Landis+Gyr

ENSURING CYBER SECURITY IN SUBSTATIONS

VISIBILITY & REAL-TIME THREAT DETECTION ACROSS THE ELECTRIC GRID

I. INTRODUCTION

By the time the lights went out in Kyiv on December 17, 2016, the cybercriminals had already been scouting the networks of energy provider Ukrenergo for about 11 months. They took over authorized accounts, created new ones, spied on the network structure, and placed various payloads with pinpoint accuracy. In the end, they had full control over a 330kV substation that supplied electricity to about 20% of Ukraine's capital. As the extended forensic analysis of the attack dubbed CRASHOVERRIDE (also Industroyer) revealed, it was mainly luck (and dilettantism on the attackers' part) that the power outage lasted only an hour and no lives were harmed.

Despite the existing, common security architecture with password protection and firewalls, the attackers were able to penetrate the network, move on to other network segments and cause significant damage.

The success of the attackers can be attributed to two reasons:

1. lack of visibility on both central network as well as substation level, and
2. lack of mechanisms to distinguish between malicious and legitimite communications over authorized channels.

This document explains, with reference to the established MITRE ATT&CK® for ICS framework, the risk posed by lack of visibility in substation control systems (SCS). Two examples are used to explain in detail the sequence of professional, targeted attacks. The document concludes with a strategy for establishing end-to-end operational visibility and real-time threat detection to improve the cyber resilience and ensure the reliability, safety and revenue of substation operations.

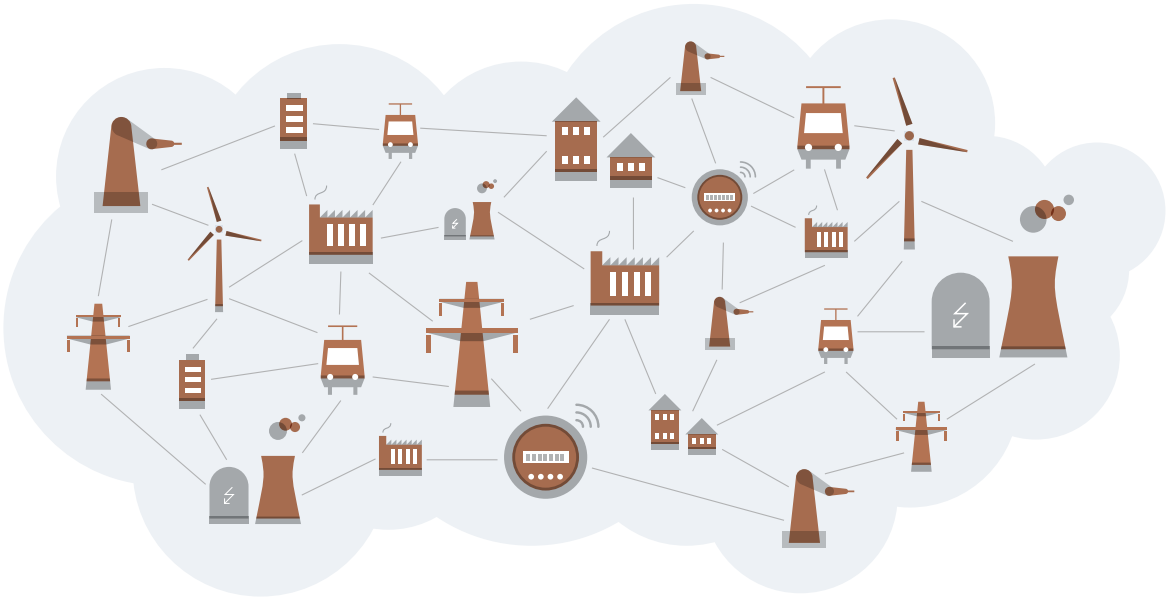
CONTENT LIST

II. INTERCONNECTEDNESS MEETS LACK OF VISIBILITY

Energy transmission and distribution networks consist of a large number of individual substations such as transformer stations, switchgear and renewable energy plants. Digitization and interconnectedness enable the remote control of substations, which are often distributed over large areas, via central control rooms. Access and control are provided via dedicated lines or VPN connections as well as local access points to the substation automation system for maintenance staff.

