

# Digitisation and cyber security

## Lessons learned from the blackout in the Ukraine

30 August 2022, Swissgrid Grid Forum, Museum of Transport, Lucerne  
[cyrill.brunschwiler@compass-security.com](mailto:cyrill.brunschwiler@compass-security.com)



# How secure is our power supply ?





Neue Zürcher Zeitung

# Ein längeres Blackout hätte katastrophale Folgen – doch undenkbar ist es nicht

Eine Welt ohne Elektrizität können wir uns kaum vorstellen. Doch das Szenario einer anhaltenden Strommangellage ist keineswegs abwegig. Und die Politik tut zu wenig, um es abzuwenden.

01.06.2021, 05.30 Uhr David Vonplon



Gaëtan Bally / Keystone

# Substation (Mettlen)



<https://www.solutec.ch/en/aktuelles/referenzen/hs-netze/380-220kV-Schaltanlage-UW-METTLEN.php>



# How secure is our power supply?



<https://www.youtube.com/watch?v=UF5EDV6T7es>

# Substation protection devices, protocol converters, automation (IEDs)



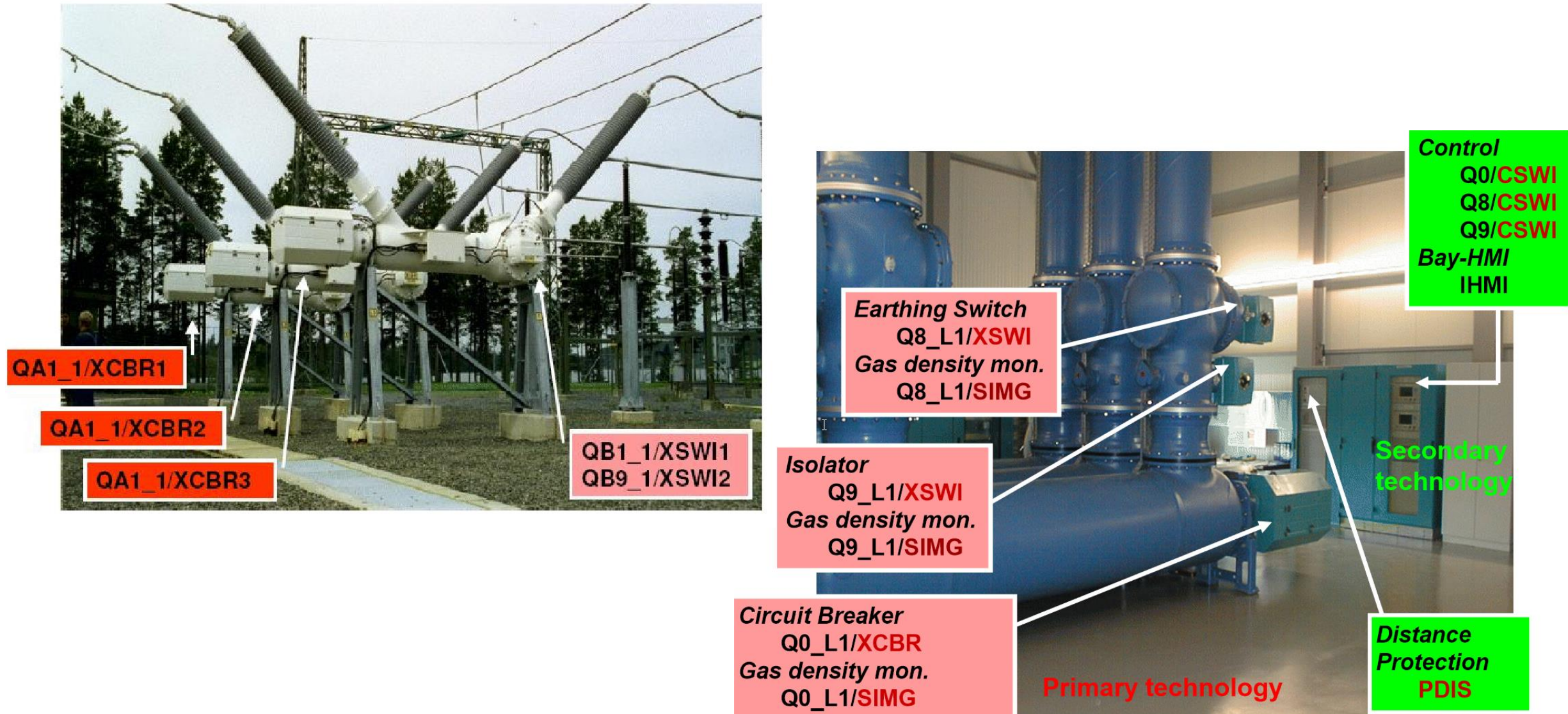
<https://new.abb.com/substation-automation/products/the-power-of-one>

<https://www.directindustry.com/prod/siemens-energy-automation/product-30064-589133.html>

