



Numérisation et Cyber Security

Leçons tirées du black-out en Ukraine

30 août 2022, Forum des réseaux de Swissgrid, Musée des transports de Lucerne
cyrill.brunschwiler@compass-security.com

Quel est le niveau de sécurité de notre approvisionnement en électricité?



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

Sous-station (SS Mettlen)



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

Quel est le niveau de sécurité de notre approvisionnement en électricité?

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

Sous-station: appareils de protection, convertisseurs de protocole, automatisations (IED)

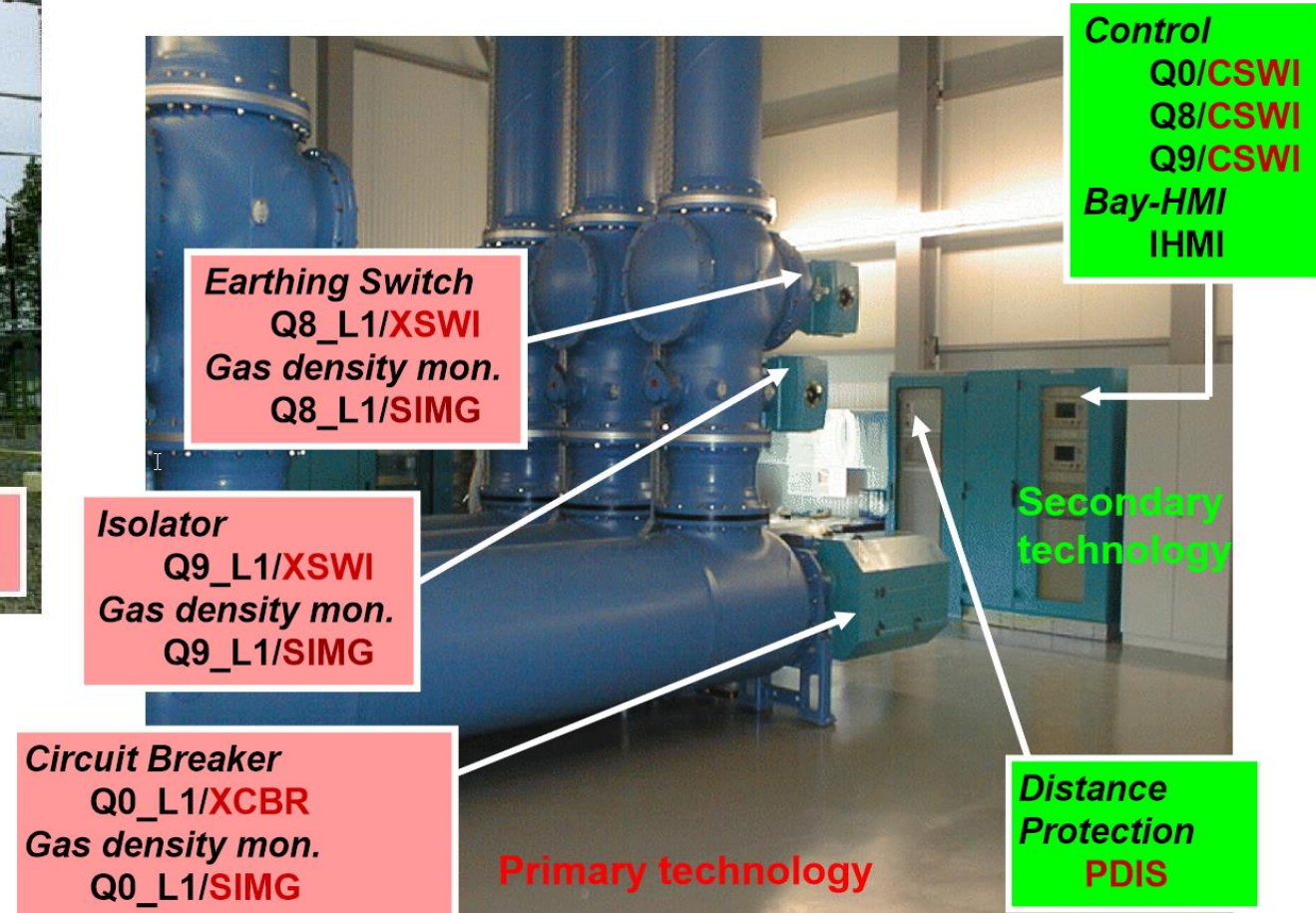
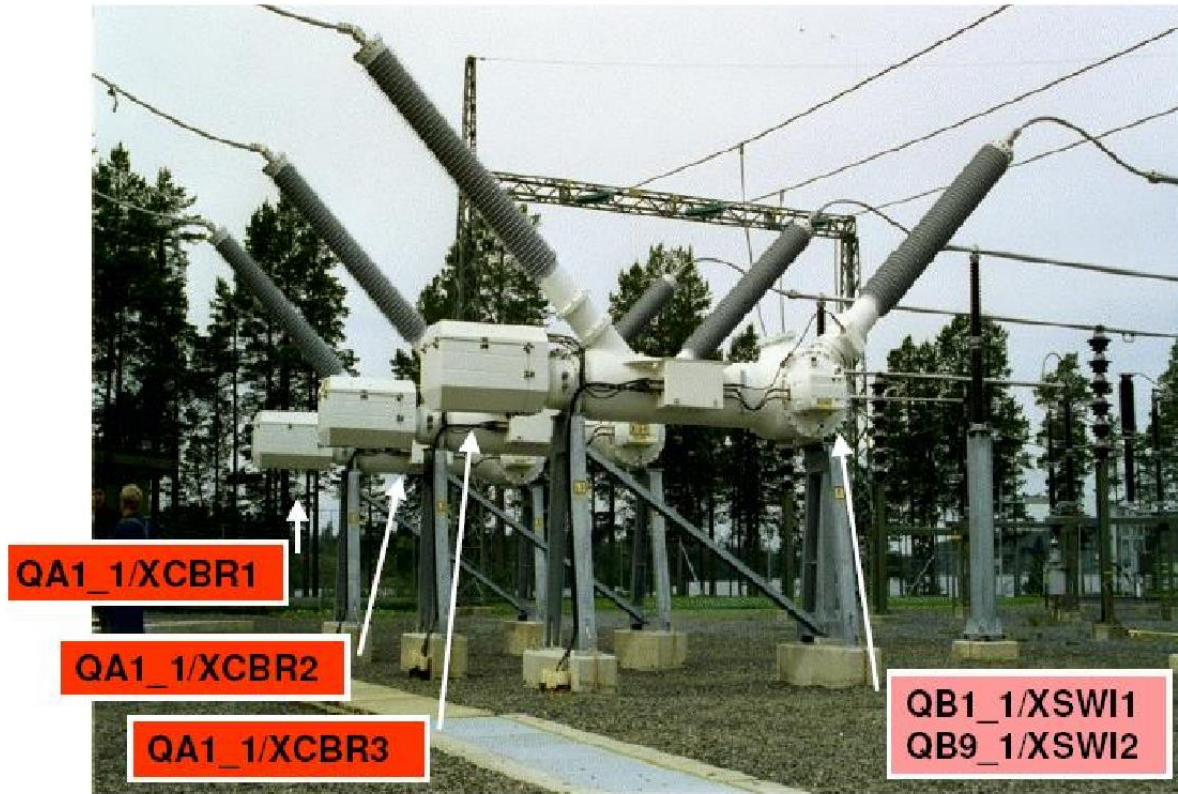


