BUSINESS CASE

Attack At Home attack surface

ICIL4.0 WP3 BC

howest
university of applied sciences

UNIVERSITEIT GENT
CAMPUS KORTRIJK

TABLE OF CONTENTS

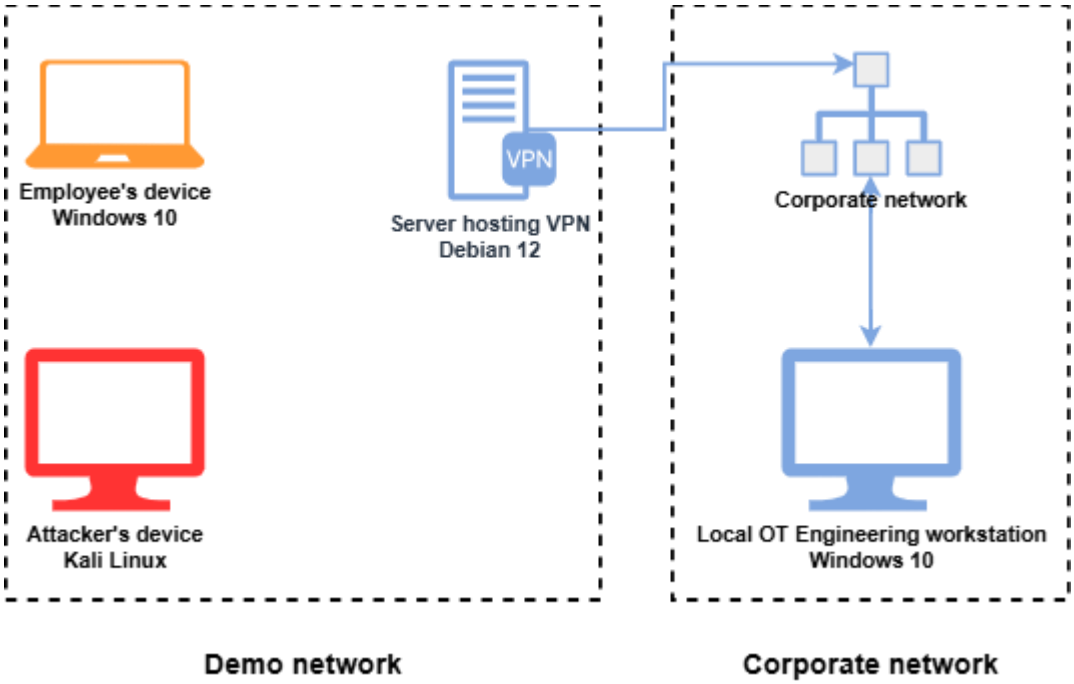
INTRODUCTION

The rapid shift to remote work during the COVID-19 pandemic reshaped the way organization's function. For many employees, working from home brought convenience: reduced commuting time and increased flexibility. Yet this change also expanded the attack surface for malicious actors. Devices that once operated within secure corporate boundaries are now placed in home environments, often less controlled and more exposed.

This raises an important question: **what are the potential consequences if an attacker compromises an employee's personal device used for remote work?**

To investigate this risk, we designed and executed a controlled demonstration. The goal was to trace a realistic intrusion path from a compromised home device to sensitive assets inside a corporate operational technology (OT) environment.

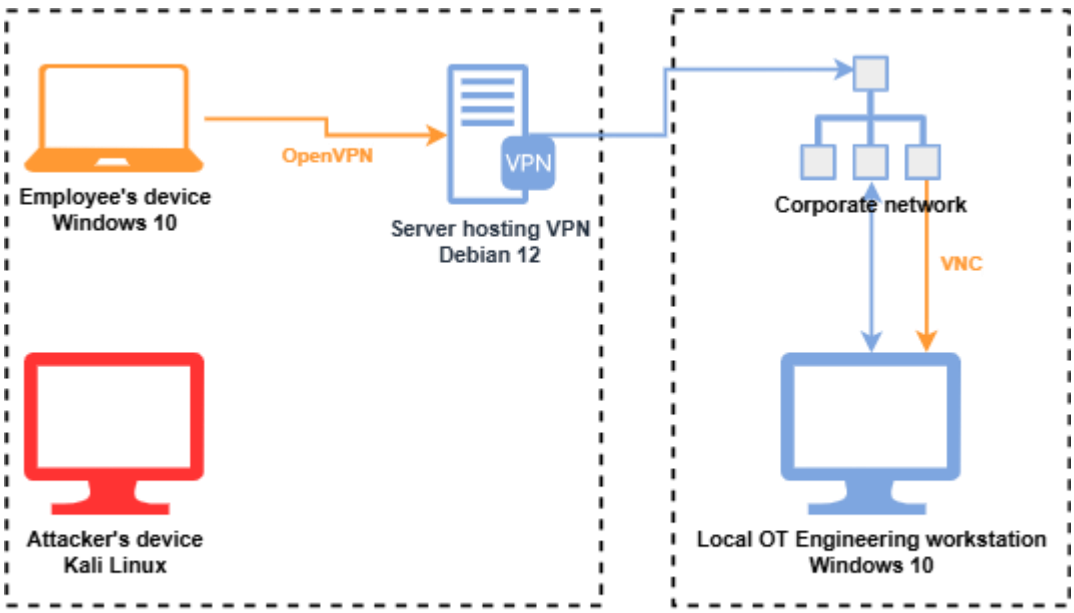
The Setup



The demonstration was implemented using virtual machines, hosted on an Intel NUC device. The environment consisted of several interconnected elements designed to mirror a remote-work configuration:

- **Demo network**: A host-only network segment with no internet access. It contained 2 devices:
  - The employee's workstation (Windows 10)
  - The attacker's machine (Kali Linux)
- **VPN Server (Debian 12)**: Equipped with 2 network adapters. 1 interface was connected to the demo network, while the other bridged into the **Fictile Network**, which represents the real corporate IT/OT environment. This server was configured to issue IP addresses within the Fictile Network to authenticated clients.
- **Local OT Engineering Workstation (Windows 10)**: An engineering machine inside the Fictile Network, accessible over VNC. In practice, this is where OT engineers carry out remote tasks on operational systems.

In this setup, the employee device connected to the OpenVPN server, thereby gaining access to the Fictile Network. From there, the employee could launch a VNC session into the OT Engineering Workstation. This arrangement created a realistic environment for examining the impact of a home-device compromise.


Employee's device
Windows 10
OpenVPN
VPN
Server hosting VPN
Debian 12
Corporate network
VNC
Attacker's device
Kali Linux
Local OT Engineering workstation
Windows 10
Demo network
Corporate network

The attack

Phase 1: Initial Payload

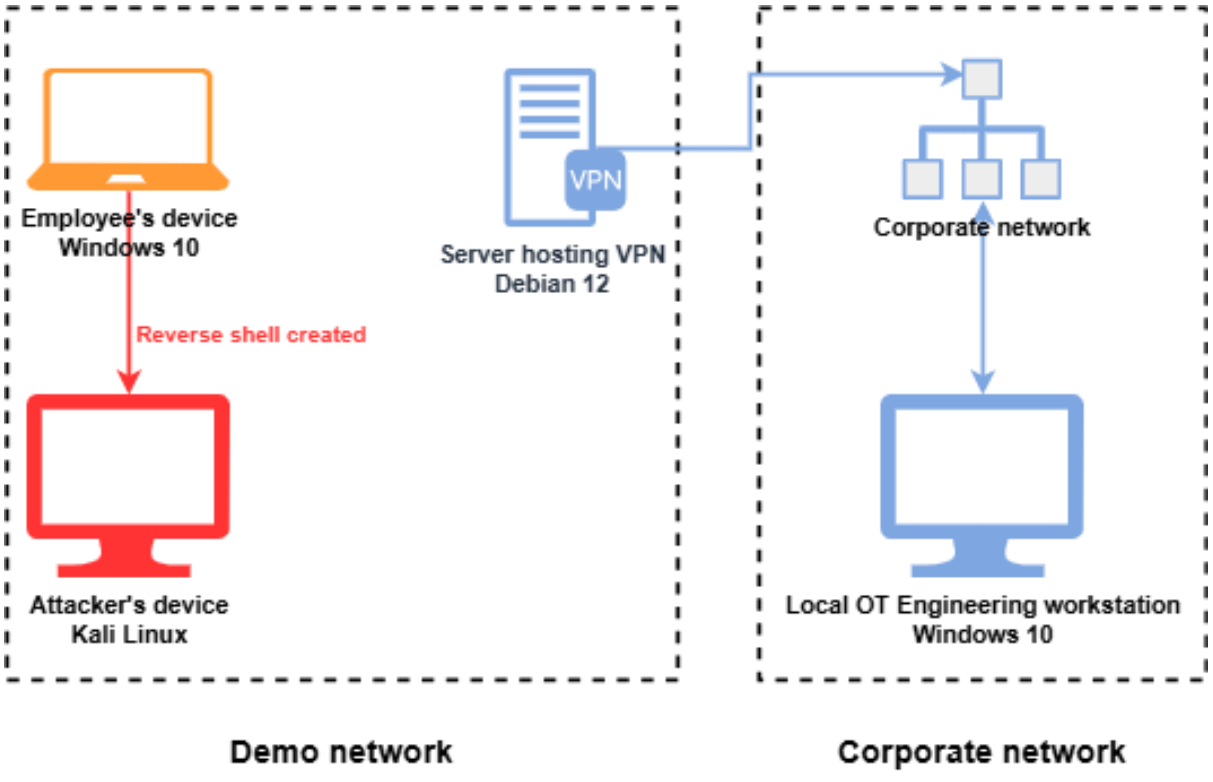
The intrusion began with a phishing attempt against the employee, referred to here as *John*. The attacker delivered a malicious file named Contract.pdf.lnk, which appeared to be a normal PDF due to hidden file extensions in Windows. The file was further disguised with an icon that could be considered a PDF.

Believing it to be legitimate, John double-clicked the file. Behind the scenes, several command prompts flashed briefly, the file removed itself, and the system restarted. This behavior indicated that the initial payload had been executed successfully.

Phase 2.1: Establishing Reverse Shell Access

The payload included a persistence mechanism that registered an executable to run each time John logged in. After the restart, this executable opened a reverse shell, establishing a background connection to the attacker's device.

