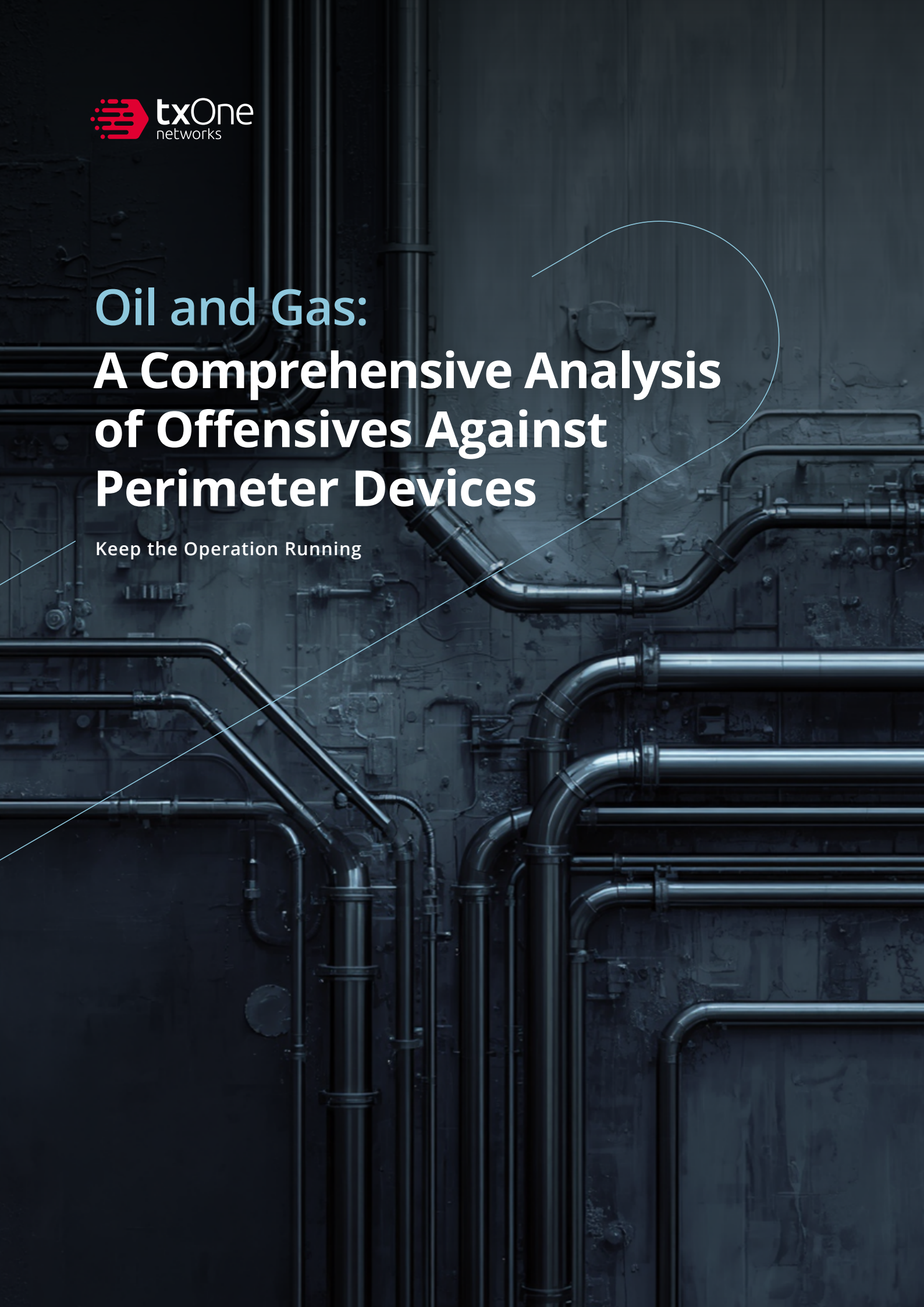

txOne networks

Oil and Gas:
A Comprehensive Analysis of Offensives Against Perimeter Devices

Keep the Operation Running

TXOne Networks

Oil and Gas:

A Comprehensive Analysis of Offensives Against Perimeter Devices

txOne networks

Oil and Gas:
A Comprehensive Analysis of Offensives Against Perimeter Devices

Table of Contents

Introduction

The Oil and Gas sector has long been a primary target for purpose-driven threat organizations. This industry is an indispensable cornerstone for all critical infrastructure sectors, supplying essential commodities such as fuel for power generation, transportation, and temperature control equipment for the telecommunications industry. Thus, it's highly susceptible to attacks from malicious actors that are seeking profit or state-sponsored attackers aiming to inflict damage on a national scale. A disruption in the stable supply chain of oil and gas can not only jeopardize the health and welfare of citizens but also bring the nation's economy to a grinding halt.