<https://new.abb.com/substation-automation/products/the-power-of-one>

<https://www.directindustry.fr/prod/siemens-energy-automation-and-smart-grid/product-30064-589133.html>

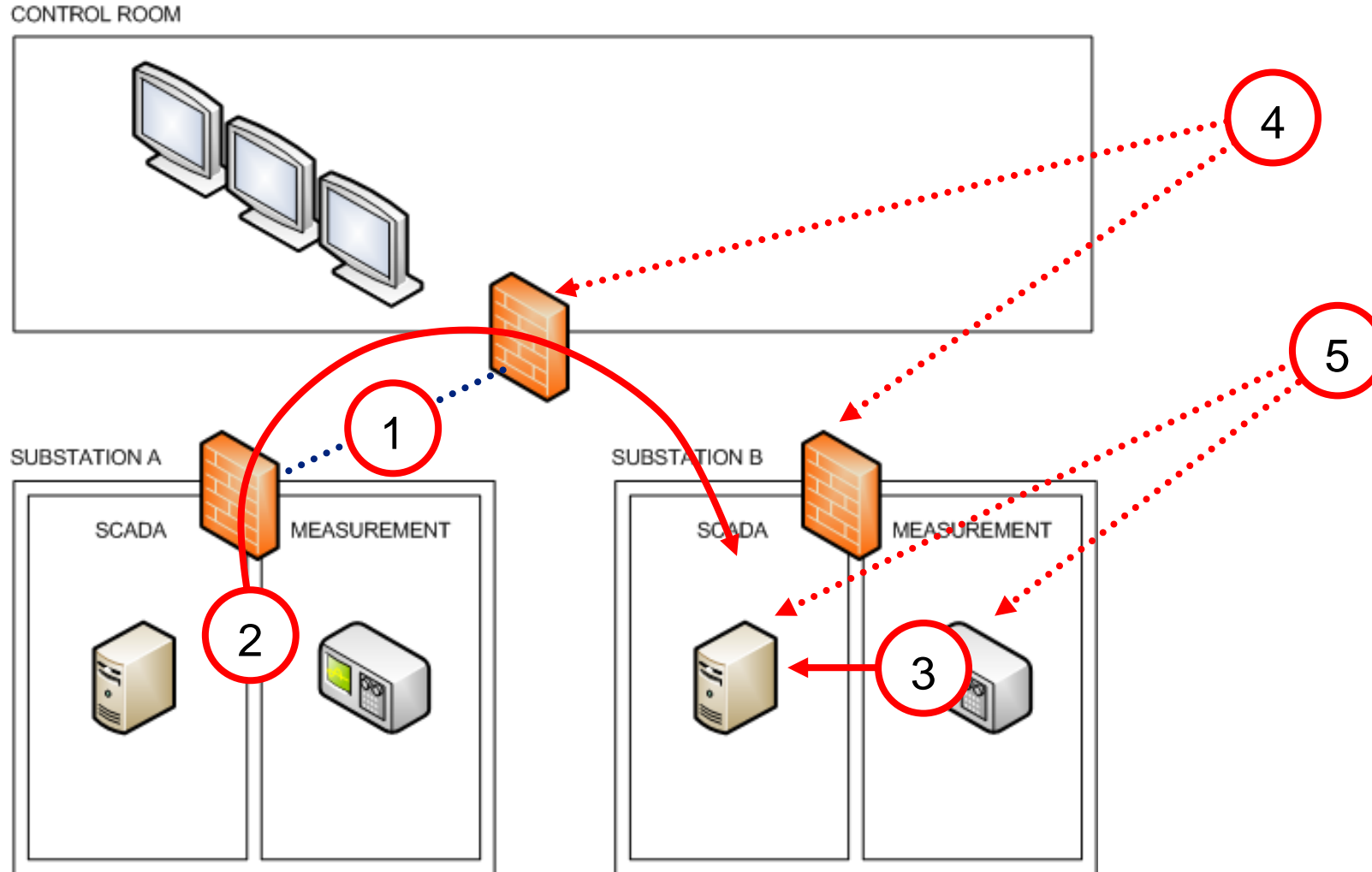
<https://www.se.com/in/en/work/products/product-launch/easergy/easergy-p3.jsp>

