How hackers infiltrate critical infrastructures

Julien Oberson – 02.03.2023

SCRT
Information Security

Presentation

# Introduction

# Anatomy of an attack

# Critical infrastructure specificities

# Pentest methodology

# Demo

# Insomni’hack

# Question

Who am I?

- # Julien Oberson
  - # Graduate engineer from HEIA-FR
  - # Currently Head of Audit division @ SCRT
    - # Pentester since 2015
    - # Incident Response team member
    - # Windows security trainer
    - # Insomni’hack organizer
  - # Former experience in critical infrastructure
- # Contact
  - # www.linkedin.com/in/joberson
  - # julien.oberson@scrt.ch

Who is SCRT?

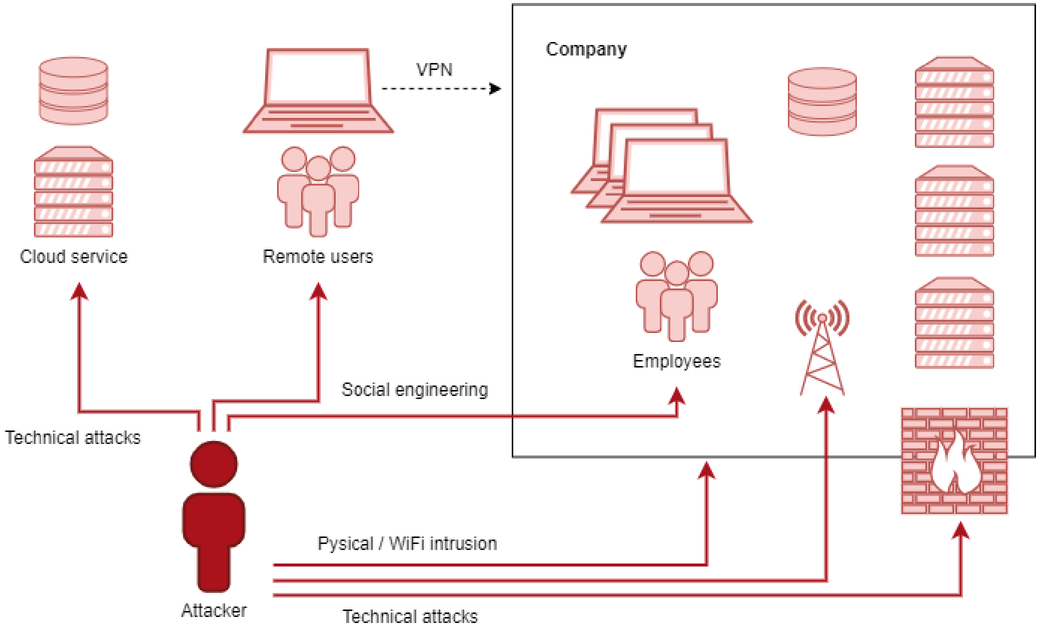
- Security company founded in 2002
- Based in Morges with branch offices in Bern and Geneva
- Employs 50+ security engineers in various departments
  - Pentest, Network, Analytics, System, Cloud, GRC
  - We are looking for talented engineers
- Acquired by Orange Cyber Defense in 2022
- Organizer of the Insomni'hack event
  - More information at the end ;-)

Anatomy of an attack

- Attackers want to earn money and tend to
  - Encrypt your data and ask for a ransom
  - Sell obtained access to other threat actors
  - Exfiltrate and sell corporate data on the black market
  - Tamper with financial information to divert bank wires
  - Use your infrastructure to attack others
  - … many other ways to steal your money
- When it comes to critical infrastructure
  - They attempt to disrupt service