While interconnectedness and digital access points to substation automation systems have increased, the cybersecurity posture of protocols, systems and devices drag behind. At the same time, many operators still lack operational and cyber visibility of their Operational Technology (OT) networks to detect any wrong-doing – be it malicious or erroneous. And even though many substations are reasonably difficult to reach directly via the Internet, there are sufficiently effective ways for attackers to gain access:

1. vulnerable devices with outdated software are not uncommon in infrastructures whose device life cycle is designed for 25 years.
2. physical intrusions are especially effective in substations located far from the control room. Before an employee can verify the alarm on site, the attackers have long since caused disruption.
3. accessing the network and taking over authorized computers and accounts via:
   a phishing campaigns;
   b remote access (both of the company's own employees and of service providers);
   c third-party devices (e.g., from maintenance technicians, vendors, service providers).



III. ATTACK TECHNIQUES AGAINST OT NETWORKS AND ICS

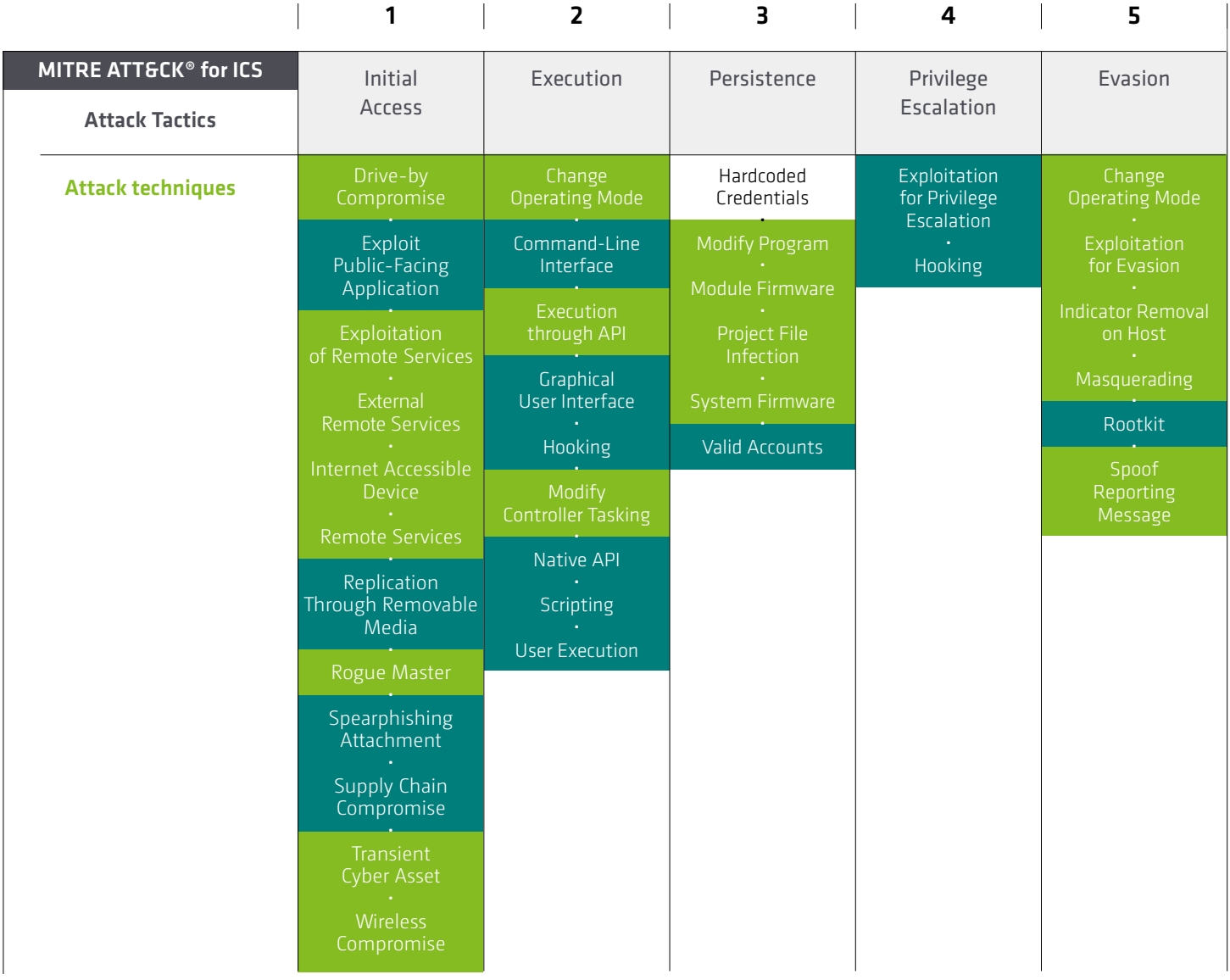
Targeted cyber attacks are rarely as simple structured as they are often portrayed in the media. State-sponsored, targeted attacks in particular – for example CRASHOVERRIDE, the Windows Exchange exploits by hacker group Hafnium and the SolarWinds[1] incident – follow a complex varied sequence of steps that often take months from initial access to disruption. This is best described by the MITRE ATT&CK®[2] framework that has become the most comprehensive resource for understanding attack techniques. MITRE ATT&CK® not only describes the single steps involved in an attack but also typical techniques. According to the MITRE ATT&CK® for ICS framework, security managers for OT networks face 12 attack phases (or tactics) encompassing at least 92 known techniques (see Figure 1)