Dénomination au moyen d'un modèle d'objet (CEI 61850 MMS)



ABB, Kirmann, https://web.fe.up.pt/~asousa/sind/acetat/AI_EPFL/AI_421_IEC61850.pdf

Scénarios d'attaque contre les sous-stations



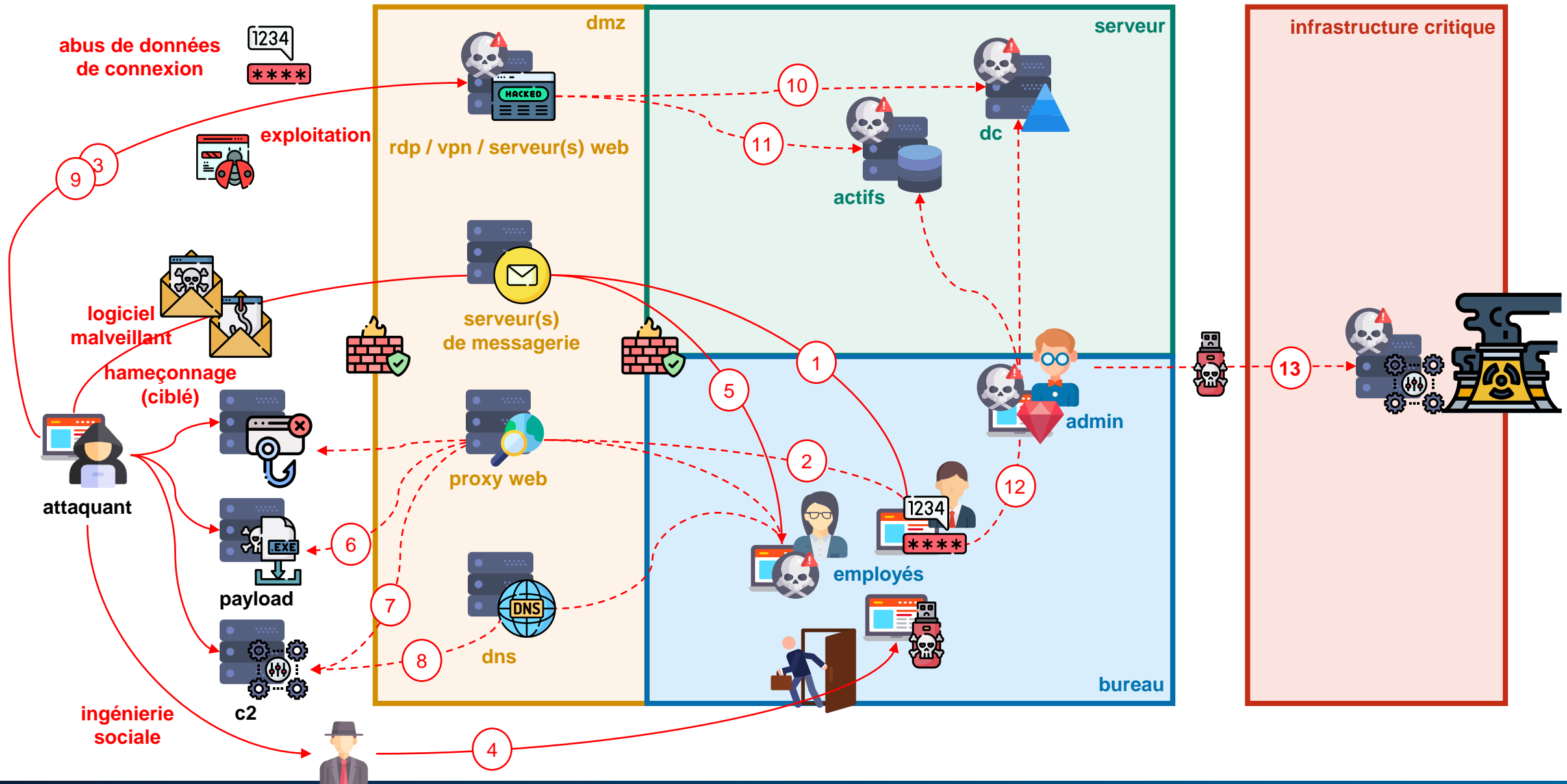
Schémas typiques d'intrusion

Tous les incidents ne sont pas aussi géniaux que ce que les médias veulent bien faire croire.

En général, les entreprises se font avoir par des pièges simples:

- spam malveillant
- mauvais mots de passe
- absence de 2FA
- vulnérabilité des appareils ou des logiciels (correctifs manquants)

Schémas typiques d'intrusion



Qu'est-ce que cela veut dire plus précisément?