Anatomy of an attack

# How attackers get access to your network?

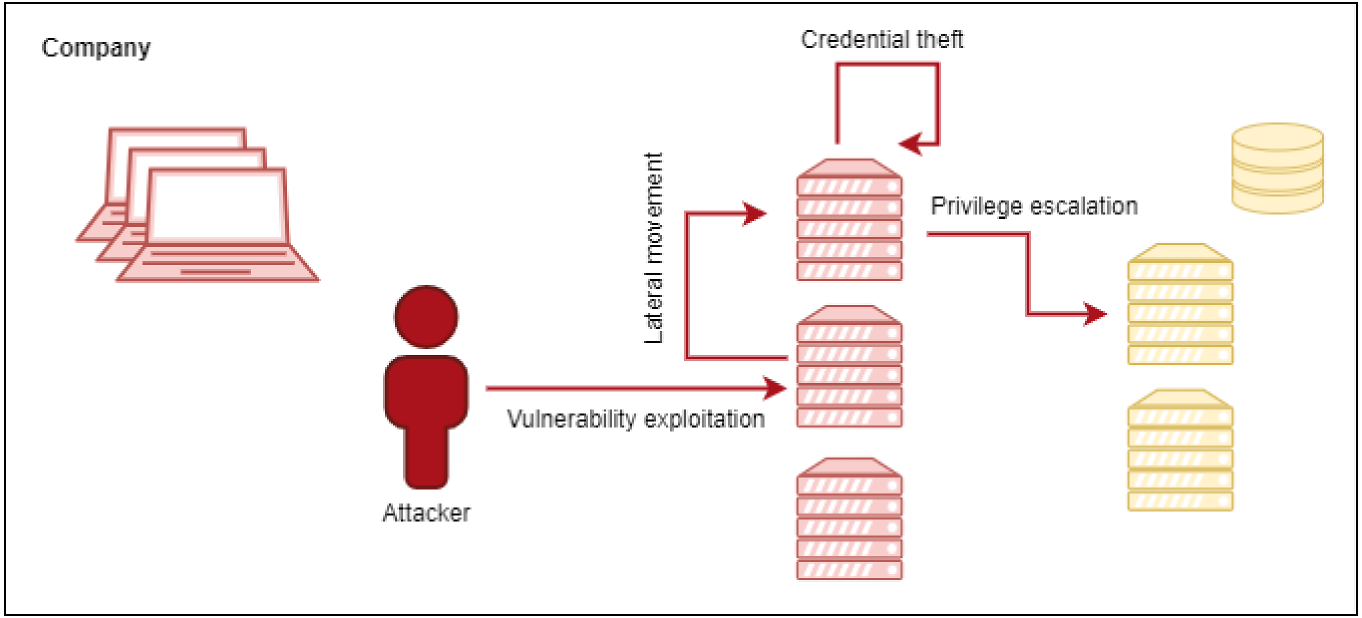


Anatomy of an attack

- Most companies rely on a Windows infrastructure
  - So no matter the final goal, internal attackers try to compromise domain administrator accounts
    - Especially since they are often excessively used
- To achieve their goal, they follow a common sequence
  1. Recon
  2. Vulnerability exploitation
  3. Privilege escalation
  4. Credential theft
  5. Lateral movements
  6. Persistence and/or ransomware deployment

Anatomy of an attack

# Typical internal privilege escalation until reaching target



Critical infrastructures

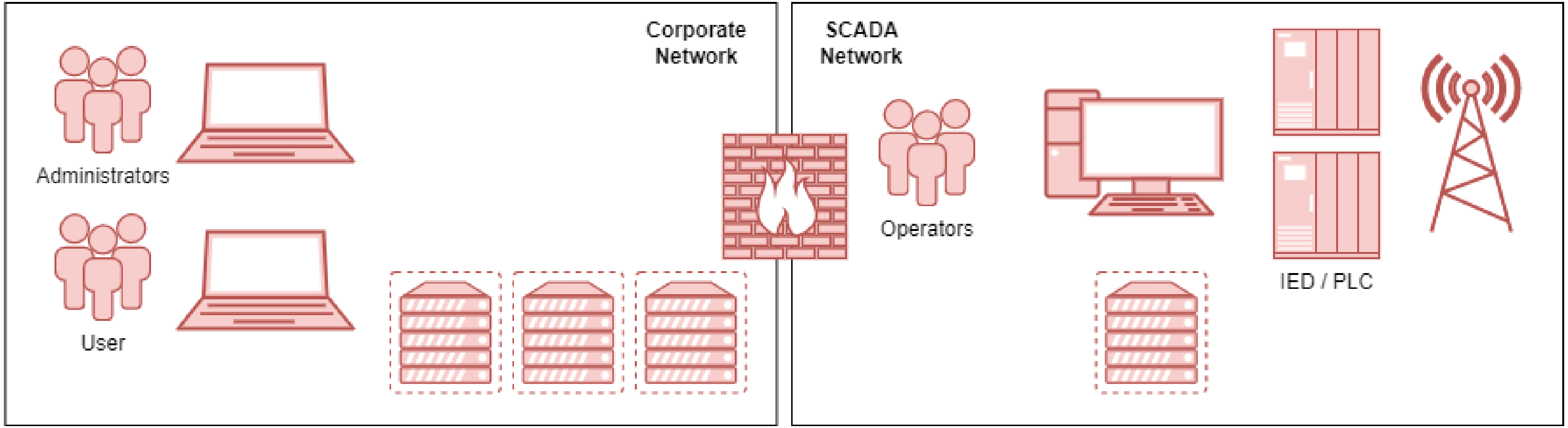
- What about critical infrastructures?
  - On top of being subject to common security flaws
  - SCADA systems themselves are notoriously prone to unsophisticated weaknesses
    - Including memory corruption, default passwords, weak crypto but also the lack of authentication and encryption
  - Companies are generally reluctant about applying updates or adding security layers on production devices