The Middle East, which is the world's largest crude oil exporting region, has continuously been the victim of extensive targeted cyberattacks. Since 2010, infamous malware such as Stuxnet, Flame, and Mini-Flame have been identified as attacking its key infrastructure. Additionally, Shamoon and Triton have significantly impacted the Middle Eastern oil sector. In 2012, Saudi Aramco, the world's leading daily crude oil producer, fell victim to the Shamoon malware attack, incapacitating over 30,000 workstations for a week. Moreover, the Triton malware targeting the Middle East's oil sector marked the historically unprecedented instance of a direct assault on a safety instrumentation system (SIS). This is a system which monitors whether factory processes remain within operational parameters and triggers alarms when potentially risky situations arise, ensuring factories return to a safe state. Should such a system be compromised, this can halt operations or cause the factory to run without crucial safety measures.

Review of Cyberattack Incidents in Critical Infrastructure

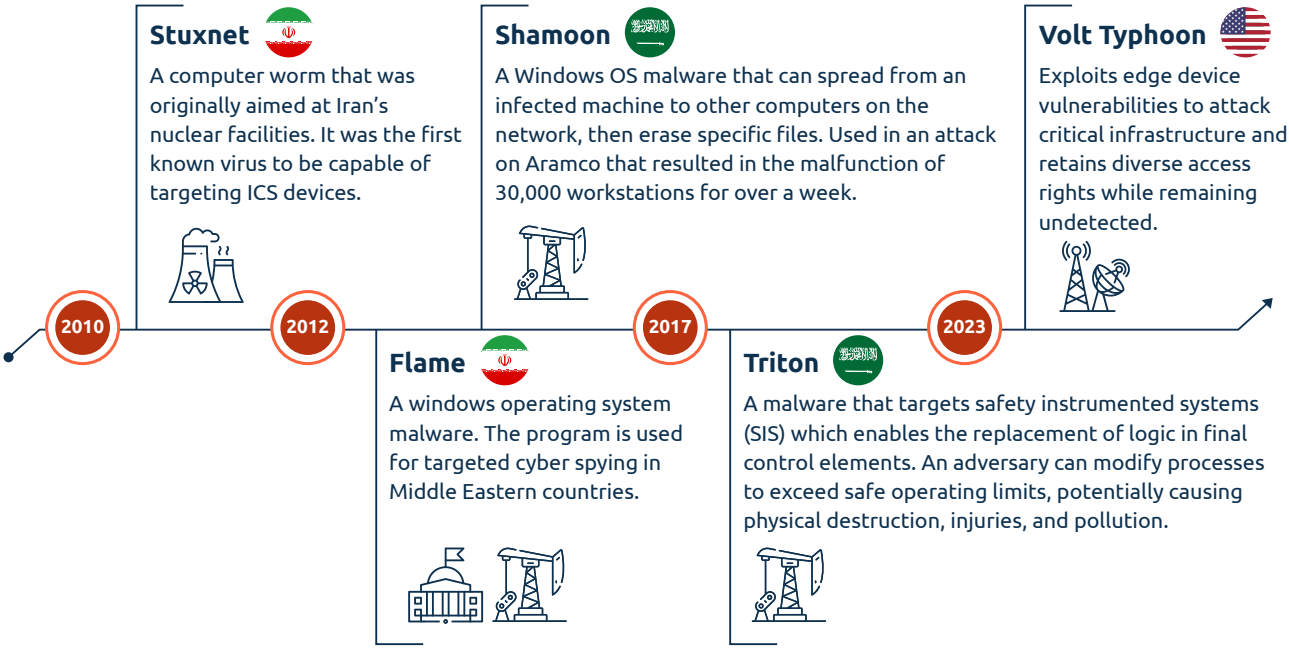

Figure 1: Cyberattack Incidents in the Critical Infrastructure Sector

From Figure 1, it's evident that highly targeted attacks against Middle Eastern critical infrastructure persist. Delving deeper into these attack methodologies, we discovered that these adversaries capitalize on vulnerabilities in internal assets or insecure configurations to perform lateral movements, aiming to inflict ever more widespread and extensive damage. In 2023, the Volt Typhoon group ingeniously leveraged low-profile SOHO edge devices as