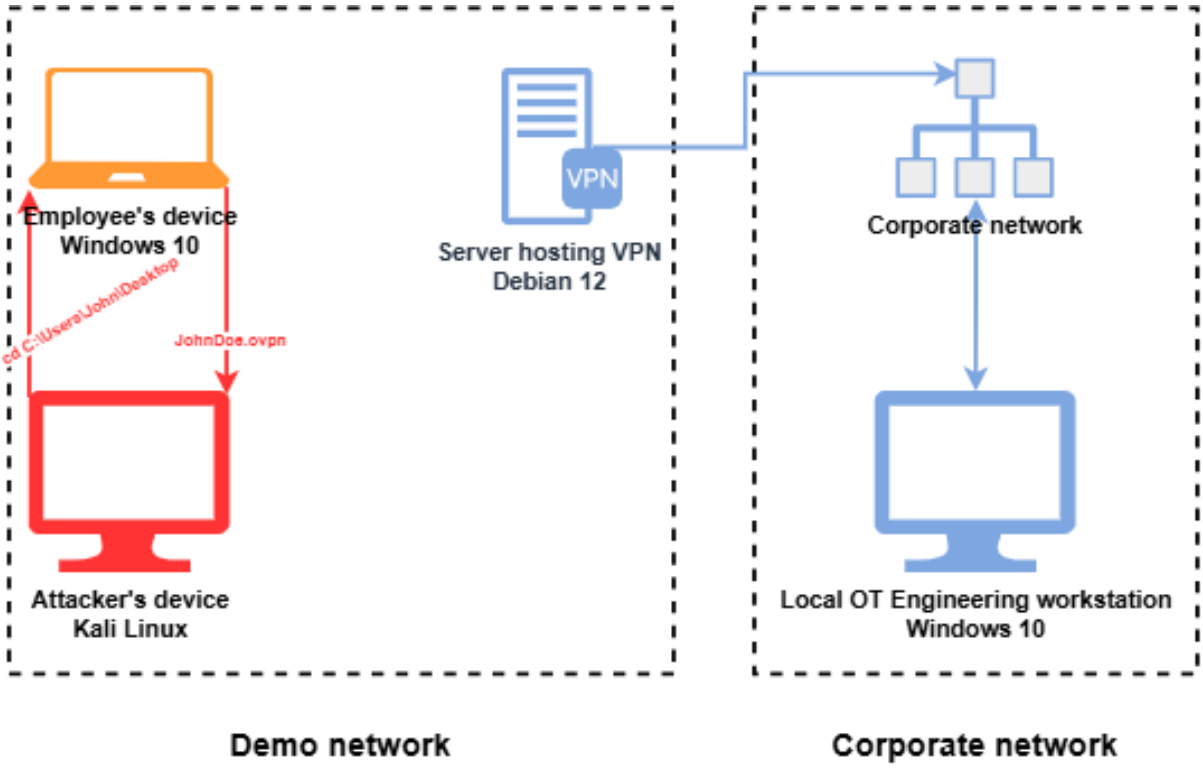
At this point, the adversary obtained full command-line access to John's system, with the ability to issue commands covertly and maintain control as long as the persistence mechanism remained active.