The MITRE ATT&CK® framework illustrates how multi-layered cyberattacks can be. While many large-scale ransomware attacks are usually intercepted by firewalls, sophisticated attacks from Advanced Persistent Threats use a variety of methods to bypass established security measures. Since time is often not critical, the attack is incremental, cautious, and in stealth mode concealing activity from firewalls and traditional intrusion detection systems. We will illustrate how such an attack could take place on the following pages.

1 *In December 2020 cybercriminals had gained access to the infrastructure and even source code repositories of Microsoft (among others) using the Orion platform by IT service provider SolarWind as stepping stone*

2 *MITRE ATT&CK® https://attack.mitre.org/matrices/ics (last access: 10.01.2024) and MITRE ATT&CK® https://attack.mitre.org/matrices/enterprise (last access: 10.01.2024)*

Figure 1 *Adversaries have a large variety of tools at their hands. This adopted MITRE ATT&CK® for ICS matrix also shows which activities can be detected by the Rhebo network-based intrusion detection system (NIDS) from Landis+Gyr (as of Jan. 2024).*



continue on next page

6	7	8	9	10	11	12
Discovery	Lateral Movement	Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Network Connection Enumeration	Default Credentials	Adversary in the Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
	Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
	Valid Accounts	Man in the Middle		Data Destruction		Loss of Protection
		Monitor Process State		Denial of Service		Loss of Safety
		Point & Tag Identification		Device Restart/Shutdown		Loss of View
		Program Upload		Manipulate I/O Image		Manipulation of Control
		Screen Capture		Modify Alarm Settings		Manipulation of View
		Wireless Sniffing		Rootkit		Theft of Operational Information
				Service Stop		
				System Firmware		

IV. HOW TO DISTRUPT A SUBSTATION

From Reconnaissance to Delivery

The control room rarely communicates with the substations directly via the Internet. Usually, the exchange of data takes place via a dedicated landline or a VPN. A classic cyberattack is therefore unlikely (as long as it does not occur via the corporate IT). More likely for initial access is a supply chain compromise. The attackers first find out how the operator's ICS is structured, which devices are probably installed in the infrastructure (especially in the substation), which service providers have access to the equipment and which software is most likely in use. This information already provides sufficient access points.

For example, a Rhebo Industrial Security Assessment at a national energy distributor identified more than 1,600 devices from about two dozen manufacturers that were distributed and connected across more than 50 sites.

Subsequently, the attackers assess which subcontractor or vendor represents an easy and sensible target. The possibilities here range from the manufacturer of the control room software to PLC device or other OT component vendors (switches, routers) to the service companies that perform maintenance and configuration, among others.

A potential target for attackers could therefore be an SME service provider contracted to configure and maintain the substation equipment *(Supply Chain Compromise)*.[3] Via a phishing campaign, the laptop of a maintenance technician is infected with a malware whose target is a switch within the substation. The installed malware remains inactive as long as no contact is made with the target system. This route is effective specifically because of the high complexity and interconnectivity of systems.

When the maintenance technician connects his laptop to a substation switch, the switch is automatically infected with the malware. The malware is programmed to follow the »living off the land« approach. This approach aims to use native devices and tools that already exist in the infrastructure. Thus, the malware has a certain flexibility and can more effectively disguise its own activities (as they act natively). To do this, the malware uses a Powershell script *(Scripting)* to find and infect other potentially vulnerable devices *(Remote System Discovery)*.

One example is the SolarWinds incident in late 2020. Hackers had infected SolarWinds' Orion network management platform in order to access customer infrastructures. Organizations affected by this supply chain compromise included technology companies such as Microsoft and CrowdStrike, as well as several government agencies.