relay points, systematically penetrating the internal networks of essential infrastructures and maintaining covert operations for up to two years. Such alarming tactics raise pressing concerns. As the oil and gas industry gradually digitalizes, is it inadvertently offering attackers potential points of initial compromise? This could potentially pave the way for large-scale attacks within Industrial Control System (ICS) environments leveraging zero-day exploits. Drawing on the Stuxnet, Triton, and Volt Typhoon incidents as case studies, Figure 2 illustrates that once attackers infiltrate critical infrastructure's internal networks, they can consistently deploy weaponized tools to cause lasting damage to the environment.

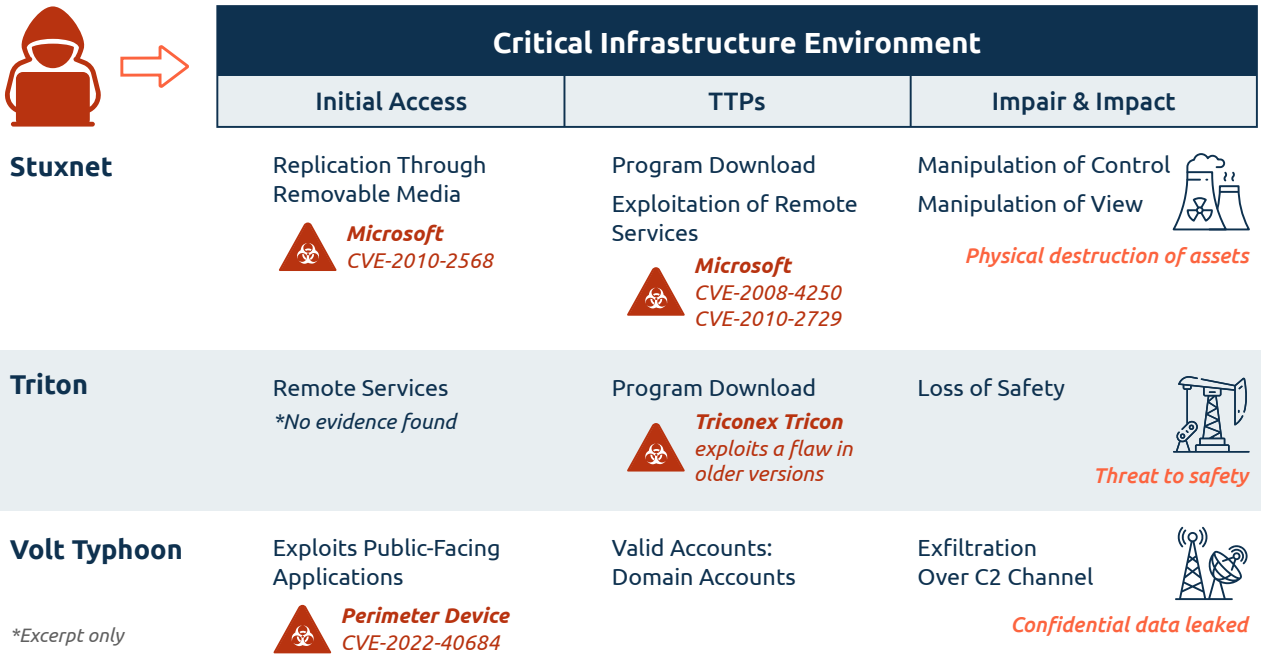

Figure 2: Attacks via Asset Vulnerabilities or Insecure Configurations

It is widely recognized that, compared to IT environments, OT (Operational Technology) environments often struggle with timely updates of known vulnerabilities. Consequently, understanding how attackers can move from external vectors to internal networks and evaluating mitigation strategies is imperative for OT environment stakeholders. Through this whitepaper, readers will gain insights into:

- The digital ecosystem of the oil and gas industry and the associated technologies employed.
- Methodologies through which attackers can exploit these technologies to initiate breaches.
- How attackers can leverage asset vulnerabilities or insecure configurations to further compromise the oil and gas industry.
- Strategies that OT environment owners can adopt to mitigate both external and internal threats.