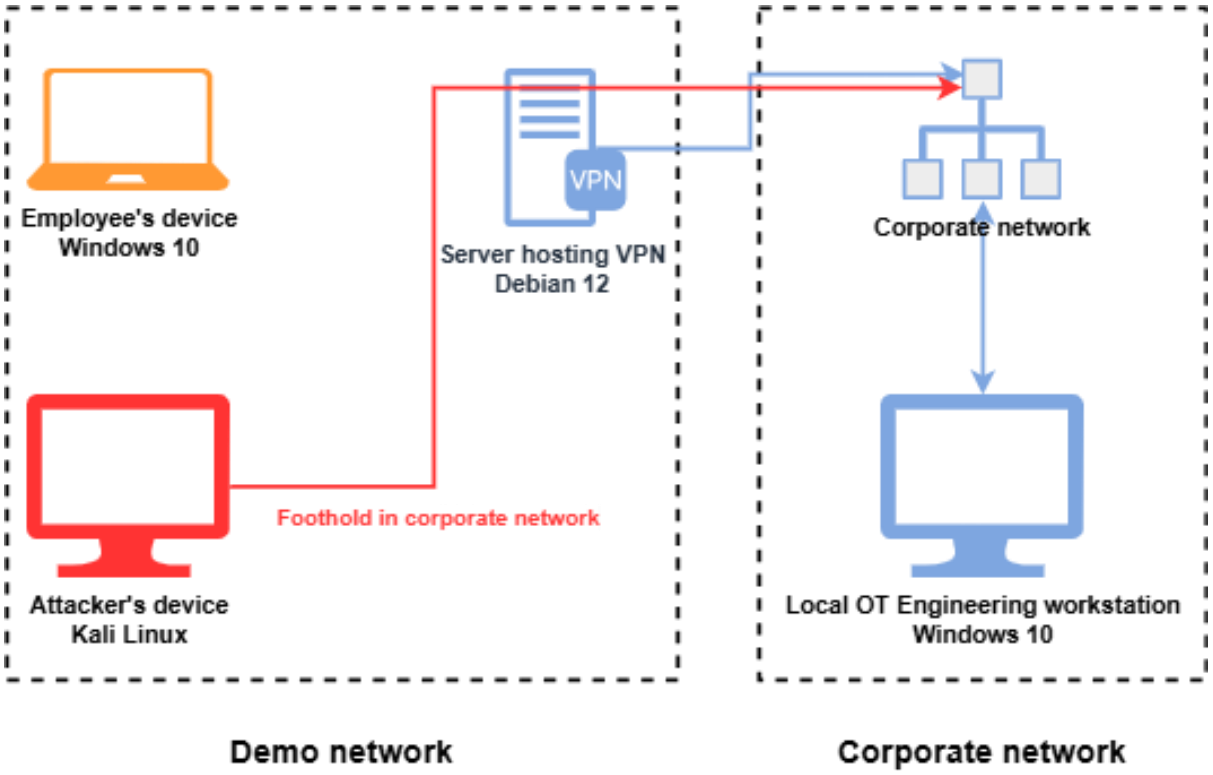
Phase 2.2: Compromising VPN Credentials

While exploring John's desktop, the attacker located 2 critical items:

1. **The OpenVPN profile file** (JohnDoe.ovpn)
2. **A confidential document** containing details about the Local OT Engineering Workstation, including its IP address, access method (VNC), and a note that the password was identical to John's personal device credentials.



The .ovpn profile also included a parameter auth-user-pass, pointing to a file where John's VPN credentials were stored in plaintext. This discovery gave the attacker all the information necessary to authenticate directly to the corporate VPN.



With these credentials, the adversary now had remote access to the Fictile Network. However, this access was limited to OSI Layer 3 and above, restricting low-level network reconnaissance. To overcome this, the attacker turned attention to the OT Engineering Workstation.

Phase 3: Escalating to OSI Layer 2 Access

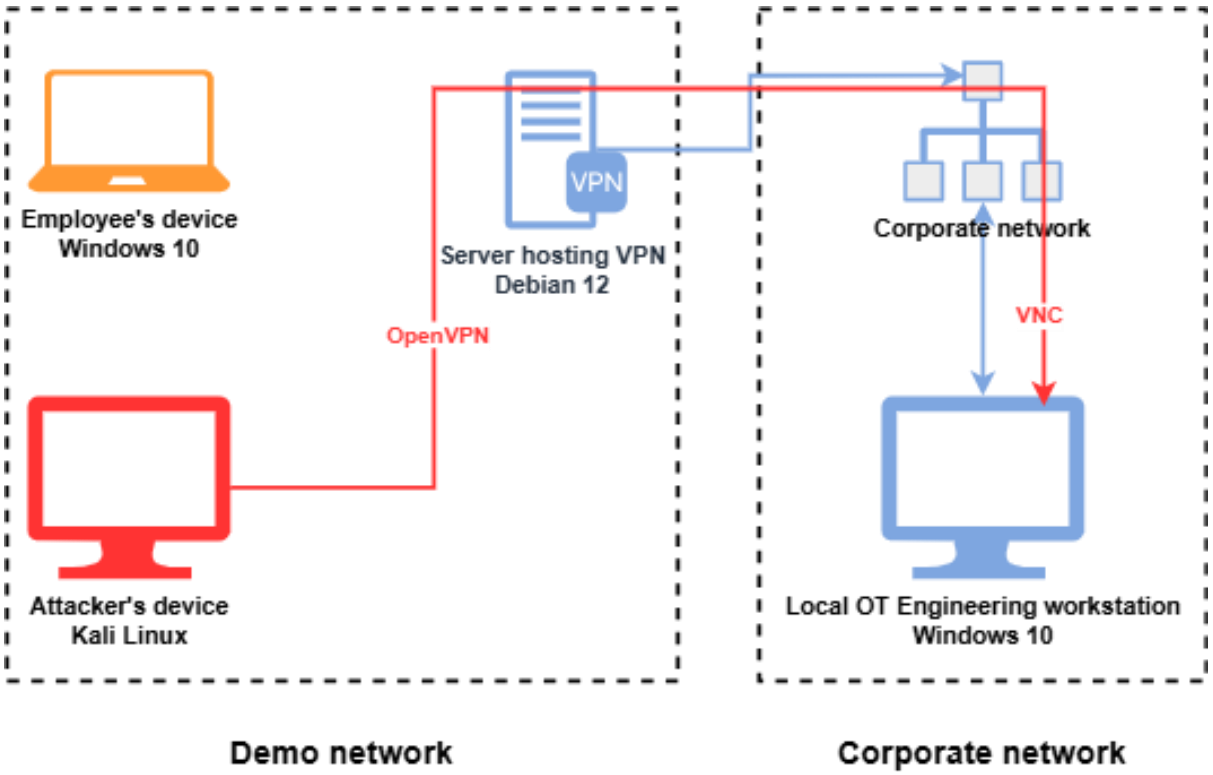
The attacker's next goal was to obtain credentials for the OT Engineering Workstation. Knowing that the password was identical to John's, the attacker sought to extract it directly. Using the elevated shell, the attacker deployed **Mimikatz**, a well-known credential extraction tool.

Because the initial payload had enabled WDigest credential caching, Mimikatz successfully retrieved John's plaintext login credentials.

At this stage, the attacker possessed:

- Valid OpenVPN credentials (allowing remote access to the Fictile Network)
- John's personal login password (which also unlocked VNC access to the OT workstation)

This combination granted the attacker a foothold at OSI Layer 2, enabling deeper interaction with OT systems.