<https://www.se.com/in/en/work/products/product-launch/easergy/easergy-p3.jsp>

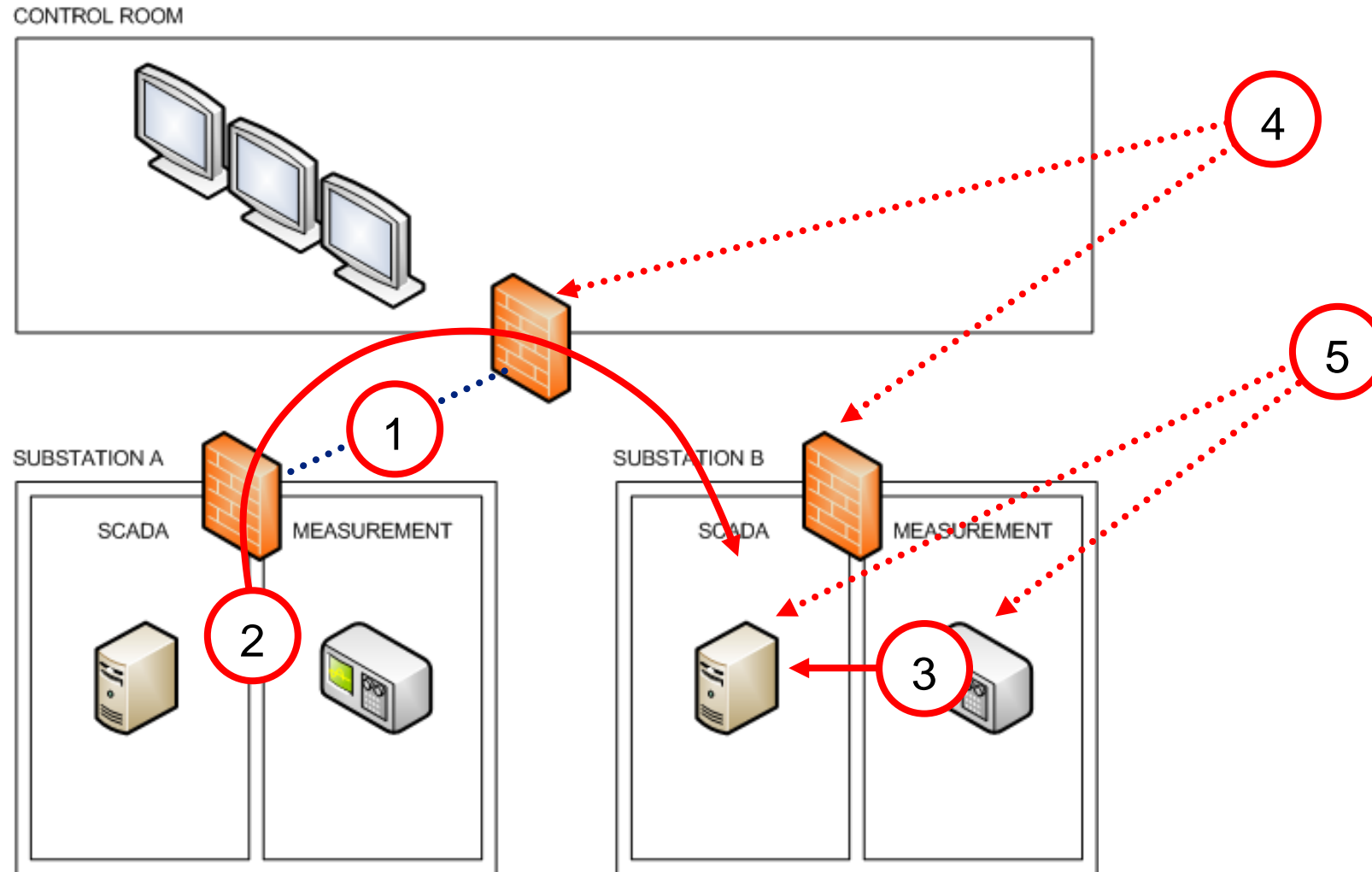


# Naming via object model (IEC 61850 MMS)



ABB, Kirrmann, [https://web.fe.up.pt/~asousa/sind/acetate/AI\\_EPFL/AI\\_421\\_IEC61850.pdf](https://web.fe.up.pt/~asousa/sind/acetate/AI_EPFL/AI_421_IEC61850.pdf)