Cadre MITRE ATT&CK

Cadre MITRE ATT&CK

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 Other Network Medium (1)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Browser Extensions	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Information Repository (2)	Data from Configuration Repository (2)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Compromise Client Software Binary	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Supply Chain Compromise (3)	System Services (2)	Software Deployment Tools	Create Account (3)	Create Account (3)	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	File and Directory Discovery	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	User Execution (2)	System Services (2)	Create or Modify System Process (4)	Create or Modify System Process (4)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Network Service Scanning	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)	Valid Accounts (4)	Windows Management Instrumentation	User Execution (2)	Event Triggered Execution (15)	Event Triggered Execution (15)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Network Share Discovery	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			Valid Accounts (4)	Event Triggered Execution (15)	Event Triggered Execution (15)	Group Policy Modification	Steal Application Access Token	Network Sniffing		Network Sniffing	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
				External Remote Services	External Remote Services	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Peripheral Device Discovery	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
				Hijack Execution Flow (11)	Hijack Execution Flow (11)	Impair Defenses (7)	Steal Web Session Cookie	Passowrd Policy Discovery		Permission Groups Discovery (3)	Protocol Tunneling		Service Stop
				Implant Container Image	Implant Container Image	Indicator Removal on Host (6)	Two-Factor Authentication Interception	Query Registry		Process Discovery	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)	Office Application Startup (6)	Indirect Command Execution	Unsecured Credentials (6)	Remote System Discovery		Query Registry	Remote Access Software		
				Pre-OS Boot (5)	Pre-OS Boot (5)	Masquerading (6)		Software Discovery (1)		Query Registry	Traffic Signaling (1)		
				Scheduled Task/Job (6)	Scheduled Task/Job (6)	Modify Authentication Process (4)		System Information Discovery		Remote System Discovery	Web Service (3)		
				Server Software Component (3)	Server Software Component (3)	Modify Cloud Compute Infrastructure (4)		System Network Configuration Discovery		Screen Capture			
				Traffic Signaling (1)	Traffic Signaling (1)	Modify Registry		System Network Connections Discovery		Video Capture			
				Valid	Valid	Modify System Image (2)							
						Network Boundary Bridging (1)							
						Obfuscated Files or Information (5)							

Cadre MITRE ATT&CK

Groupes

			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, VOODOO BEAR	<p>Sandworm Team 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 Sandworm Team for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide NotPetya attack, targeting of the 2017 French presidential campaign, the 2018 Olympic Destroyer 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 APT28.</p>
G0029	Scarlet Mimic		<p>Scarlet Mimic 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

Piratage en Ukraine

Étape 1

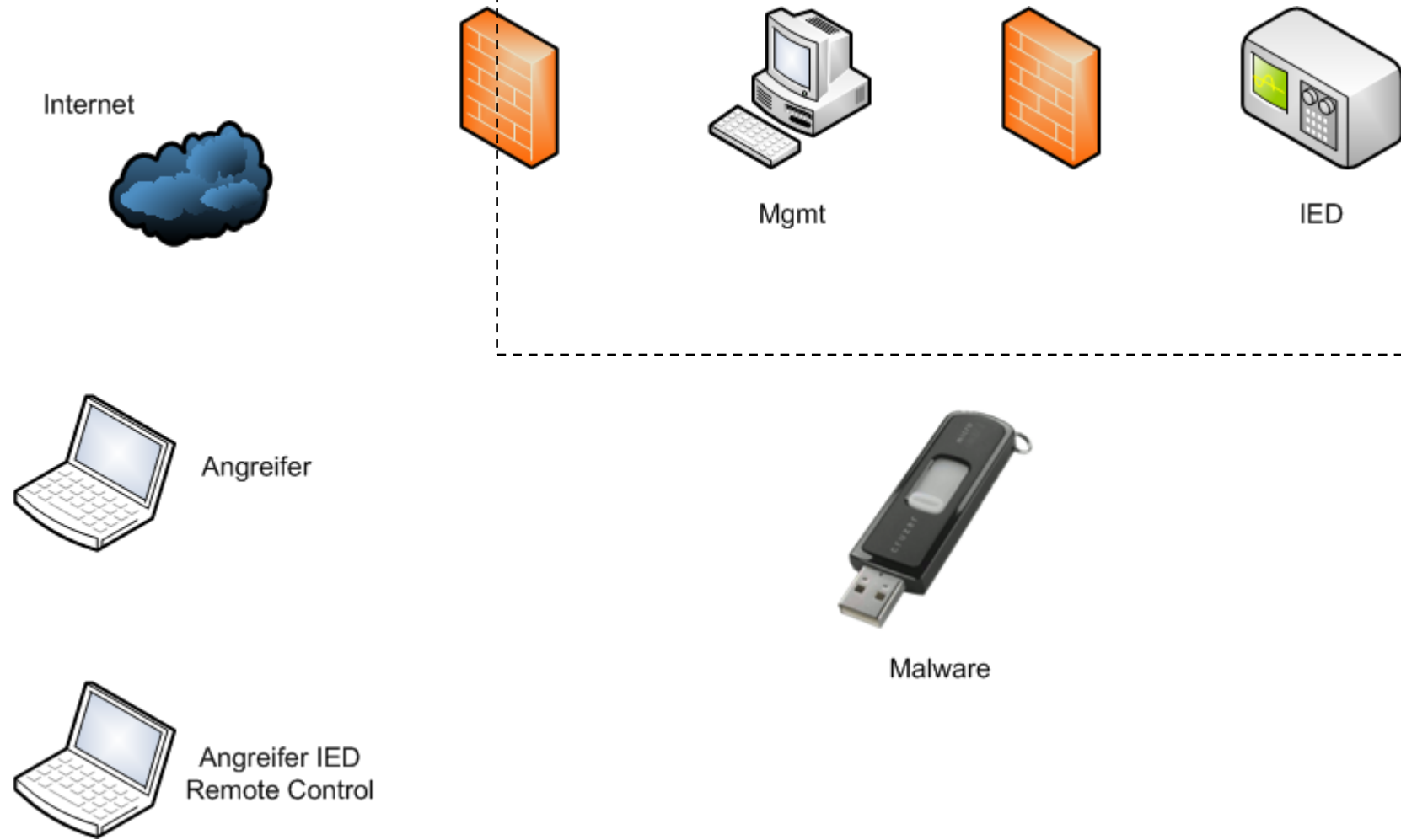
- E-mails de phishing avec des macros Word et des chevaux de Troie BlackEnergy
- Données d'accès VPN et mots de passe volés
- Analyse de réseau et mouvement latéral