Overview of the Oil and Gas Industry Ecosystem

In general terms, the oil and gas industry can be segmented into upstream, midstream, and downstream operations.

The upstream segment, also known as the exploration & production sector, focuses on the exploration and production of crude oil and natural gas. Production involves extracting these natural resources from either terrestrial or subsea sources. This process is inherently high-risk, not just due to the challenging environments but also the astronomical costs of drilling equipment. The capital outlay can only be justified once the extraction has been proven successful.

Midstream operations encompass the transportation and storage of oil and gas. While transportation using surface or maritime vehicles is straightforward, using vast networks of pipelines is also a standard approach. Governments typically seek equilibrium between their reserves and domestic energy requirements.

Downstream operations typically refer to refining crude oil, the processing and purifying of natural gas, and marketing and distributing the finished products. This segment represents the final stages of delivering petroleum and natural gas to consumers. Take oil refining, for instance: different petroleum products have distinct boiling points, so crude oil is heated at the bottom of a distillation chamber until all components vaporize and rise within the chamber. Equipment then collects the various petroleum products.

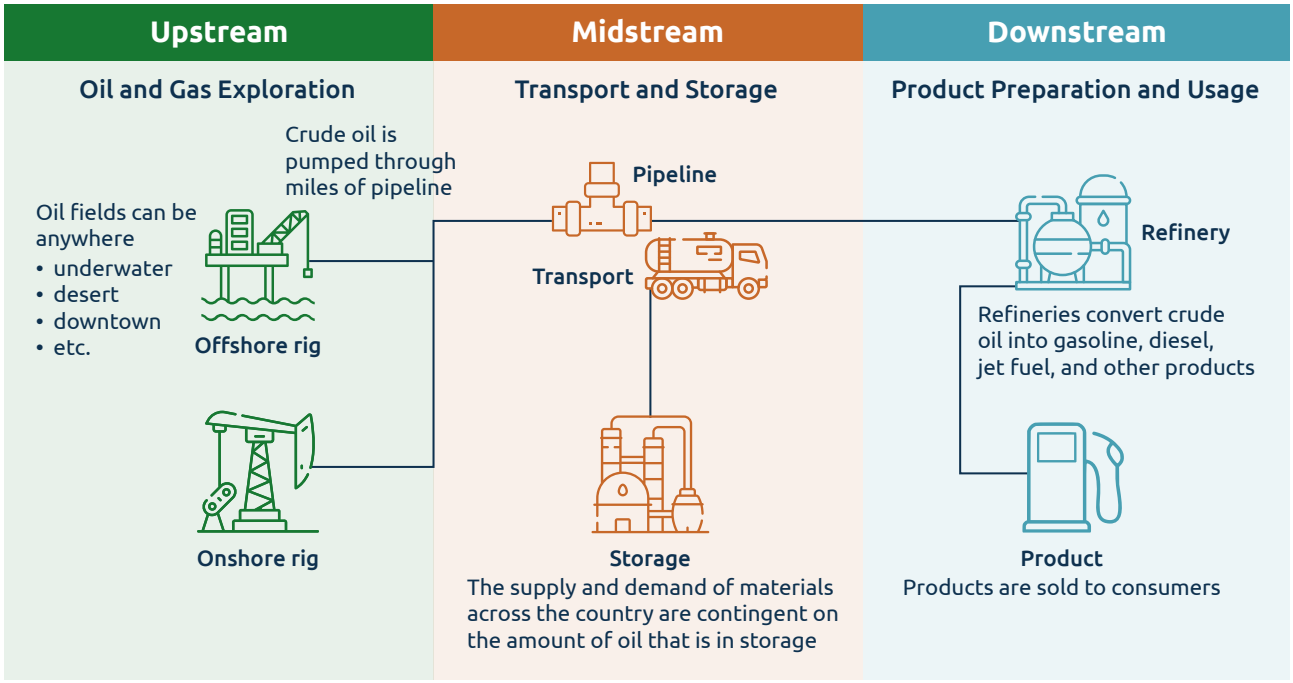

Figure 3: Oil and Gas Industry Ecosystem

According to a report by CISA on the energy sector,[1] the oil industry, given its global nature, is faced with a diverse risk landscape. Beyond geographical concerns, its operations may span multiple jurisdictions, including overseas. Thus, the primary risks faced by the oil and gas industry are:

- Natural disasters and extreme weather events.
- Regulatory and legislative shifts—particularly in environmental and health sectors—along with the rising cost of compliance.
- Unpredictable fluctuations in oil and gas prices and demands.
- Operational perils, including blowouts, spills, and personal injuries.
- Disruptions stemming from political instability, civil upheaval, or terrorist actions.
- Transportation infrastructure limitations hampering resource movement.
- Inadequate or unavailable insurance provisions.
- Aging infrastructure and an aging workforce.
- Cyber threats, most notably insider risks.

When we analyze these risks alongside historical cyber incidents, it becomes clear that cyberattacks directed at the oil and gas industry are frequently carried out by threat actors with political affiliations, insurgent backing, or ties to terrorist entities. Successful exploitation could escalate to threats at the national economic level and result in environmental degradation, and the well-being and health of citizens being put in jeopardy. Additionally, the oil and gas industry remains a prime target for purpose-driven adversaries due to its interdependence with other critical infrastructure sectors, as depicted in Figure 4.

(Sub) sector Generating the Service	ONG	Electricity	Transportation	Water	Communication
ONG	N/A	Fuel to operate power plant motors and generators	Fuel to operate transport vehicles	Fuel to operate pumps and treatment	Fuel to maintain temperatures for equipment; fuel for backup power
Electricity	Electricity for extraction and transport (pumps, generators)	N/A	Power for overhead transit lines	Electric power to operate pumps and treatment	Energy to run cell towers and other transmission equipment
Transportation	Delivery of supplies and workers	Delivery of supplies and workers	N/A	Delivery of supplies and workers	Delivery of supplies and workers

Water	Production water	Cooling and production water	Water for vehicular operation and cleaning	N/A	Water for equipment and cleaning
Communication	Breakage, leak detection and remote control of operations	Detection and maintenance of operations and electric transmission	Identification and location of disabled vehicles, rails and roads; the provision of user service information	Detection and control of water supply and quality	N/A