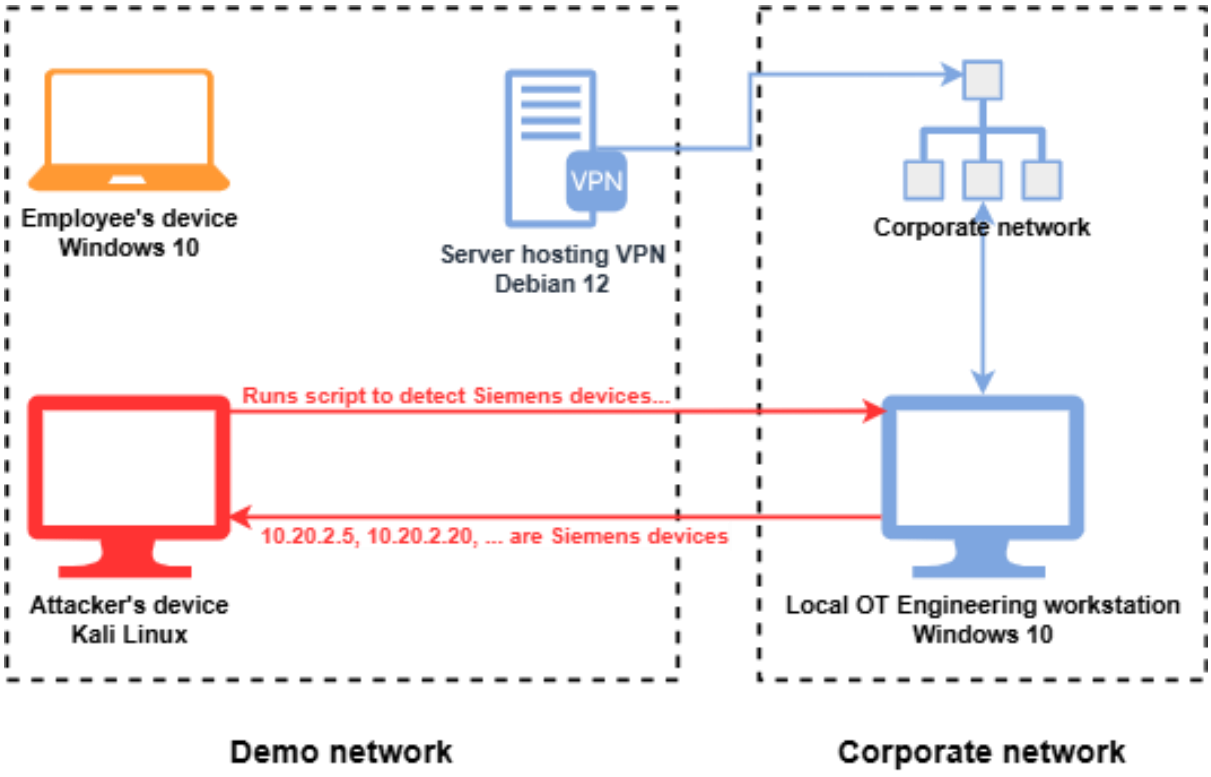
Phase 4: Surveillance and attack Execution

With full access secured, the attacker connected to the corporate VPN using John's stolen profile and credentials, then initiated a VNC session into the OT Engineering Workstation.

From this position, the attacker deployed a custom script to scan the internal network for Siemens industrial devices. The scan produced a list of reachable systems, confirming the ability to map and target OT assets.

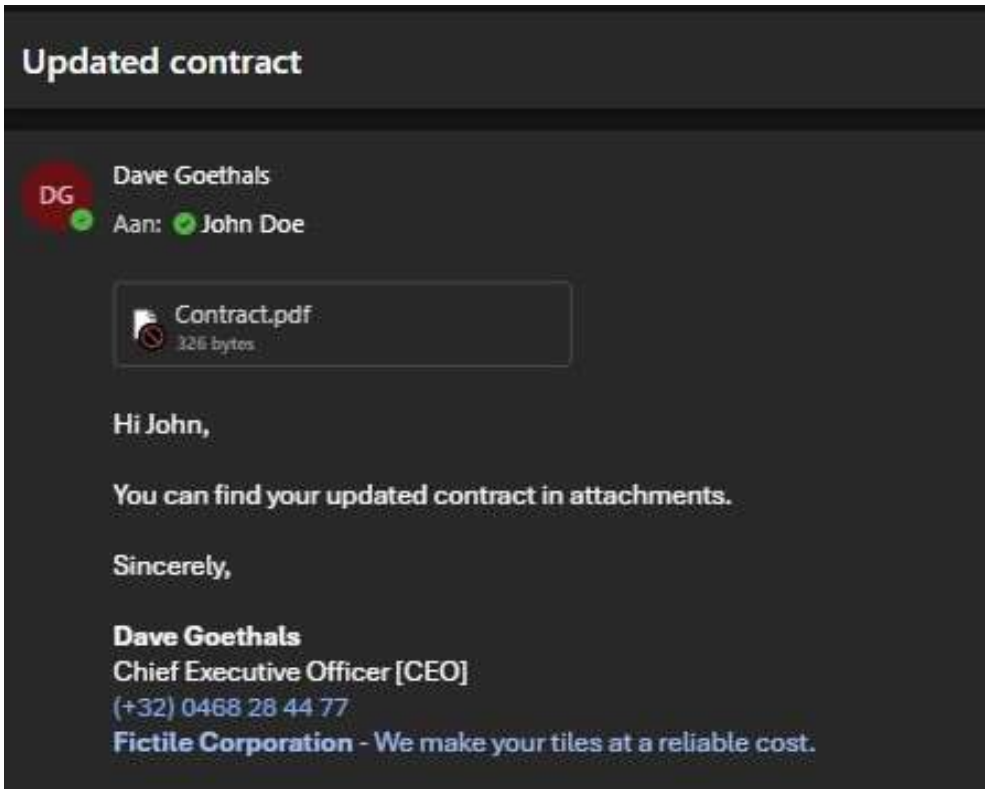
To demonstrate control, the attacker issued a command through the script that caused an indicator LED on 1 of the Siemens devices to blink. While this was a benign action, it symbolized the potential for far more disruptive or destructive activity.