Étape 2

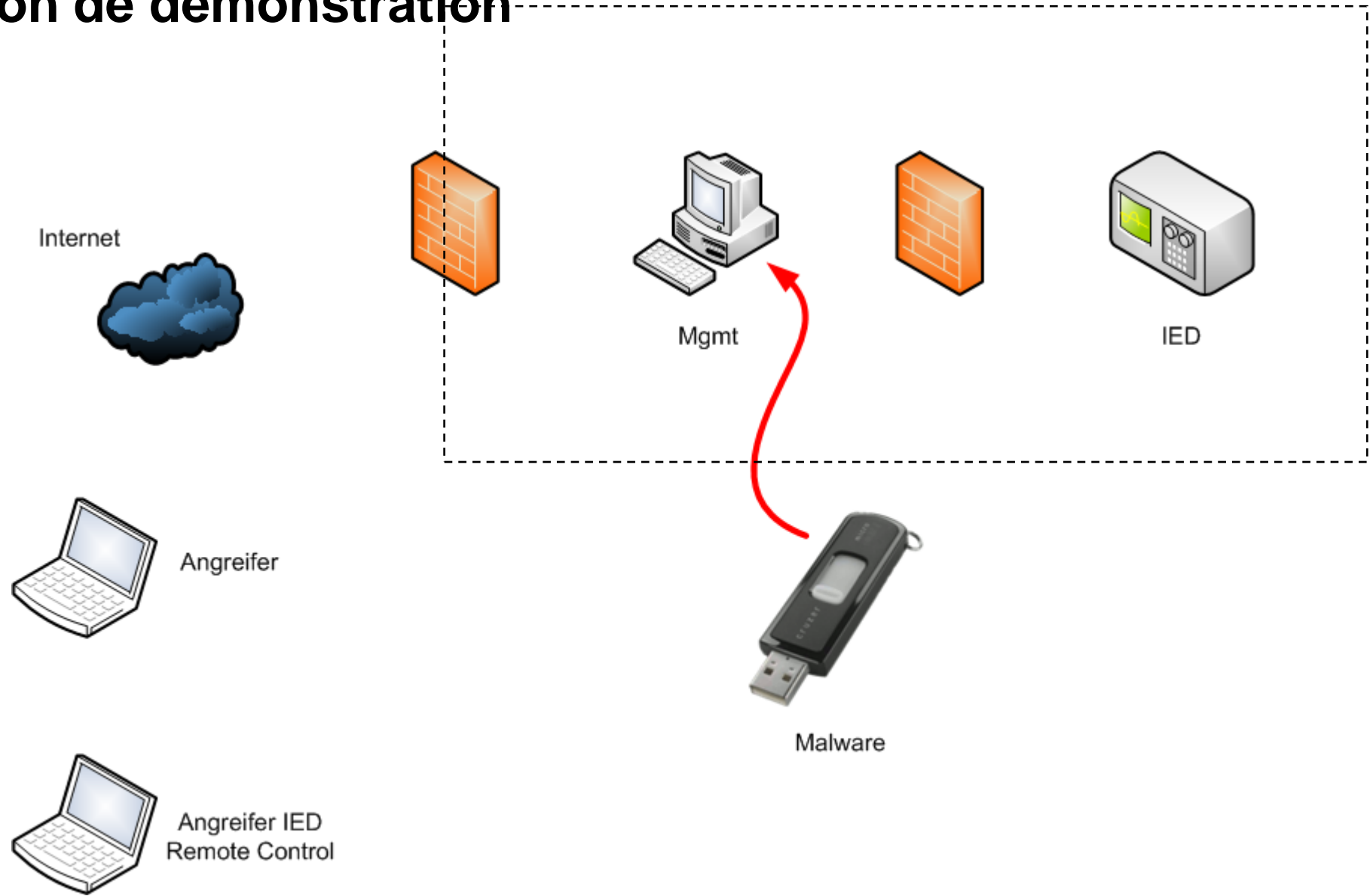
- Micrologiciel malveillant développé
- Environnement SCADA repris via l'interface utilisateur
- Sectionneur ouvert
- Coupure UPS orchestrée, micrologiciel chargé sur le convertisseur, journaux et disques effacés
- Déni de service téléphonique