Figure 4: Interdependence Among Critical Infrastructure Sectors

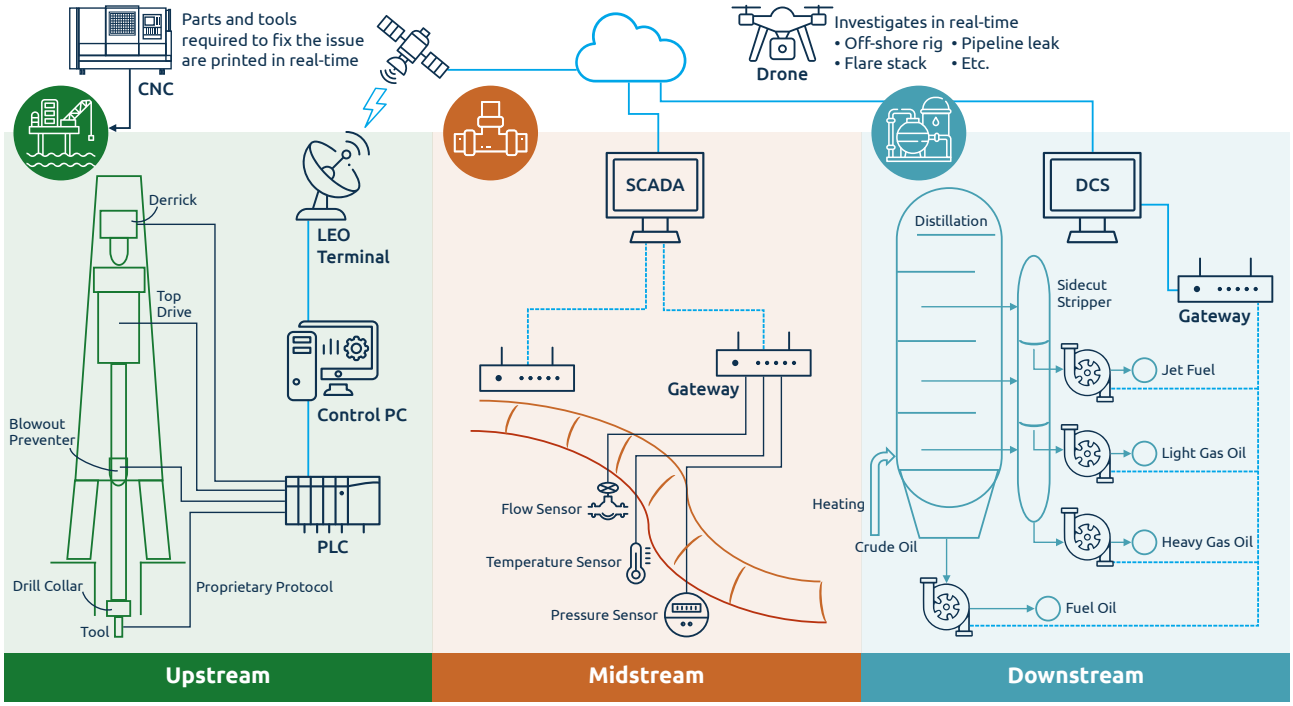

Figure 5: Digitalized Oil and Gas Industry

Referring to Figure 5, we can see that sensors and controllers associated with rigs, pipelines, or distillation in OT environments frequently seek connections with external networks. This connectivity facilitates comprehensive analysis for decision-makers in response to market dynamics, policy shifts, and environmental changes. The modes of OT external connections include:

- **OPC:** Among IT-OT interoperability, OPC UA stands out as one of the most frequently adopted standardized communication protocols across various industries. Within the oil and gas sector, the OPC Foundation collaborates with the Drilling Systems Automation Technical Section to utilize OPC UA as their standard protocol for communications throughout the drilling process. For instance, Equinor, an international energy company headquartered in Norway, extensively incorporates OPC UA into their drilling platforms.[2]

- **LEO Terminal:** Considering that rigs and pipelines are often located in remote areas, maintaining network connectivity becomes crucial. Digitalized oil and gas operations turn to LEO (Low Earth Orbit) technology capable of comprehensive global coverage to maintain a line of sight with their equipment. In OT domains, essential data is collated via controllers and dispatched to LEO for subsequent external utilization. Conversely, the Terminal can receive signals from LEO to relay commands to controllers. For example, an offshore oil platform in Senegal connects to its headquarters in the Netherlands through this technology. SAIPEM, an offshore drilling and pipeline construction company, employs this approach for seamless connectivity between its expansive fleet and onshore bases.[3]

- **SOHO Devices:** Here, SOHO broadly refers to hardware devices that route data from one LAN to another network. Amid IIoT (Industrial Internet of Things) proliferation, we observe myriad instances of site devices connecting to other networks. A salient example in the digitalized oil and gas sector involves 'digital twin' technology, collecting relevant data from physical asset sensors into a centralized data repository to craft 3D models. This repository often facilitates inter-departmental data sharing, including engineering, procurement, and operations—necessitating SOHO devices for routing. The technology leverages operational data and historical records for predictive behavior analytics. Pan American Energy, an Argentinian oil and gas enterprise, leverages digital twin technology in refineries to optimize the lifespan of physical assets.[4] [5]

Furthermore, our observations have indicated several prevailing technologies within the digital transformation journey of the oil and gas industry, such as:

- **CNC and Industrial Robots:** In the upstream sector, adapting to extreme natural conditions often necessitates specialized tooling solutions. Consequently, CNC (Computer Numerical Control) machinery is invaluable because it allows for the real-time fabrication of critical components and tools tailored to address specific challenges. Similarly, given the high-risk nature of oil drilling operations, innovative solutions are paramount for enhancing safety and efficiency. For instance, Transocean, a leading offshore drilling contractor, leveraged FANUC's industrial robotics capabilities to devise an automated solution that manages drilling riser connections, traditionally one of the most labor-intensive operations.[6]