From Lateral Movement To Impact

A typical target in an OT infrastructure is a vulnerable SQL server that is used as a historian. As is often the case, it is accessed using a standard password *(Valid Accounts).*

The log data of most substation devices are managed on the historian. It is connected to many devices such as switches in the local ICS and also to the control room. This makes it an optimal beachhead. Automated scripts are used to identify and analyze the networked devices in the substation *(Network Sniffing, Automated Collection),* leveraging standard scripts and functions in the native DNP, IEC-61850 and OPC-DA protocols.

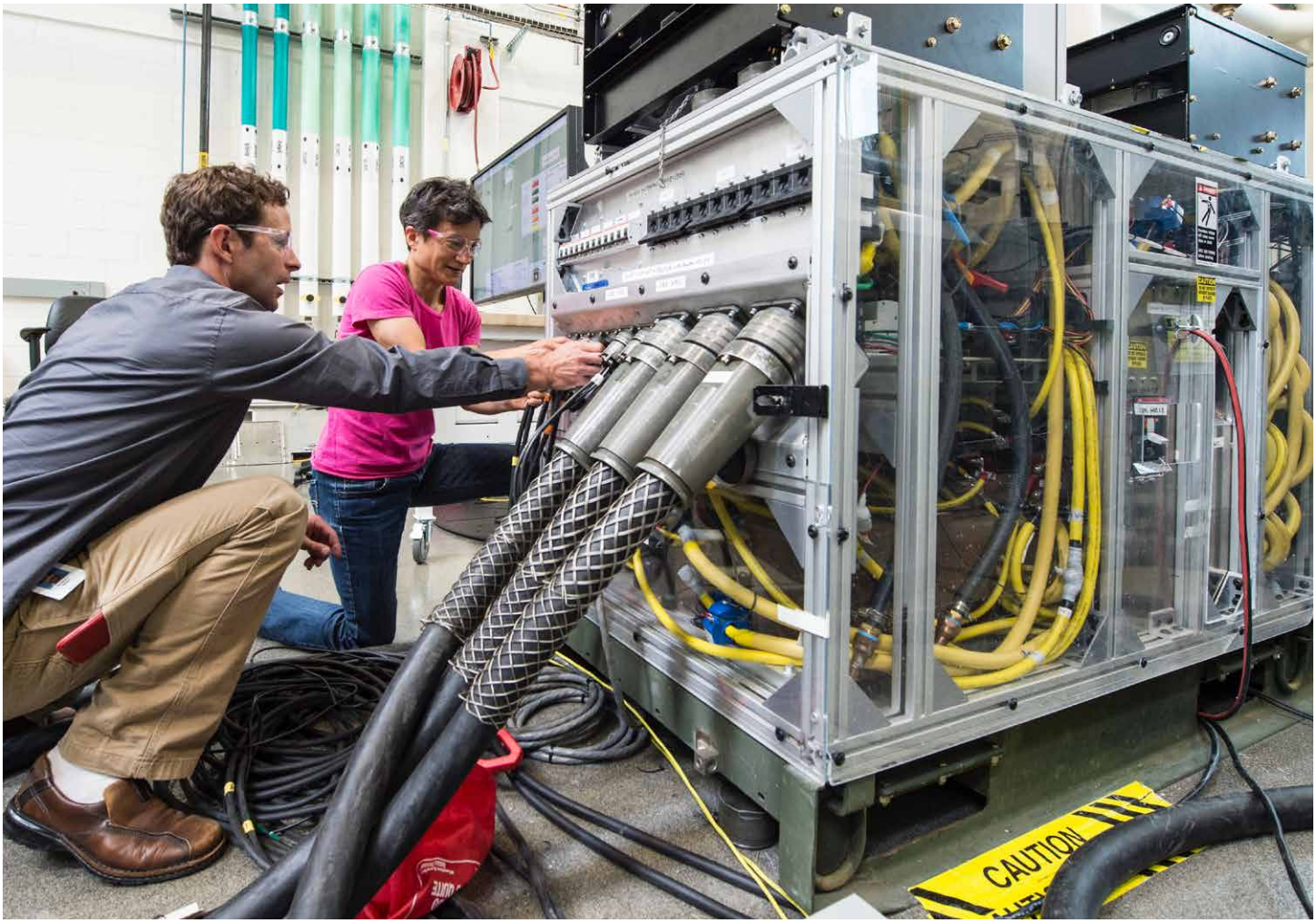
The beachhead gives the attackers access to the field level *(Valid Accounts).* Automated scripts are used to establish connections to the target systems – the relays – by exploiting the native protocol resources.