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

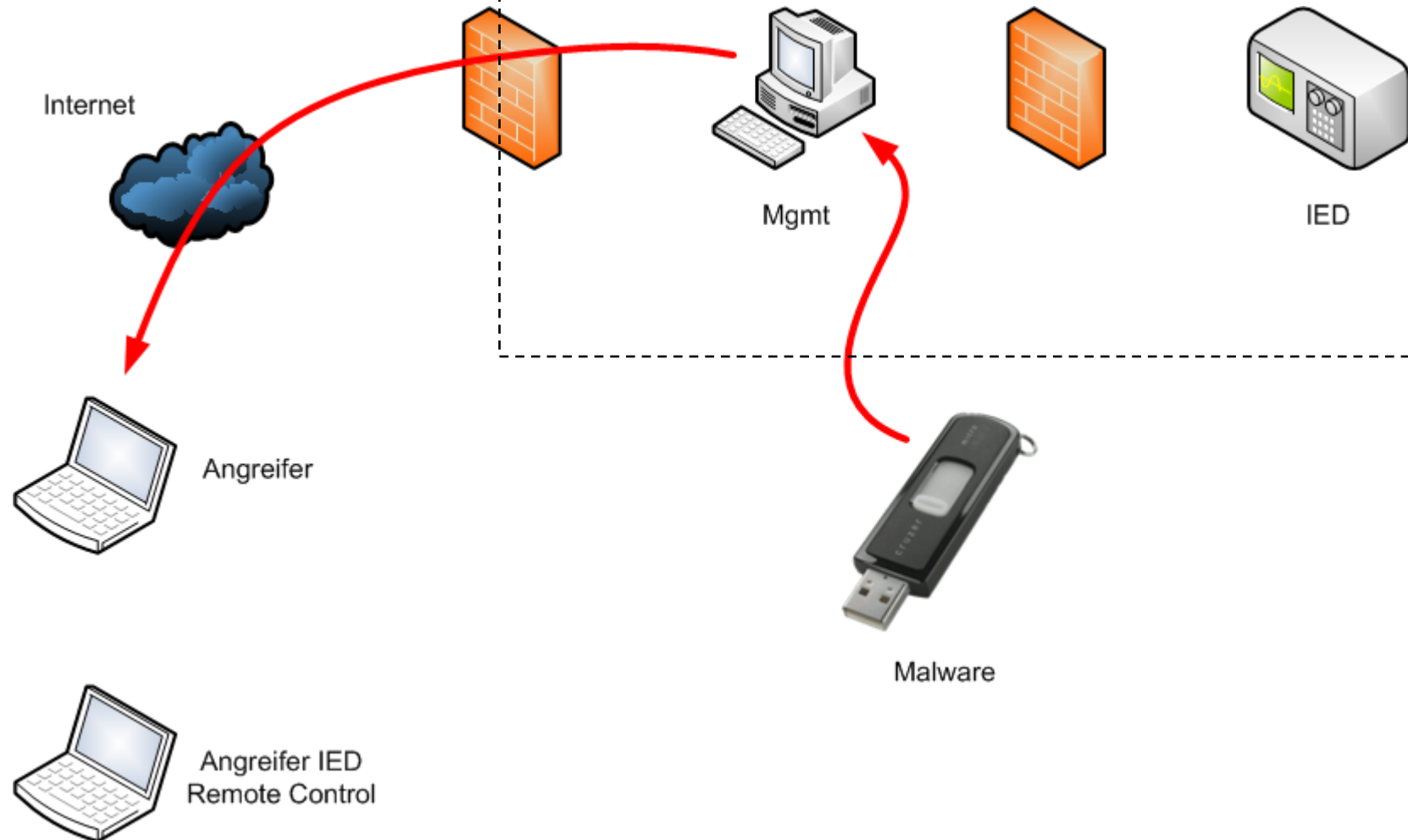
Configuration de démonstration



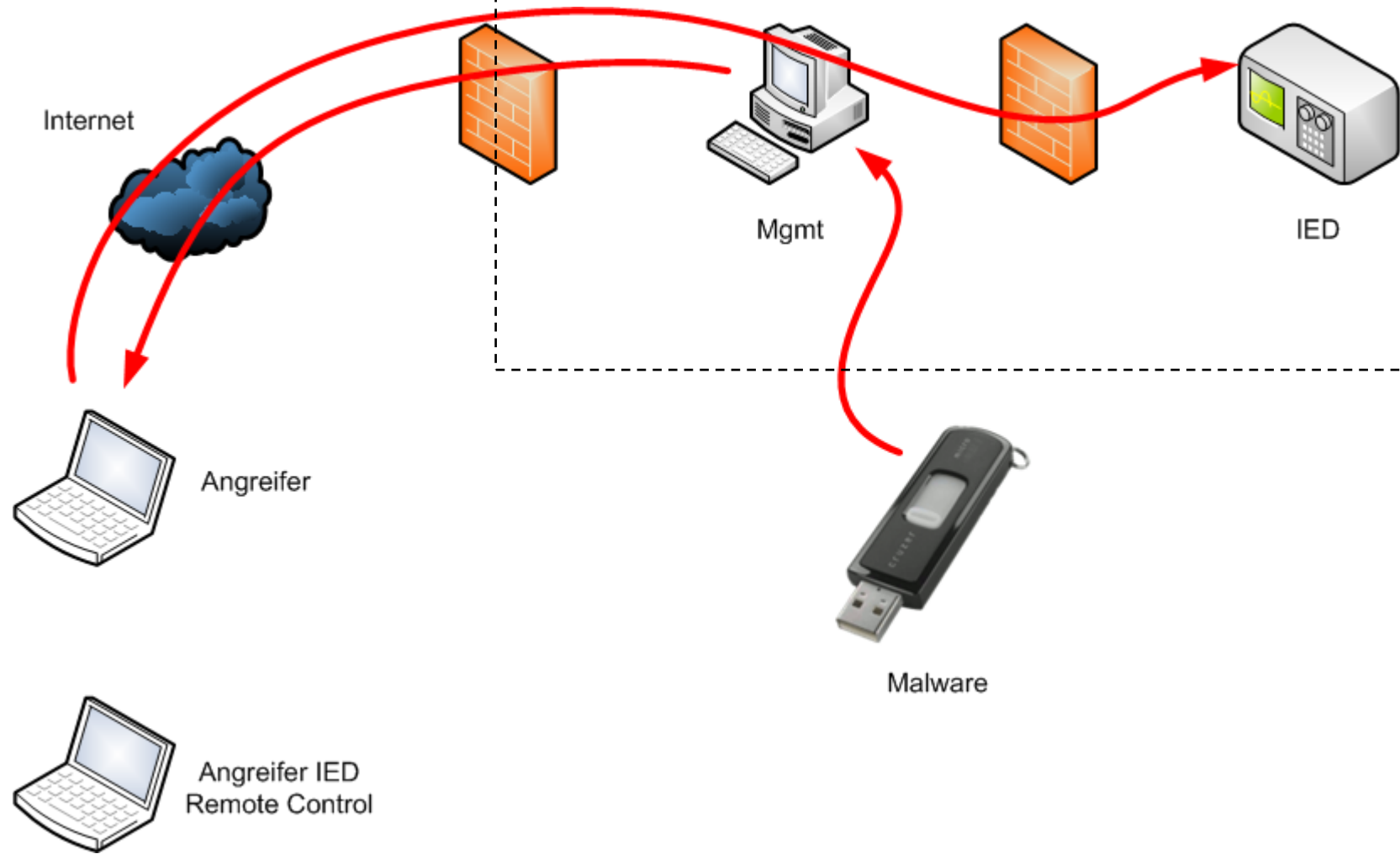
