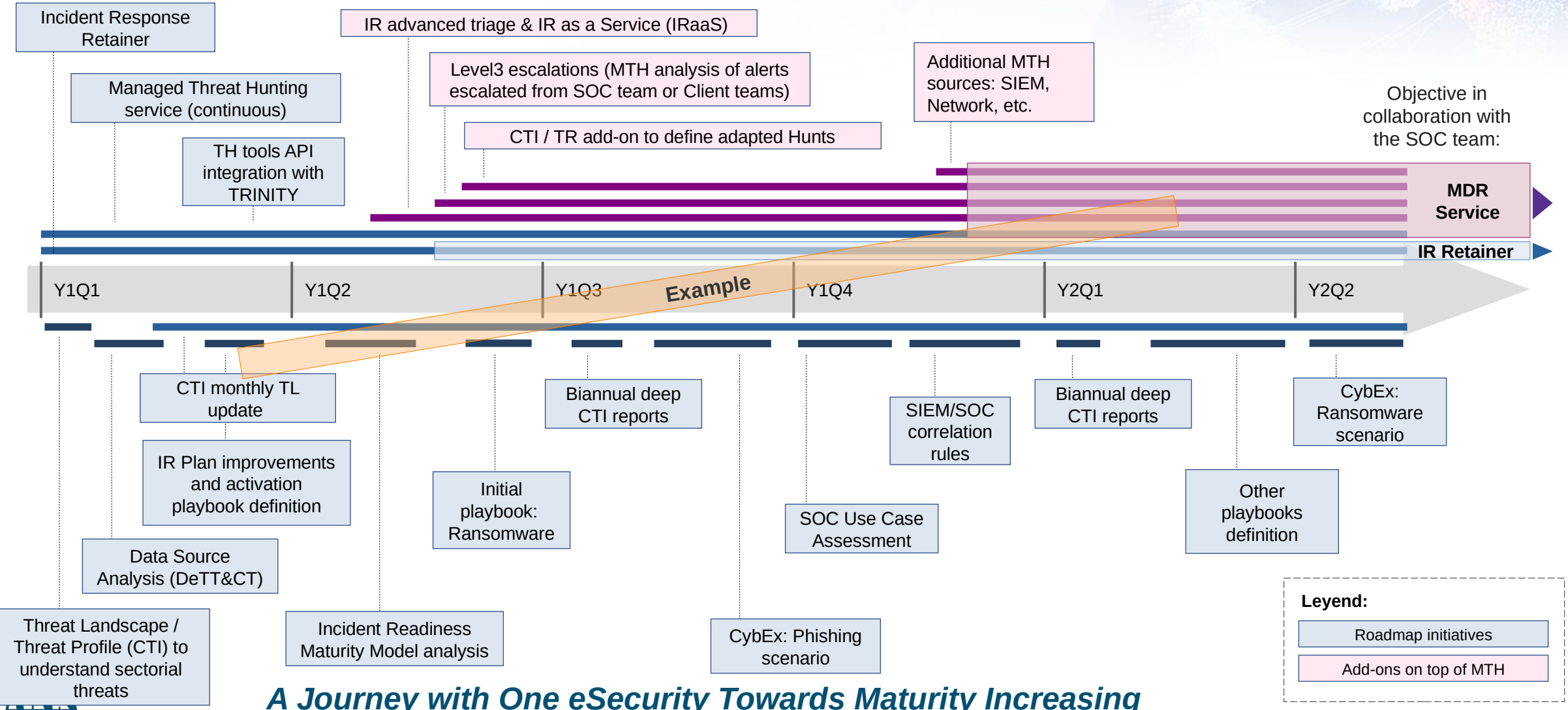
DFIR Consultancy (CyCons)

- Incident Readiness (IRMM)
- Incident Response Plan, playbooks and procedures
- Threat detection improvements
- Workshops of real cases

Cyber-exercises (CybEx)

CTI and Threat Research

How Can We Help?
Strategically



Upcoming Talks & Courses

- **SANS AI CyberSecurity Forum**
  - **April 26, 2024**

    https://www.sans.org/webcasts/sans-ai-cybersecurity-forum-insights-front-lines/

- **SANS FOR500 / FOR508**
  - **May 20-25 / May 27-Jun 1**

Thank you!

one-esecurity.com/events_training/2024/mte_eu_apac_apr24.html

Jess Garcia

@j3ssgarcia

jess.garcia@one-esecurity.com

Sales Inquiries

sales@one-esecurity.com

(one) eSecurity

www one-esecurity.com

One_eSecurity

One eSecurity