3 *The following italic brackets refer to the specific techniques according the MITRE ATT&CK® framework*

In the early morning hours, a timer in the malware triggers the payloads. This has two effects. First, the substation relays are completely opened and the power supply is interrupted *(Manipulation of Control, Loss of Availability).* Second, the security processes are stopped *(Alarm Suppression),* the readings are manipulated *(Spoof Reporting Message)* and access from the control room is blocked *(Loss of Control).*

The grid operator only becomes aware of the disruption when reports flood customer service the following minutes. The attempt to analyze the situation from the control room and to react fails due to the blocked access *(Loss of View, Loss of Control).* As an emergency measure, the substation is set to manual control and isolated from the rest of the network. This also prevents an overspill. It is only when a team of technicians reaches the substation that normal conditions can gradually be restored manually. For two hours, around 100,000 customers are affected by a partial blackout.

The (fictitious) attack described here is a relatively simple campaign that did not cause any major damage. The potential of such attacks was demonstrated a few years ago by the CRASHOVERRIDE incident, which is worth a second look.



V. THE CASE OF KYIV

The 2016 cyber attack on the Ukrenergo substation in Kyiv marks the first (known) cyber attack on an electric substation using OT-specific malware. The malware known as CRASHOVERRIDE or Industroyer was specifically programmed for the protocols used in European electric utilities: IEC 60870-5-101, IEC 60870-5-104, IEC-61850 and OPC. CRASHOVERRIDE was thus able to directly target and manipulate devices within the substation automation system. The attack stretched over an entire year from initial access to power outage, as the reconstructed timeline showcases, underlining the extensive resources the attackers had at hand.

JANUARY 2016

The attackers launched a large-scale spearfishing campaign, which helped establish the first access to the network of Ukrainian energy supplier Ukrenergo.[4]

FEBRUARY – DECEMBER 2016

The attackers presumably spied on the network, took over further accounts with administrator rights, consolidated remote access and laterally moved towards the substation's OT network.

1ST DECEMBER 2016

The attackers moved from corporate IT to the OT of a 330kV substation. In quick succession, several user accounts on the access server were modified, as well as two accounts with the names »admin« and »system« were newly created. They were assigned to the local domain, and privileges were delegated. The system's event logging was then turned off. These steps were completed in about a minute, showing the attackers' confidence and level of automation.

1–11 DECEMBER 2016

The attackers probably used this time to orient themselves in the substations OT network and identify vulnerable devices. Files were loaded into the substation automation system as .txt and renamed to .exe there via »move« command. Thus they bypassed the extension tracking of the firewalls. At scripting level, various VBS and BAT scripts were used to move data, browse the infrastructure and package PowerShell applications.

12–15 DECEMBER 2016

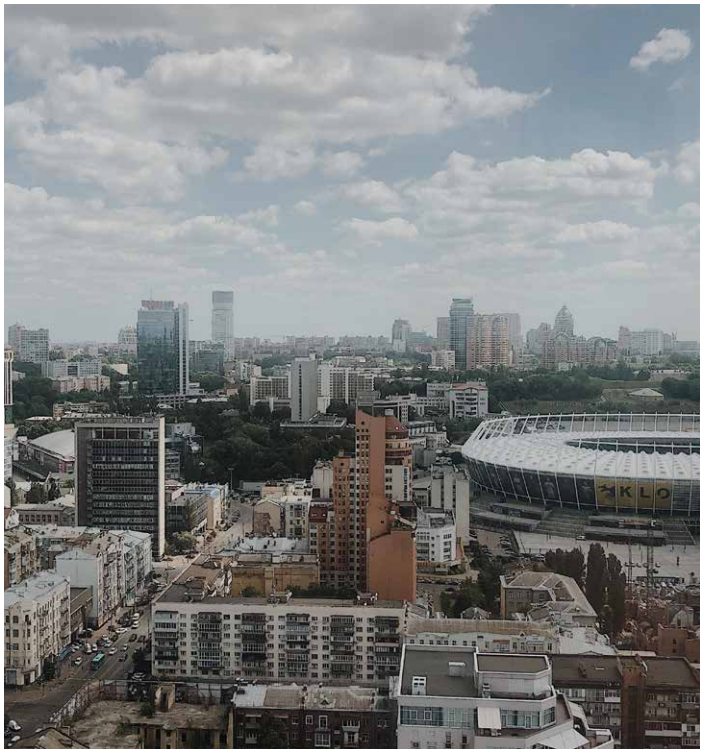
The attackers took over three Microsoft Windows Servers 2003, which were presumably used as historians and had high connectivity. They acted as beachheads[5], gaining code execution privileges on devices within the network. This was followed by a phase of information gathering (retrieval and listing of directories) and testing (connectivity to specific devices, authentication via RPC).