Configuration de démonstration



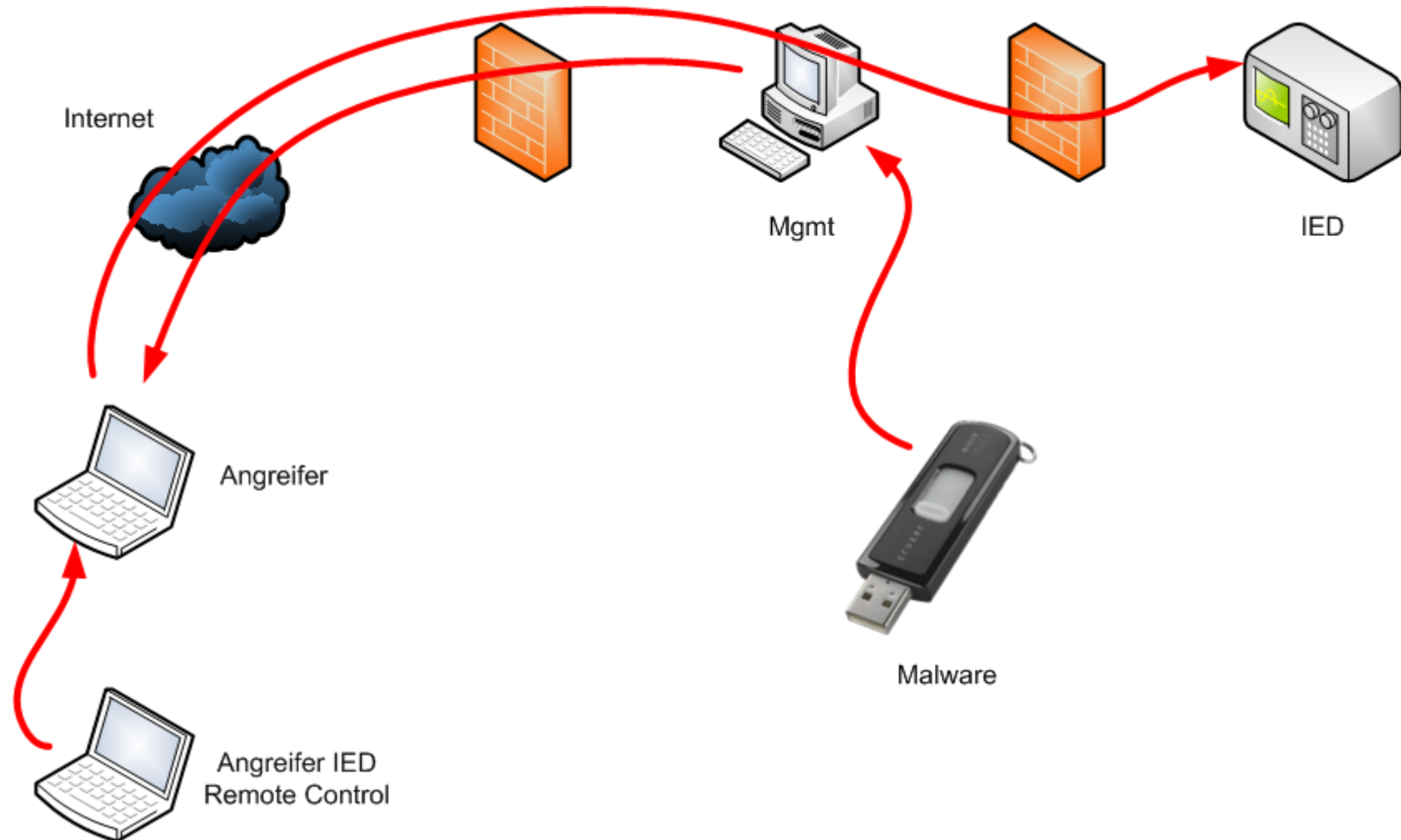
Configuration de démonstration



Configuration de démonstration



Configuration de démonstration



Et si cela arrivait?