# Attacks against substations – scenarios





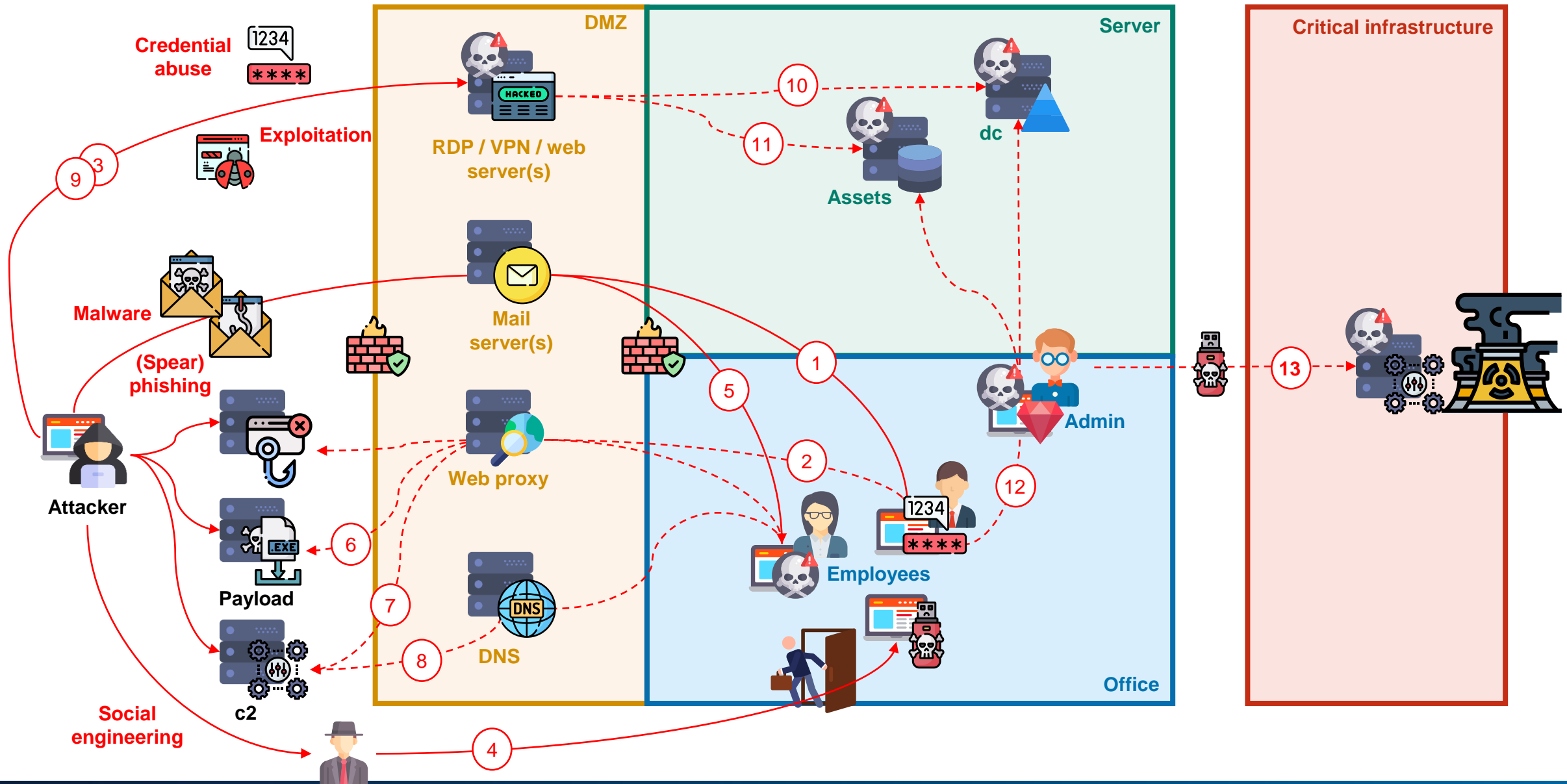
# Typical intrusion patterns

Not every intrusion is as ingenious as the media are led to believe.

In most cases, security breaches have simple causes:

- Malspam
- Weak passwords
- No 2FA
- Vulnerability of equipment or software (lack of patches)

# Typical intrusion patterns





# MITRE ATT&CK framework

MITRE | ATT&CK®

Matrices

Tactics ▾

Techniques ▾

Mitigations ▾

Groups

Software

Resources ▾

Blog ↗

Contribute

Search 🔍

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	System Services (2)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	User Execution (2)	Create Account (3)	Group Policy Modification	Group Policy Modification	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Windows Management Instrumentation	Create or Modify System Process (4)	Hijack Execution Flow (11)	Hide Artifacts (7)	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites				Event Triggered Execution (15)	Process Injection (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
				External Remote Services	Scheduled Task/Job (6)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Email Collection (3)	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
				Hijack Execution Flow (11)	Valid Accounts (4)	Indicator Removal on Host (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Non-Standard Port		Service Stop
				Implant Container Image		Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Protocol Tunneling		System Shutdown/Reboot
				Office Application Startup (6)		Masquerading (6)	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (2)	Proxy (4)		
				Pre-OS Boot (5)		Modify Authentication Process (4)		Query Registry		Screen Capture	Remote Access Software		
				Scheduled Task/Job (6)		Modify Cloud Compute Infrastructure (4)		Remote System Discovery		Video Capture	Traffic Signaling (1)		
				Server Software Component (3)		Modify Registry		Software Discovery (1)			Web Service (3)		
				Traffic Signaling (1)		Modify System Image (2)		System Information Discovery					
				Valid		Network Boundary Bridging (1)		System Network Configuration Discovery					
						Obfuscated Files or Information (5)		System Network Connections Discovery					