Critical infrastructures

- If not properly segregated, internal attackers can compromise SCADA equipment directly
  - Because of that, the most common mitigation consists in isolating SCADA devices on dedicated networks
- In practice, these networks are rarely air-gaped
  - Statistics have to be extracted for billing purposes
  - Communicating with ICS partners is often mandatory
  - Smart grid requires interactions with customers
  - Device vendors have to perform maintenance
  - …

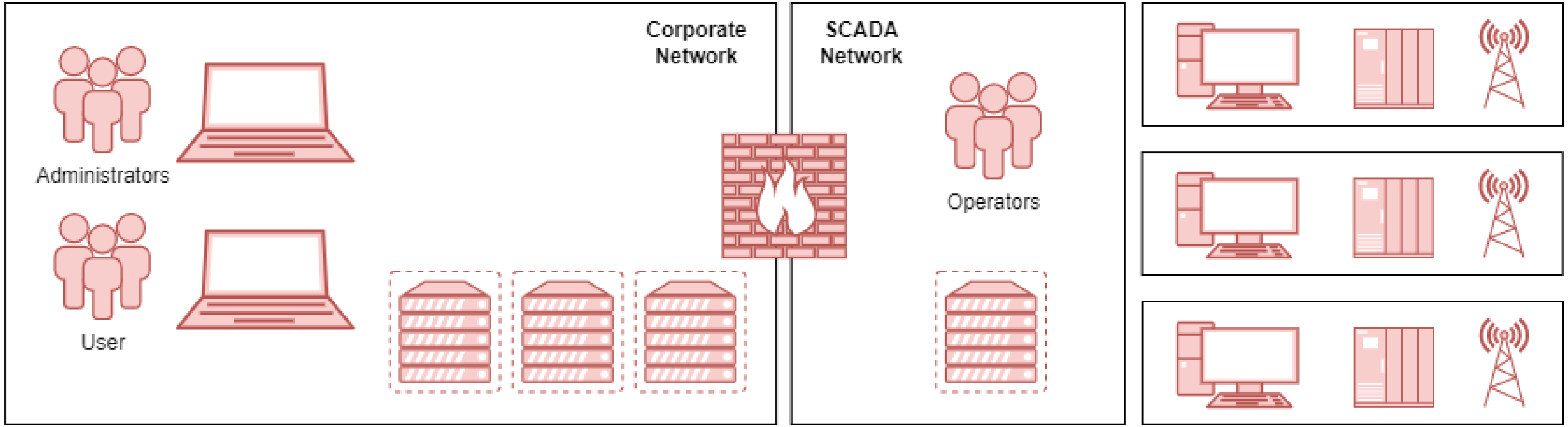
Critical infrastructures

- So corporate and SCADA networks are connected
  - But a firewall restricts network traffic
    - The filtering policy has to be strong to prevent breaches
  - If SCADA relies on Windows, domains should be segregated



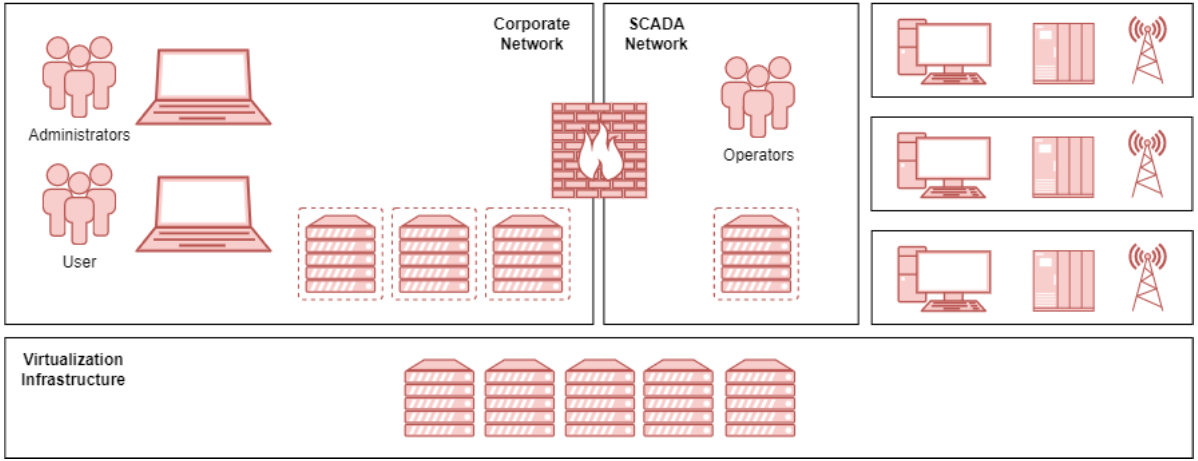
Critical infrastructures

- # SCADA networks can be spread over numerous locations
  - # With heterogenous physical protections
  - # Some «locations» might be protected with a simple lock
    - # Thus allowing to easily gain access to the network