16 DECEMBER 2016

The CRASHOVERRIDE launcher was loaded onto the target system.

17 DECEMBER 2016

The payloads (in DLL format) were loaded onto the target devices in a protocol-specific manner, e.g. devices that used IEC 60870-5-104 received only the IEC 60870-5-104 payload module. The services in the malware were started manually and given a timer for automated payload execution in the evening. Two hours after execution, the wiper module started to cover all traces, crashing the system and preventing a restart. At this point, the control room at Ukrenergo had lost both view and control of the substation. They had to switch to manual operation for several months to reset the systems to normal operation and repair the infrastructure.



According to recent findings, the attack did not end at this point. Artifacts of a hybrid payload that combined functions for OPC and IEC-61850, and had a timer for December 20, 2016. indicate that the attackers aimed to disable the safety mechanisms of the switch gear. Fortunately, a coding error foiled the correct implementation. If successful, this step would likely have caused major equipment damage and jeopardized human lives.

The 2016 attack provides two lessons-learned:

1. Signature-based intrusion detection has limited ability to detect targeted attacks.
2. The control room needs full visibility in its substations to detect malicious behavior from the very start.

This requires continuous behavioral monitoring that analyzes communication across all 7 levels of the OSI model.

That way, even malicious events that occur via authorized channels or are otherwise invisible to classic signature-based detection systems can be detected at an early stage. An OT monitoring also supports the implementation of IEC-6235111[6] and IEC-6185012[7] standards relevant for energy companies.

4 *Joe Slowik Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE, 2018, Dragos Inc.*

5 *The beachhead ensures that access to the system remains possible even after a system reboot or reconfiguration.*

6 *Set of international standards for the security of energy management systems and their data transmission*

7 *Set of international standards for the automation of the energy sector*

VI. REAL-TIME 360° VISIBILITY FROM THE CONTROL ROOM TO THE SUBSTATIONS

Operators of power generation, transmission and distribution systems face the challenge of establishing an end-to-end system for intrusion detection. They must establish visibility across all operational systems and detect and report any form of threat (i.e. communication anomaly) in real-time. This includes substations in particular, because they are usually remotely controlled and far away from the control room. A rapid manual response to incidents at substations is therefore limited.

Landis+Gyr's Rhebo Industrial Security Assessments at customer sites as well as continuous OT monitoring using Landis+Gyr's OT network intrusion detection systems (NIDS) Rhebo Industrial Protector have revealed a wide range of anomalies and threats at energy companies.

These include:

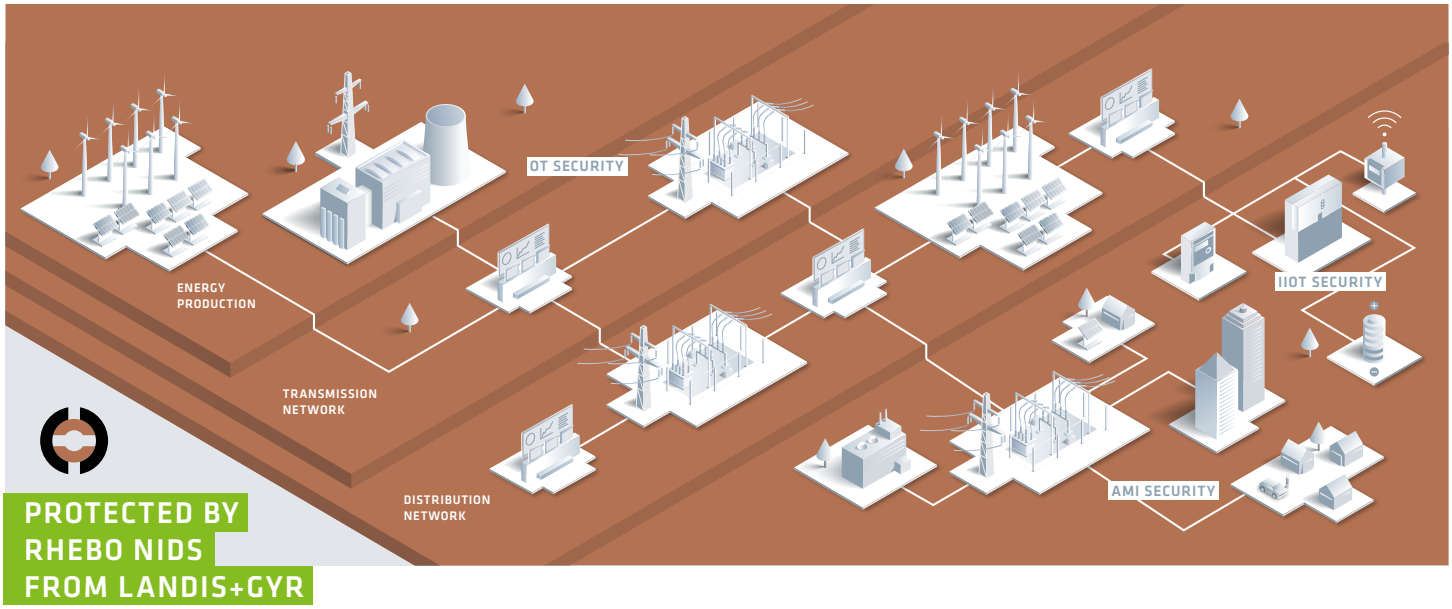
- new users in the OT;
- new protocols between devices;
- new connections between known users (e.g., from maintenance laptops);
- new connections to or from the control room;
- network scans;
- communication on unknown ports;
- unsuccessful access attempts;
- changes in time synchronization;
- use of SNTP;
- technical error states.