The attack path was complete: starting from a phishing email, the adversary escalated to full access over critical operational devices.



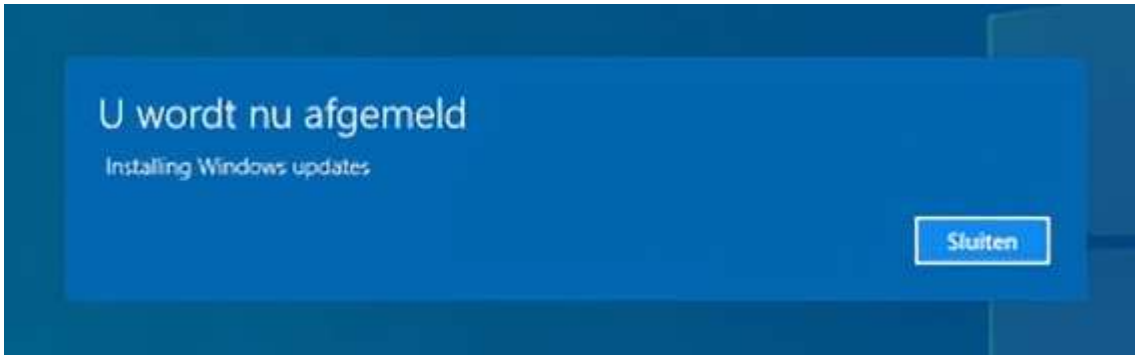
Showcase

John receives the email from a spoofed email address, impersonating Fictile's CEO, Dave Goethals.



On the attacker's machine, they start their scripts. All necessary files being copied to the webroot, and the Netcat listener is started.

John downloads the file to their desktop, and executes it.
Right after this, a computer restart is forced.



The malicious payload has done 2 things in the registry of John's Windows computer: it created persistence, making the reverse shell call out to the attacker's device each time John logs in. Besides that, it also activated WDigest logon-credentials caching.

As John logged in after the computer restarted, the reverse shell is ran by the persistence method, and the attacker is now inside John's device.

```
listening on [any] 4444 ...
connect to [192.168.72.201] from (UNKNOWN) [192.168.72.101] 65526
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. Alle rechten voorbehouden.

C:\Windows\system32>whoami
whoami
desktop-bhb6blg\john

C:\Windows\system32>
```

The attacker eventually finds John's desktop, and notices 2 critical files: his OpenVPN profile, and a confidential file containing information about the Local OT Engineering Workstation.

```
C:\Users\John\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1C40-0B37

 Directory of C:\Users\John\Desktop

30/09/2025  11:22    <DIR>          .
30/09/2025  11:22    <DIR>          ..
22/09/2025  10:29             6.259 JohnDoe.ovpn
29/09/2025  20:35               362 Local Workstation.txt
               2 File(s)          6.621 bytes
               2 Dir(s)  44.499.681.280 bytes free
```

```
C:\Users\John\Desktop>type "Local Workstation.txt"
type "Local Workstation.txt"
CONFIDENTIAL - For the intended employee only

Employee: John Doe
Role: OT Engineer

Local OT engineering workstation: 10.20.0.176
Connection method: TightVNC.
Password: The same password used for your login on your personal laptop.

Do NOT share this information externally.

IT/OT helpdesk contact: internal-support@fictilecorp.com
Date: 12/08/2025
```

After extracting the OpenVPN profile file to the attacker's own device, and checking the content, the parameter "auth-user-pass" is defined

```
auth-user-pass C:\\Users\\John\\.openvpn\\pass.txt
```

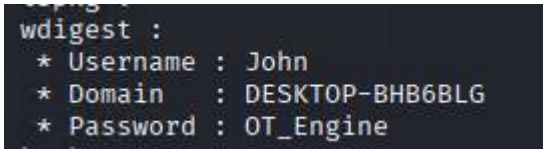
Getting the contents of the pass.txt file on John's device, the attacker obtains the plaintext credentials for John's VPN connection. The attacker now has an initial foothold into the company's network.

```
C:\Users\John\.openvpn>type pass.txt
type pass.txt
JohnDoe
J0hnDoe_ThePro
```

However, the VPN will limit the attacker to OSI Layer 3 and higher, and for a low-level network reconnaissance, you need to have OSI Layer 2 as well, so they decide to divert attention to the OT Engineering Workstation. After having checked the contents earlier, the attacker has the IP address, connection method (VNC), and information about the password: the password is the same as John's personal login on the compromised device. So now the attacker decides to extract John's password, which the payload's activation of WDigest credentials caching helps with. To do this, the attacker downloads Mimikatz, a well-known credential extracting tool, on John's device.