Critical infrastructures

- Even when the network is properly filtered there might be some interdependence between infrastructure components
  - The virtual / storage infrastructure can be shared
  - Network devices are generally managed from the corporate side



Critical infrastructures

- # Considering that, an attacker can
  - # Try to access the SCADA network directly by taking advantage of weak physical protections
  - # Compromise the corporate network and
    - # Disrupt corporate-side services on which the business relies on
    - # Exploit filtering policy issues to access vulnerable SCADA devices
    - # Compromise a network admin to tamper with the filtering policy
    - # Compromise the virtualization infrastructure to jump on SCADA

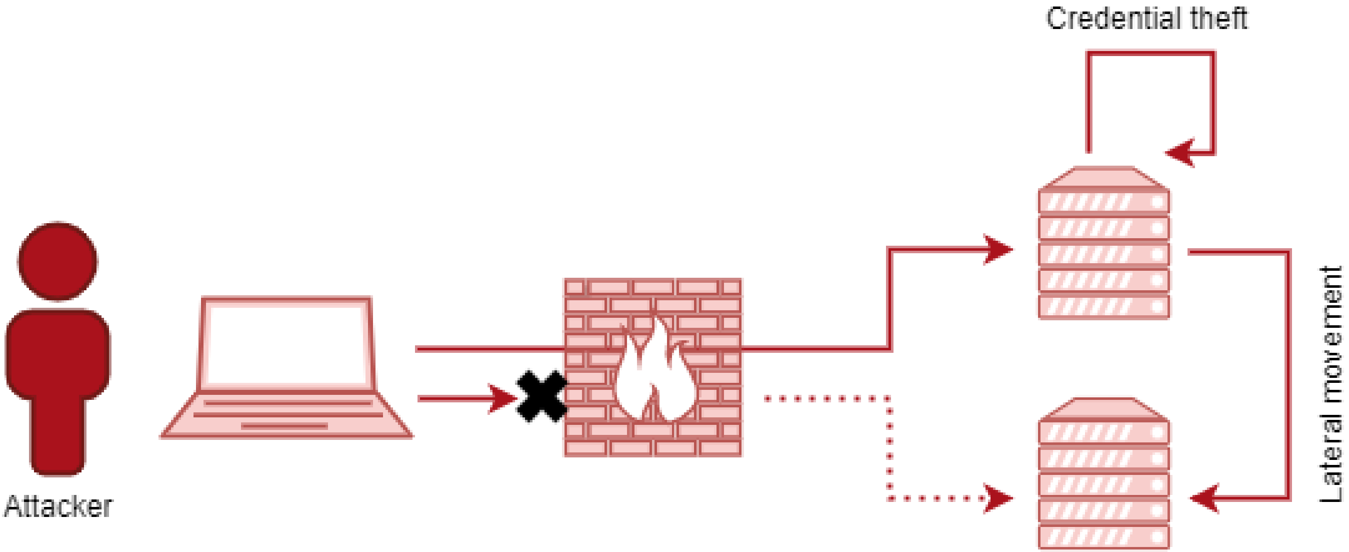
Pentest Methodology

- A pentest aims at simulating an attacker’s behaviour and is therefore based on the typical attack steps
- Multiple pentest types can be used to assess various parts of the information system
  - Application pentest
  - External pentest
  - Internal pentest
  - Social engineering
  - Physical intrusion
  - Red Team / Purple Team
  - …

Internal pentest

- Internal pentests typically simulate the previous steps
  - It assumes a physical breach or workstation infection and evaluates internal attack paths
- They make it possible to identify
  - Weak filtering policies
  - Update management issues
  - Password misconfigurations and weaknesses
  - Active Directory configuration issues
  - Presence of legacy protocols
  - Improper use of privilege accounts
  - … and many more

Demo time!



What is insomni'hack?

# Security conference including

  # Workshops

  # Conferences

  # Capture the flag (CTF)

# Hosted in Lausanne (EPFL)

  # SwissTech Convention Center

# Next edition on March 20th to 24th

  # More information on: www.insomnihack.ch

# Dedicated CTF ranking for academic related team

Questions?