This multitude of anomalies highlights the urgent need for end-to-end visibility into the infrastructure. It also proves that the ability to detect communication that sometimes appears legitimate, takes place within the boundaries of OT networks, and is ultimately bypassing firewalls is key.

Landis+Gyr's Rhebo network intrusion detection system (NIDS) enables a scalable end-to-end OT monitoring of distributed industrial infrastructure with continuous threat detection. Communication changes occurring within the utilities, that indicate sophisticated cyberattack campaigns, malicious insider threats, scans and technical error states or malfunctioning devices get detected, evaluated, documented and reported to the control room in real-time. The use of deep packet inspection technology ensures that any changes to the authorized communication pattern are detected. This enables to identify malicious communication at an early stage, which either takes place via authorized channels (including administrator accounts) or uses other obfuscation tactics.

The sensors of the OT NIDS are integrated at critical points in the local infrastructure via non-invasive mirror ports or network taps. Anomaly reports are sent in real-time to the central Rhebo controller that can run isolated within the monitored substation or in the central control room. There, anomalies can be analyzed, localized and assessed on the basis of the forensic data and risk assessment provided, and countermeasures can be initiated. The threat detection system itself does not intervene in the industrial processes. The decision-making on how to deal with suspicious events rests entirely with the company's operational experts.

This enables to effectively prevent damage to substations and critical power infrastructure and to stop the attack from spreading to other locations or the control room.



VII. OT SECURITY IN 3 STEPS WITH LANDIS+GYR

1

OT RISK ANALYSIS AND VULNERABILITY ASSESSMENT

The first easy step to OT security:
Rhebo Industrial Security Assessment

Cybersecurity starts with visibility.

The Rhebo Industrial Security Assessment is an OT cyberrisk and vulnerabillity analysis that provides a deep understanding of your ICS / OT assets, risk exposure as well as recommendations for effective measures for hardening the systems.

You profit from

- the identification of all devices and systems within the OT including their properties, firmware versions, protocols, connections and communication behavior (Asset Discovery & Inventory);
- an in-depth analysis of existing CVE-documented vulnerabilities;
- the identification of risk exposure, security gaps and technical error states;
- a detailed audit report and workshop with actionable recommendations.

2

OT NETWORK INTRUSION DETECTION SYSTEM (NIDS)

The seamless transition to comprehensive OT security:
Rhebo Industrial Protector

Cybersecurity does not end at the network perimeters.

The NIDS Rhebo Industrial Protector combines OT monitoring with next generation OT threat and intrusion detection to detect anomalous communication within OT networks. It advances the existing perimeter firewall security by integrating OT-dedicated, network-based anomaly detection that reports security incidents in real-time while not interfering with the critical industrial processes.

You profit from

- real-time visibility of communication behavior of all OT and ICS assets (protocols, connections, frequencies);
- real-time reporting and localization of events (anomalies) that indicate cyberattacks, manipulation or technical error states;
- early identification of attacks via backdoors, previously unknown vulnerabilities and internal adversaries that firewalls fail to detect (defense-in-depth).

3

MANAGED DETECTION AND RESPONSE

The recipe to peace of mind.
We monitor so you don't have to:
Rhebo Managed Protection

Cybersecurity needs resources and know-how.