# MITRE ATT&CK framework

## Groups

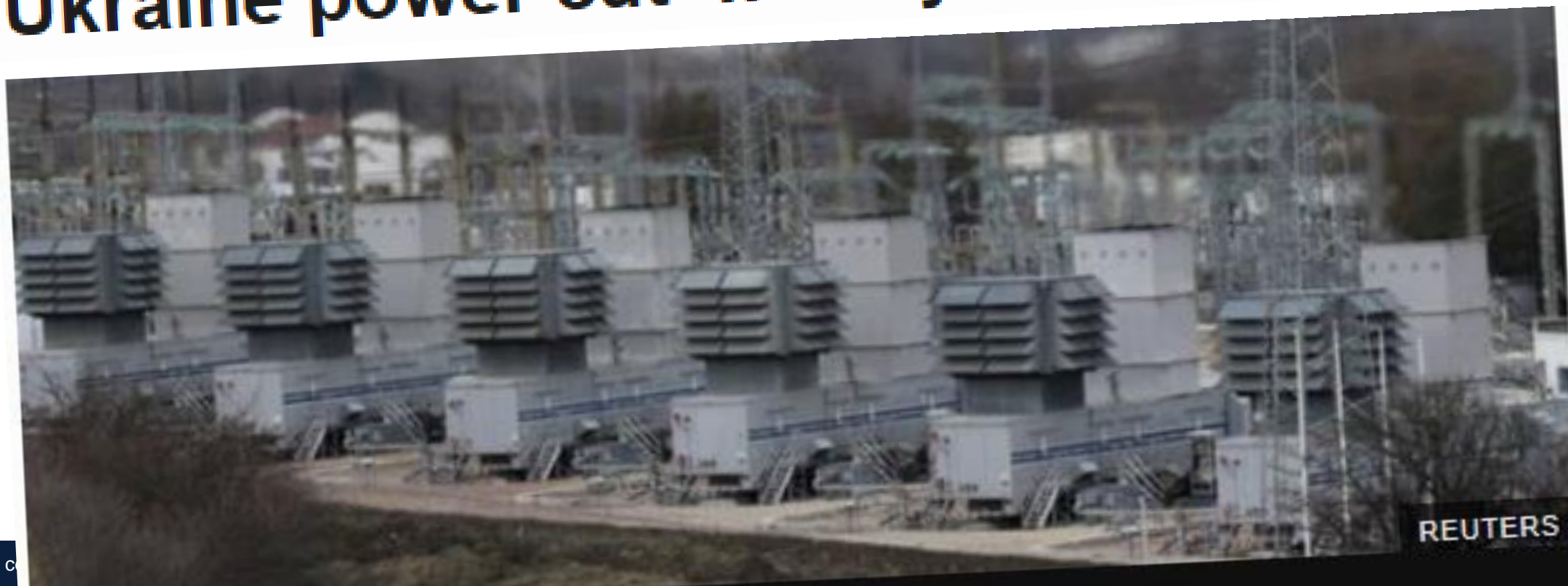
			primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name (RTM).
G0034	Sandworm Team	ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VODOO BEAR	<p><a href="#">Sandworm Team</a> is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455. This group has been active since at least 2009.</p> <p>In October 2020, the US indicted six GRU Unit 74455 officers associated with <a href="#">Sandworm Team</a> for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide <a href="#">NotPetya</a> attack, targeting of the 2017 French presidential campaign, the 2018 <a href="#">Olympic Destroyer</a> attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019. Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as <a href="#">APT28</a>.</p>
G0029	Scarlet Mimic		<p><a href="#">Scarlet Mimic</a> is a threat group that has targeted minority rights activists.</p>



## NEWS

[Home](#)[Video](#)[World](#)[UK](#)[Business](#)[Tech](#)[Science](#)[Stories](#)[Entertainment & Arts](#)

# Ukraine power cut 'was cyber-attack'



REUTERS

# Ukraine hack

## Step 1

- Phishing e-mails with Word macro, BlackEnergy trojan loaded
- VPN logons and passwords stolen
- Network analysis and lateral movement