The attacker now runs the "Bluetooth driver" (renamed Mimikatz), and makes sure that privileges are escalated.

After verifying Mimikatz is running escalated, the attacker now uses it to drop all cached credentials. Thanks to WDigest, John's personal login is now given as well, including the password.

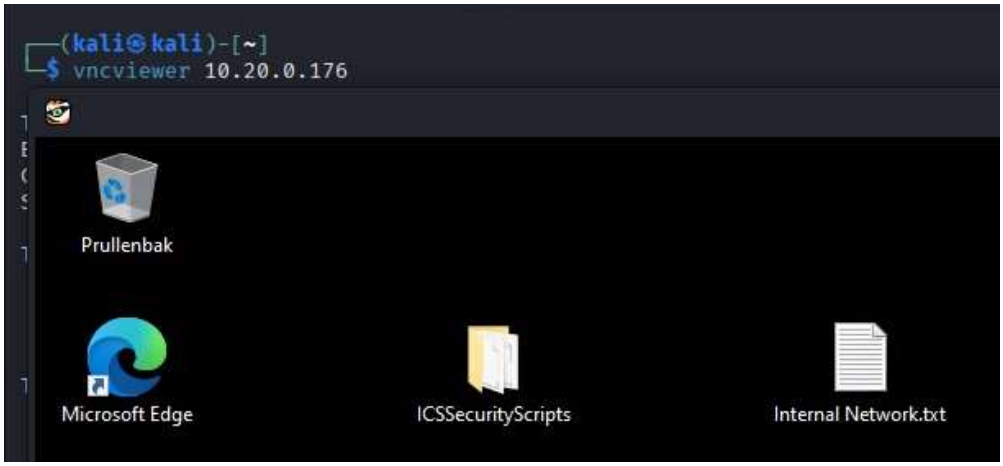


The attacker now has everything needed to start entering the company network on OSI Layer 2. He exits Mimikatz, deletes it from John's system, and exits the reverse shell, which also closes the executable on John's system, making it no longer appear in active processes list.

He connects to the OpenVPN using the extracted OpenVPN profile from John, and the stolen credentials, and is given an IP address inside the company network.

```
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1420 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.20.190.130/25 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::b3b2:a676:8829:9edb/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```

Now a VNC connection is established to the workstation IP address, using John's personal account password.



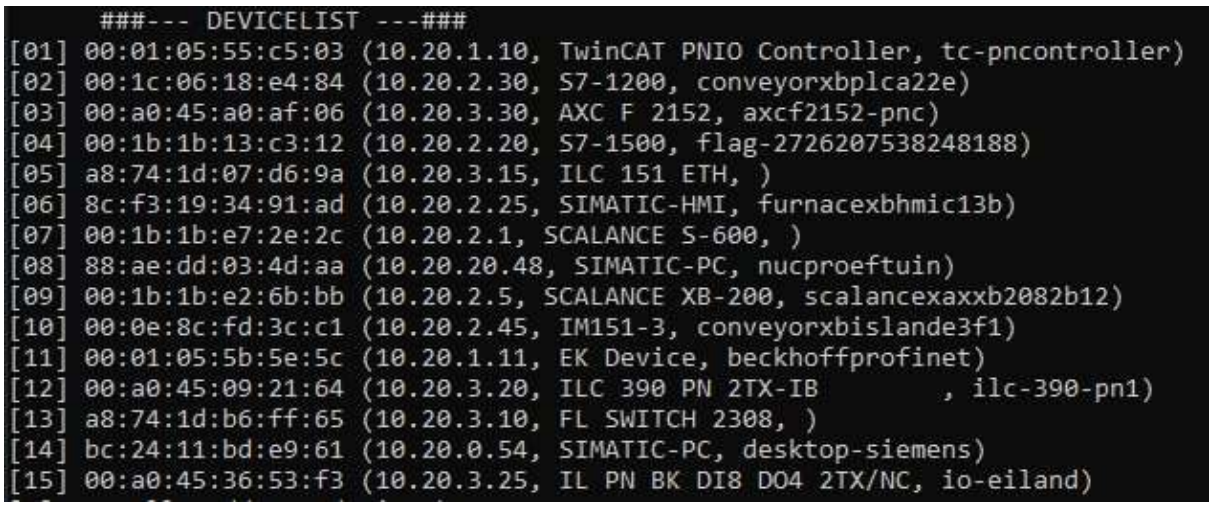
Clearly, the team did not expect a compromise of their workstation, as they have a file named "Internal Network.txt" on their desktop, with information about the network.

Internal Network.txt - Kladblok

Bestand Bewerken Opmaak Beeld Help

```
CONFIDENTIAL - This information is only for OT engineering personnel.

Internal Network: 10.20.0.0/16

Press (Beckhoff): 10.20.1.0-255
Oven (Siemens): 10.20.2.0-255
Painter (Phoenix Contact): 10.20.3.0-255

Do NOT share this information with non-OT engineering personnel.