Comportements des attaquants

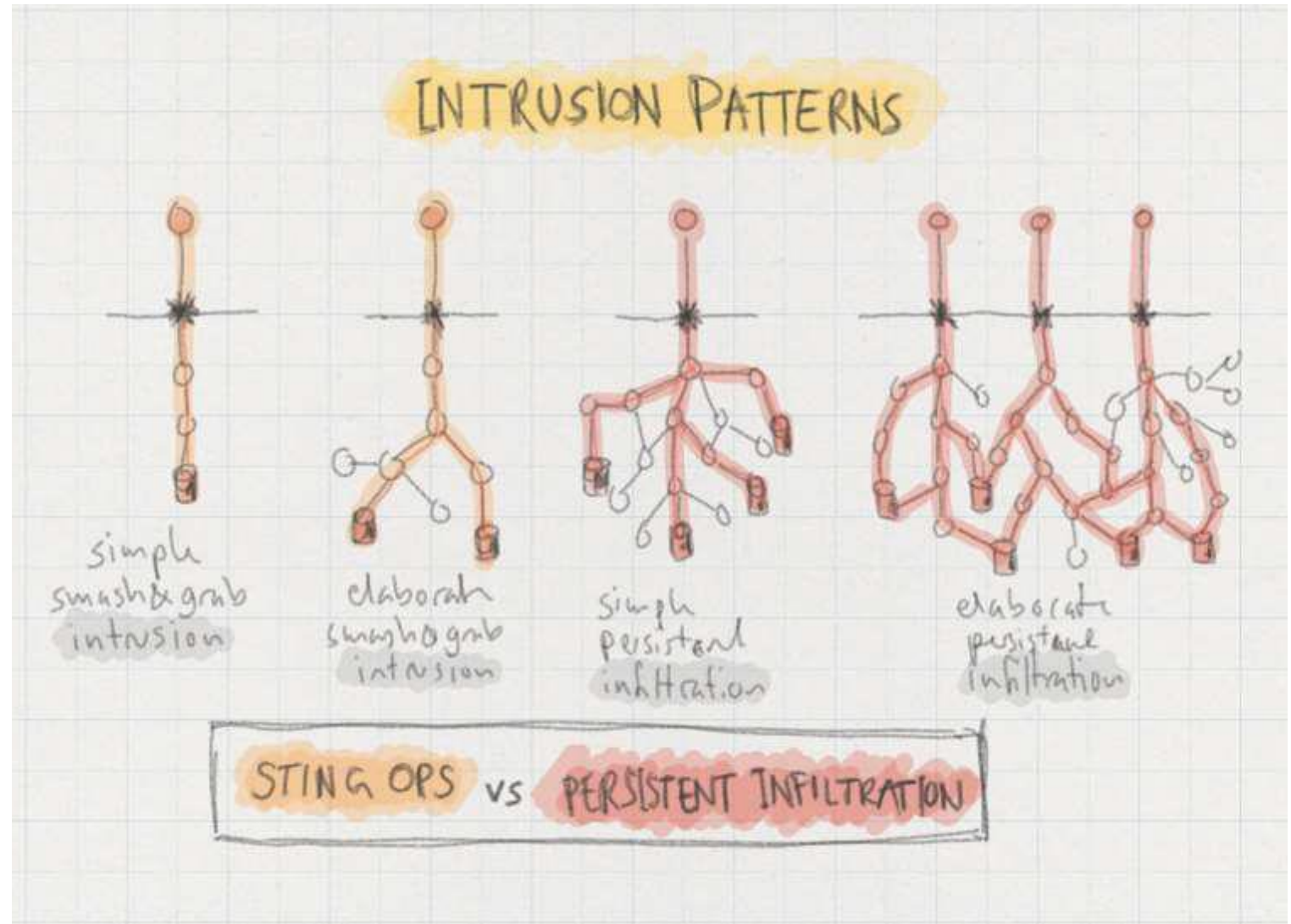
Modèles d'intrusion

Opération Sting

Aussi appelée «smash and grab» («fracasser et saisir» en français). Une attaque directe pour obtenir une information spécifique ou effectuer une action.

Infiltration persistante

Une campagne de longue durée pendant laquelle votre adversaire obtient et maintient un accès non autorisé à votre infrastructure.



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

Fix the Grid!

Protection de base pour «Operational Technology» dans le domaine de l'approvisionnement en électricité

2.6.1 Principes de sécurité physique

(11) ... les ordinateurs portables, les PC portables de paramétrage ou de commande à distance et les ordinateurs de poche **doivent** être strictement sécurisés et ne pas être utilisés en dehors du réseau ICS.

Protection de base pour «Operational Technology» dans le domaine de l'approvisionnement en électricité

2.8.3 Accès à distance et authentification

(3) ... Les accès aux stations Jump **doivent** être effectués au moyen d'une authentification à deux facteurs et peuvent être surveillés et contrôlés à tout moment. (...)

alk:~\$ Merci de votre attention...