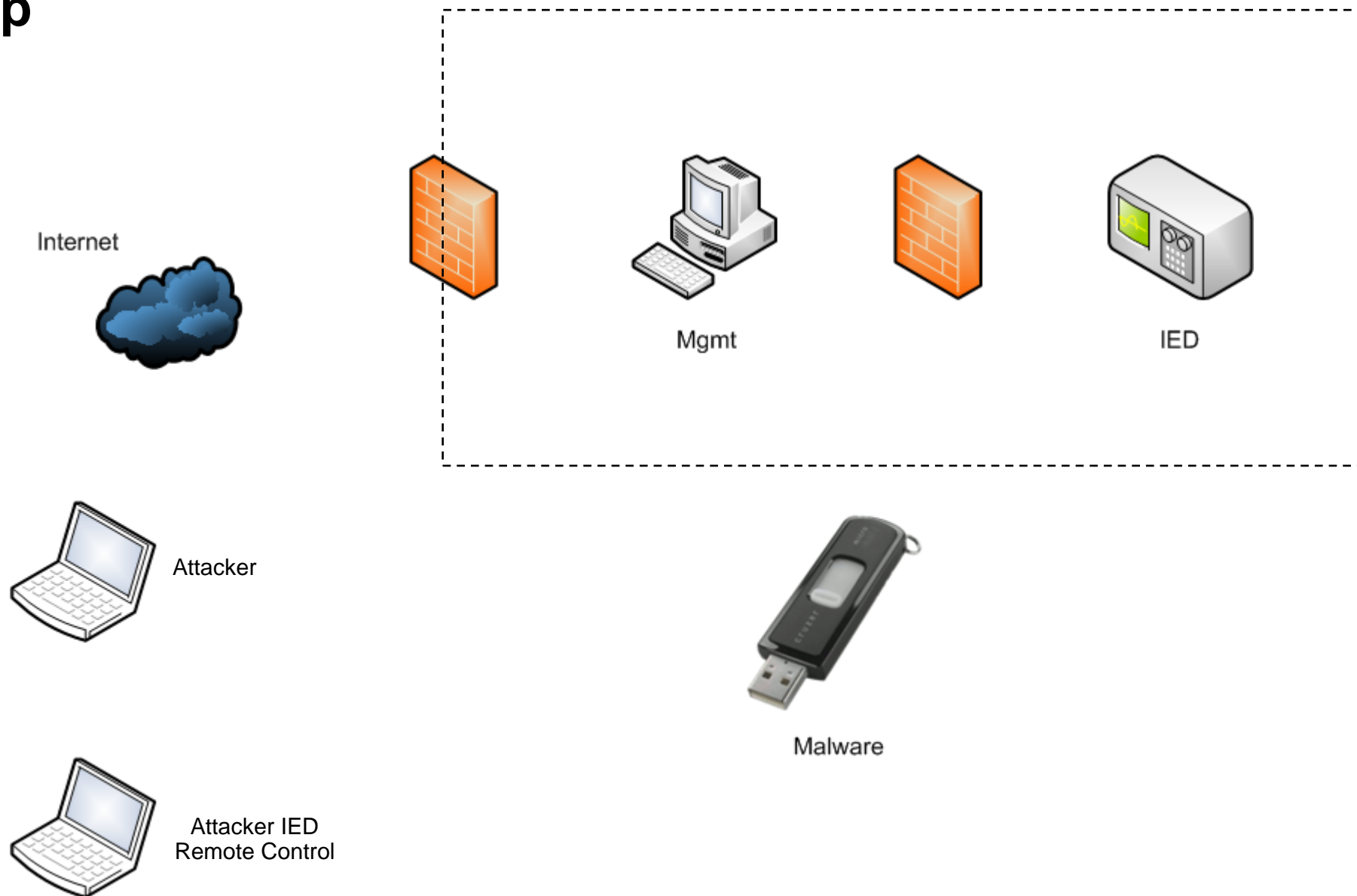
## Step 2

- Malicious firmware developed
- SCADA environment taken over via user interface
- Disconnecting switch opened
- UPS shutdown orchestrated, firmware loaded onto converter, logs and disks deleted
- Denial of telephony service

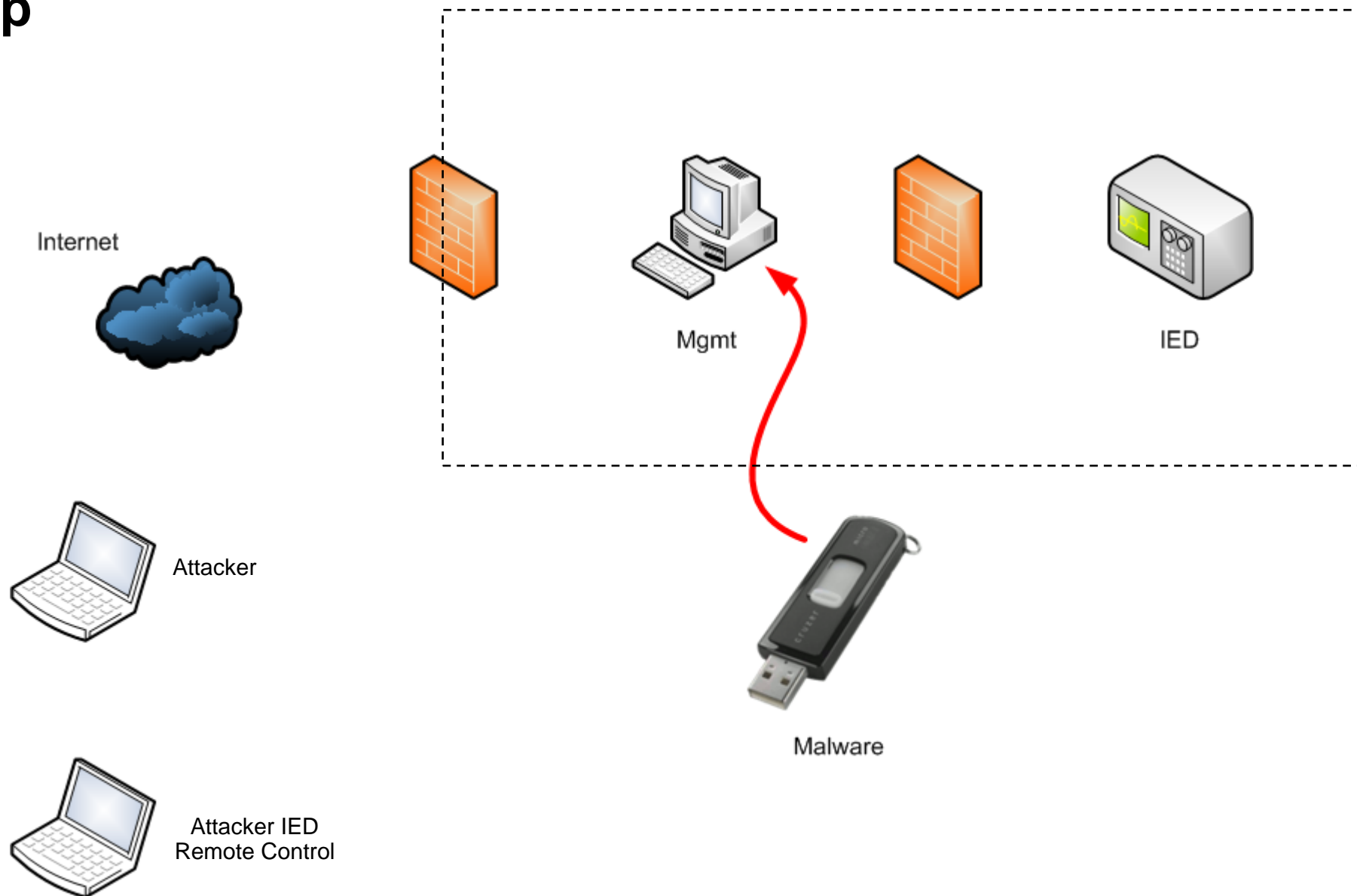
[https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)