With Rhebo Managed Protection, we support you in operating the OT NIDS Rhebo Industrial Protector, in particular in evaluating and responding to incidents, as well as continuously reviewing and improving mitigation mechanisms.

You profit from

- expert support for running the OT NIDS;
- fast forensic analyses and assessment of OT security incidents;
- fast actionability in case of incidents;
- regular OT cyber risk analyses and vulnerability assessments for continuous improvement.

VIII. EASY INTEGRATION AND PROFESSIONAL MANAGED SERVICES

A particular challenge for power companies is to implement and manage cybersecurity across a large number of connected substations. This is made more difficult by the fact that substations rarely have personnel specifically dedicated to cybersecurity and OT device bugs and malfunctions.

For this reason, Landis+Gyr's OT NIDS Rhebo Industrial Protector can be installed not only as a hardware sensor in the local OT network. The OT monitoring is also available as a software sensor that can be directly integrated on various OT components that might already be in place. This includes several security gateways, edge computing devices, firewalls and substation servers, e.g.:

- Barracuda SecureConnector;
- Bosch Rexroth ctrlX AUTOMATION Plattform and IoT Gateway Protected Edge (PC PR21);
- Cisco IE4000 and IR829;
- NSYS icom MRO-L200, MRX-3 and MRX-5;
- RAD SecFlow-1v;
- SIEMENS Ruggedcom RX1400 and RX1500 with APE;
- Welotec IEC 61850-3 Substation Server;
- Paessler PRTG Network Monitor;
- WAGO Edge Computer & Edge Controller.

Additionally, security alerts can be easily forwarded to existing SIEM systems like Splunk and IBM QRadar. With these integration solutions, distribution system operators and transmission system operators combine several advantages of a modern digital automation architecture at the same time:

- process efficiency and automation;
- network condition monitoring;
- big data analytics;
- remote maintenance and comprehensive cybersecurity.

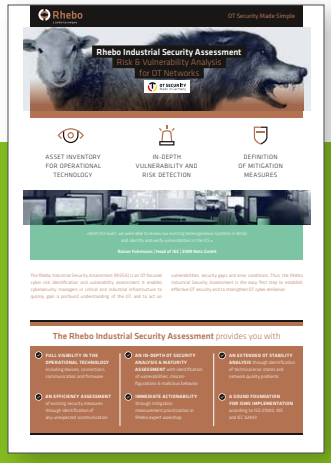
Additionally, the professional Managed Protection services by Landis+Gyr support energy suppliers and grid operators in analyzing, evaluating and combating anomalies detected and reported by Rhebo Industrial Protector in their OT. Depending on individual needs, service level agreements range from operational support to full managed services. This allows distribution system operators and transmission system operators to concentrate on their core business.

INTEGRATIONSPARTNER

IBM Security · splunk> · rexroth A Bosch Company · PAESSLER THE MONITORING EXPERTS · RAD Your Network's Edge® · WAGO · CISCO · Barracuda · WELOTEC · INSYS icom

EXPLORE LANDIS+GYR AND ITS RHEBO SECURITY PORTFOLIO FOR ELECTRICAL UTILITIES

Landis+Gyr's OT Security
Security for electrical substations, grids and utilities.



Rhebo Industrial Security Assessment
OT risk analysis and vulnerability assessment

Rhebo Industrial Protector
The network intrusion detection system (NIDS) for OT security

DOWNLOAD AT WWW.LANDISGYR.COM/SOLUTION/CYBERSECURITY

SECURE YOUR SUBSTATION CONTROL SYSTEM AGAINST CYBERATTACKS, MANIPULATION AND DISRUPTION

CONTACT US

WWW.LANDISGYR.COM/CONTACT | +1 855 3455 454

ABOUT LANDIS+GYR

Landis+Gyr is the leading global provider of integrated energy management solutions for the utility sector. Offering one of the broadest portfolios, we deliver innovative and flexible solutions to help utilities solve their complex challenges in smart metering, grid edge intelligence and smart infrastructure. With sales of USD 1.8 billion, Landis+Gyr employs approximately 5,600 people in over 30 countries across five continents, with the sole mission of helping the world manage energy better.

www.landisgyr.com/solution/cybersecurity

ABOUT RHEBO

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The German company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. Since 2021, Rhebo is part of the Landis+Gyr AG.

www.rhebo.com

Landis+Gyr & Rhebo 30000 Mill Creek Avenue, Suite 100 | Alpharetta, GA 30022 | USA