IT/OT helpdesk contact: internal-support@fictilecorp.com
```

The attacker now runs a specific script on the OT engineering workstation, which first runs a discovery subscript, reporting a list of devices that responded from multiple vendors, including Beckhoff and Siemens.



The attacker now uses further capabilities of the script, making the physical LED blink successfully.
While this did not have any impact on the device, the small Python script has the capabilities to do other things, such as changing its outputs or CPU state, possibly disrupting production.

How to prevent this scenario from happening

The case study illustrated how a compromise that begins with a single employee device can cascade into unauthorized access to critical OT systems. Preventing such an outcome requires a **defense-in-depth strategy**, combining user education, endpoint protections, credential management, and network security.
Below, we outline key measures aligned with widely recognized cybersecurity frameworks.

1. User Awareness and Training

The attack was initiated through phishing, 1 of the most common and effective intrusion methods. To mitigate this vector:

- **Security Awareness Programs**: Employees should undergo continuous training on recognizing phishing attempts, suspicious file attachments, and social engineering tactics. Training should include hands-on exercises, such as simulated phishing campaigns.
- **Safe Defaults**: Configure endpoints to display full file extensions (e.g. .lnk, .exe, .scr), to reduce the chance of file masquerading.
- **Reporting Mechanisms**: Provide users with a simple, immediate way to report suspected phishing attempts to the security team.

2. Endpoint Hardening

Once the malicious payload executed, persistence and credential theft became possible. Reducing endpoint exposure is critical:

- **Application Control**: Implement application whitelisting so that only approved software can run.
- **Privilege Management**: Enforce least privilege on user accounts. Administrative rights should not be granted for daily operations.
- **Credential Protection**: Disable insecure mechanisms such as WDigest credential caching, which store plaintext passwords in memory.
- **Endpoint Detection and Response (EDR)**: Deploy solutions capable of detecting anomalous behavior such as reverse shell activity, unauthorized credential dumping tools, and unexpected persistence techniques.
- **Patch Management**: Maintain up-to-date operating systems and applications to minimize the exploitation of known vulnerabilities.

3. Credential and Identity Management

Compromised credentials were a turning point in this scenario. Stronger practices are needed to protect authentication mechanisms:

- **Multi-Factor Authentication (MFA)**: All remote access, particularly VPN connections, should require MFA to limit the impact of stolen credentials.
- **Secure Credential Storage**: Prohibit plaintext storage of credentials on endpoints. Instead, rely on centralized password vaults or hardware tokens.
- **Rotation and Expiration**: Enforce regular rotation of VPN and system passwords. Credentials shared across IT and OT systems (as in this case) should be eliminated.
- **Behavioral Monitoring**: Apply monitoring for unusual login behavior (e.g. VPN connections from unexpected geographies or at unusual hours)

4. Network Security and Segmentation

Even after VPN compromise, attackers should face barriers that slow down or prevent lateral movement:

- **Segmentation of IT and OT**: Maintain strict boundaries between IT and OT environments using firewalls and demilitarized zones (DMZs). VPN users should not have direct, unrestricted access to OT systems.
- **Microsegmentation**: Apply more granular network policies that limit user devices to only the services they require.
- **Zero Trust Principles**: Shift away from implicit trust based on network location. Every access request should be authenticated, authorized, and continuously validated.
- **Network Monitoring**: Use intrusion detection/prevention systems (IDS/IPS) tuned for both IT and OT protocols to detect reconnaissance or anomalous commands (e.g. unusual Siemens device scans).

5. Monitoring, Detection, and Incident Response

Rapid detection and response can stop an intrusion before it escalates:

- **Log Aggregation and SIEM**: Collect and analyze VPN logs, endpoint activity, and network events for suspicious behavior.
- **Threat Analysis**: Regularly check your SIEM for indicators of compromise (IoCs), such as alerts of malicious tools or anomalous remote sessions.
- **Incident Response Playbooks**: Establish clear processes for revoking compromised credentials, isolating infected endpoints, and communicating with stakeholders.
- **Testing and Exercises**: Conduct red team/blue team exercises to evaluate the resilience of both technical defenses and incident response capabilities.

6. Governance and Compliance Alignment

Organizations should anchor their defenses in established standards to ensure a structured and auditable approach:

- **NIST Cybersecurity Framework (CSF)**: Follow its core functions: Identify, Protect, Detect, Response, Recover, to guide security program maturity.
- **MITRE ATT&CK**: Map observed techniques (e.g. phishing, persistence via startup entries, credential dumping with Mimikatz, remote desktop/VNC access) to ATT&CK tactics for coverage analysis.
- **IEC 62443**: Apply OT-specific controls for secure remote access and defense against lateral movement in industrial environments.
- **ENISA Guidelines**: Incorporate ENISA's recommendations on securing remote work and critical infrastructure networks.

Conclusion

This scenario demonstrates that a single phishing email can enable attackers to pivot from a home device into core operational networks. Preventing such intrusions requires more than 1 defensive measure: it demands a layered security strategy that considers the human factor, technical hardening, identify and access management, and resilient network design. By combining these practices with continuous monitoring and adherence to recognized security frameworks, organizations can significantly reduce the likelihood and impact of similar attacks.