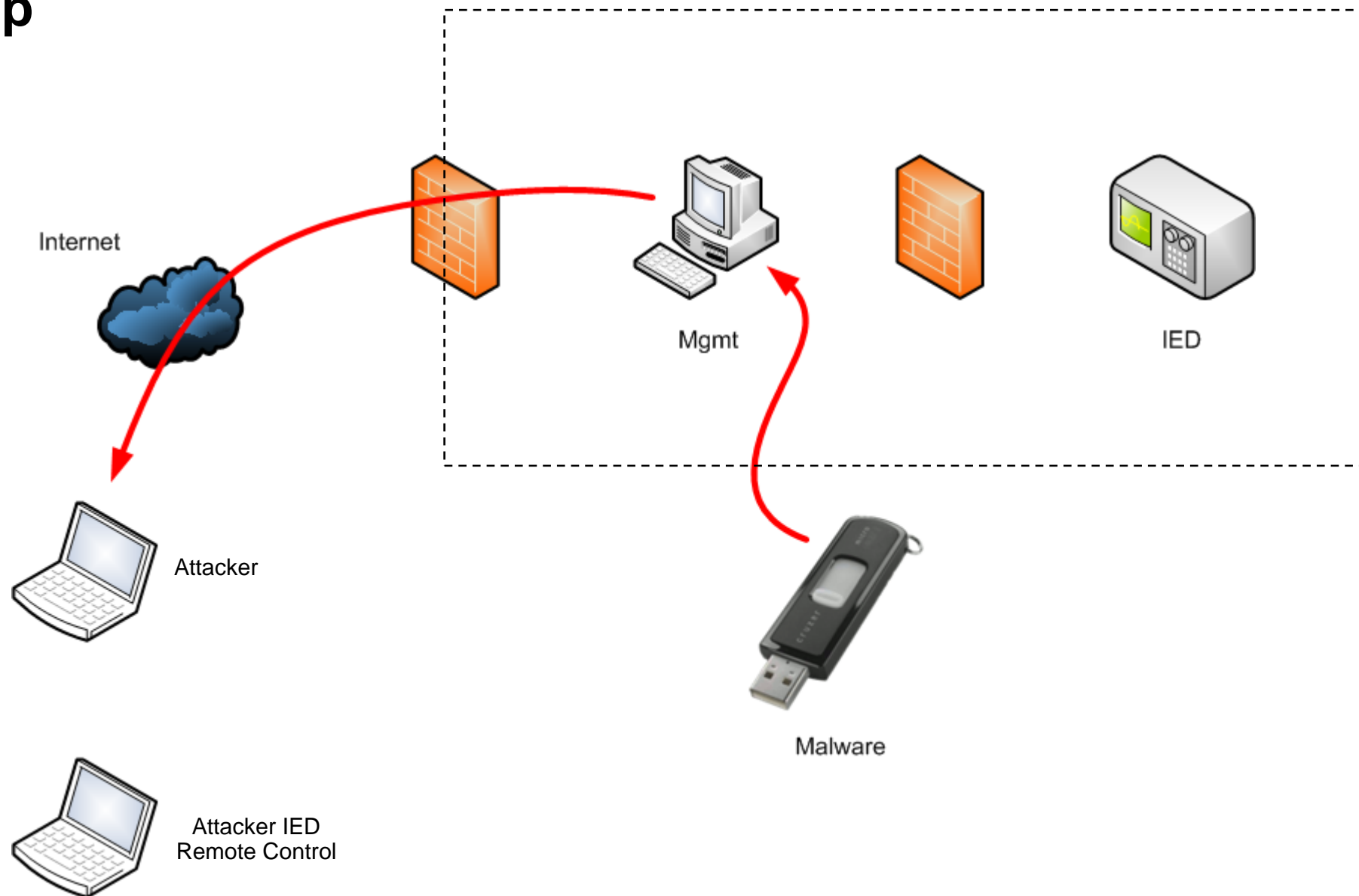
# Demo set-up



# Demo set-up

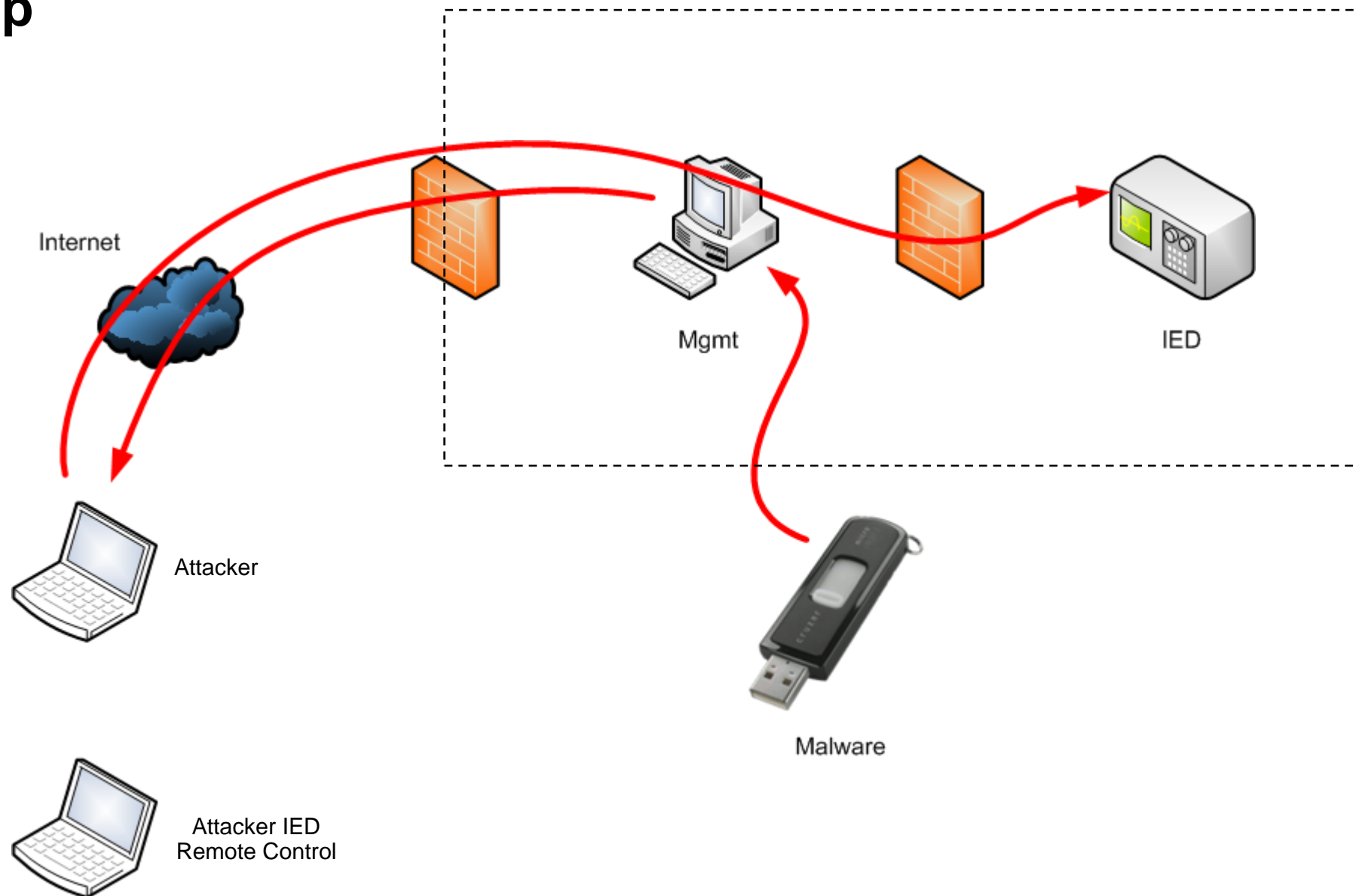


# Demo set-up

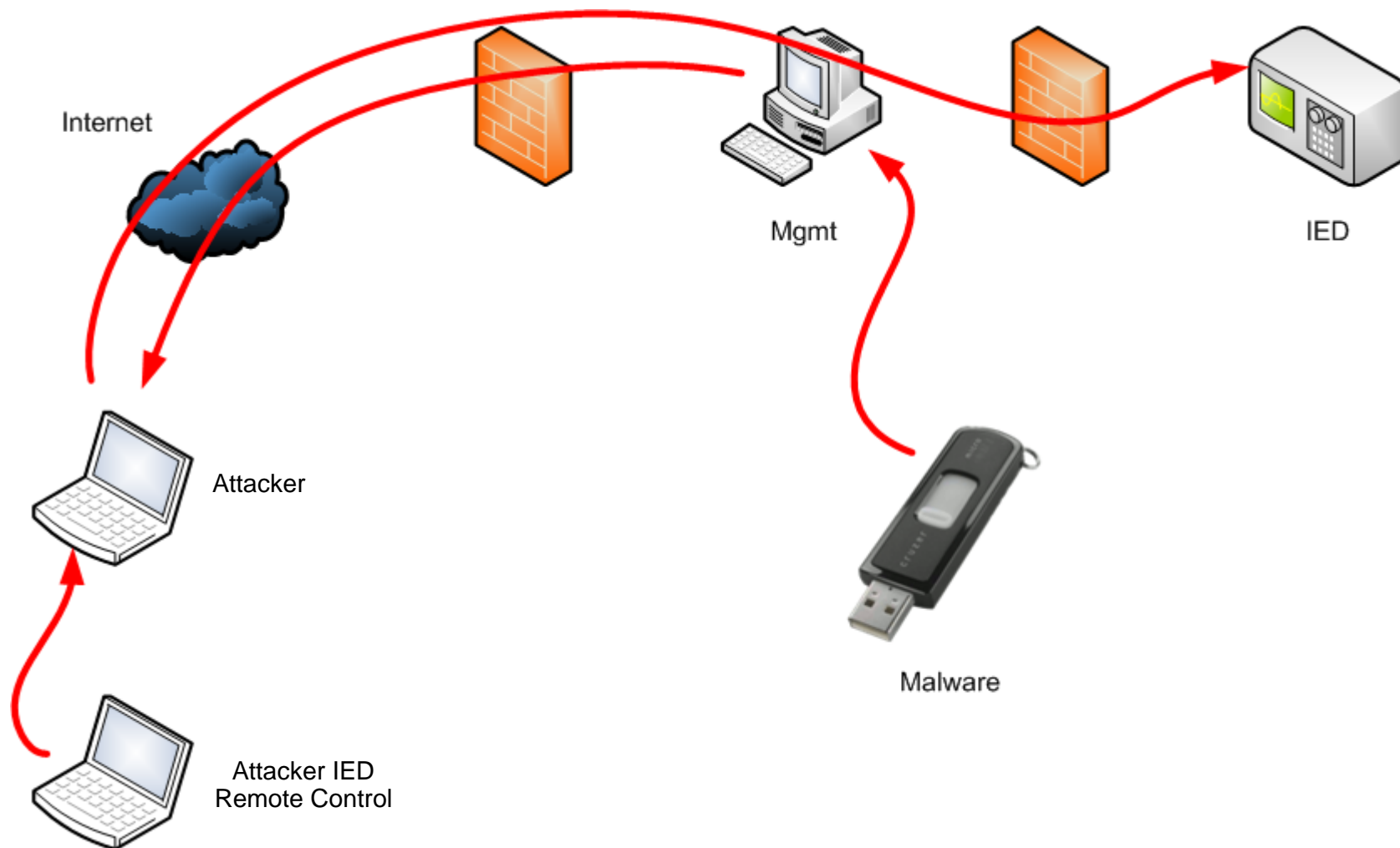




# Demo set-up



# Demo set-up





# How to react ?





# Behaviour of attackers

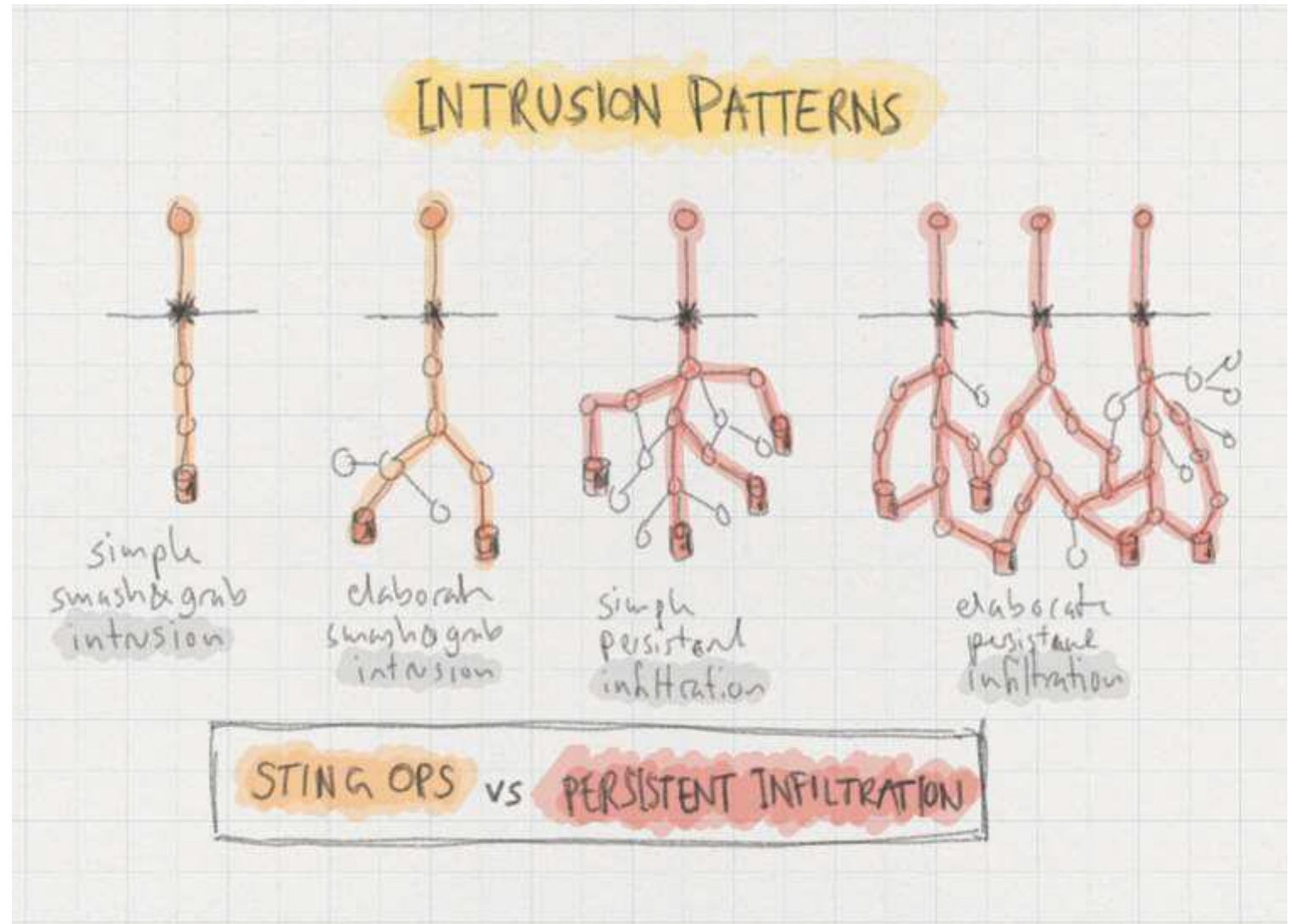
## Intrusion patterns

### Sting operation

Also called «smash and grab».  
A direct attack to obtain a certain piece of information or to carry out an action.

### Persistent infiltration

A prolonged campaign in which your adversary gains and maintains unauthorised access to your infrastructure over an extended period of time.



[Source]: <https://www.slideshare.net/FrodeHommedal/taking-the-attacker-eviction-red-pill>  
[https://www.youtube.com/watch?time\\_continue=3&v=WAvO0Y0nOws](https://www.youtube.com/watch?time_continue=3&v=WAvO0Y0nOws)

**Fix the grid!**

# Basic protection for «operational technology» in the supply of electricity

## 2.6.1 Physical security principles

(11) ... laptops, portable parameterising or remote-controlled PCs and handheld devices **have to** be strictly secured and not used outside the ICS network.



# Basic protection for «operational technology» in the supply of electricity

## 2.8.3 Remote access and authentication

(3) ... access to the jump stations **have to** take place by means of two-factor authentication and be monitored and controlled at all times. ...

alk:~\$ Thank you for your attention...