- **Inspection Robots:** The vast, remote, and often treacherous terrains that characterize the oil and gas industry — whether upstream, midstream, or downstream — necessitate cutting-edge monitoring solutions. Inspection robots have become indispensable tools, aiding in the timely detection of anomalies in physical assets or the operational environment. These state-of-the-art robots are often equipped with high-definition cameras, thermal imaging capabilities, or LIDAR (Light Detection and Ranging) sensors to capture a broad spectrum of data. Drones, for example, have become the go-to solution for many complex inspections. A notable application is by Sinopec, China's leading oil and gas company, which utilizes Microdrones drones for routine inspections across its extensive pipeline network spanning over 6,000 kilometers.[7]

Threat Terrain of the Digitalized Oil and Gas Industry

Traditionally, the oil and gas industry has protected its Operational Technology (OT) environments from external cyber threats through network isolation. This strategy required OT stakeholders to merely uphold compliance with internal procedures and safeguard against internal threats to deter the majority of cyberattacks. However, with the advent and advantages of interconnected technologies, the oil and gas industry inevitably adopted digital solutions for valuable real-time analysis and surveillance, enhancing operational and production efficiencies to keep pace with competitors. A unique challenge for oil extraction is its occurrence in remote or inaccessible locations, with pipelines often extending for miles. Historically, long-distance communication for monitoring equipment was facilitated through dedicated networks. But today's interconnected trend results in inter-device dependencies, potentially expanding the attack surface and the consequential impact of a breach.

Upstream

As depicted in Figure 6, rigs in remote areas frequently utilize LEO (Low Earth Orbit) technology for consistent external communication due to its low latency, radiation, and cost. However, since LEO connectivity is IP-based and lacks stringent security checks, it becomes vulnerable. If adversaries intercept its signal, data tampering becomes all too easy. Additionally, terminals supporting LEO services have been found susceptible to password breaches and unrecorded backdoor vulnerabilities, allowing attackers potential access to upstream control networks. For instance, if a CNC machine is tricked into consistently producing flawed tools, significant drilling investments could be compromised. Similarly, a malfunctioning industrial robot during drilling riser connections might result in riser damage, or worse, compromise the seal integrity of the well.

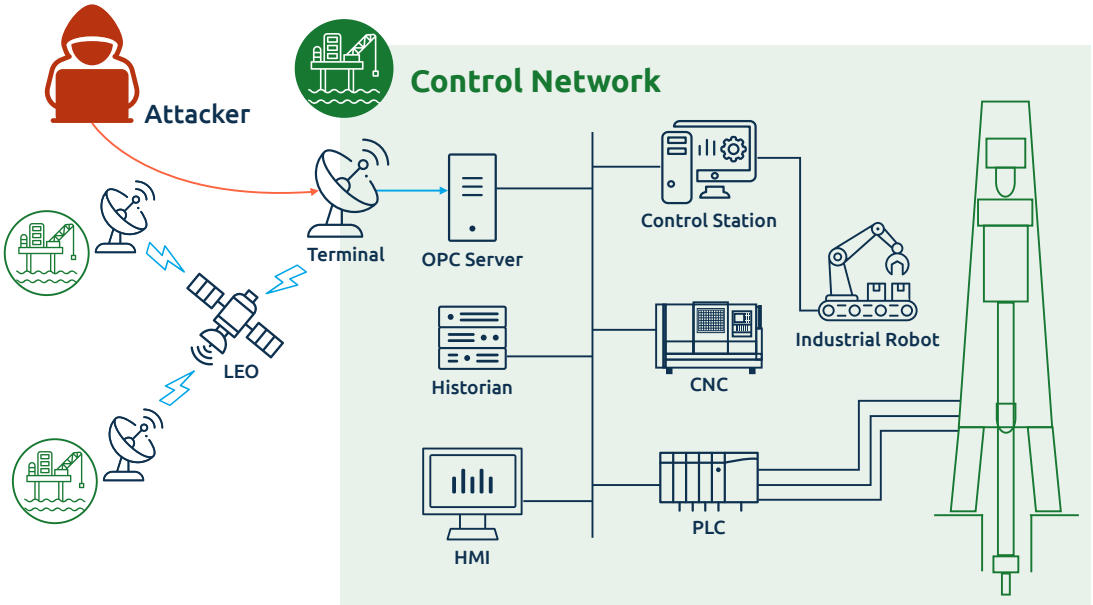

Figure 6: Initial Access Attack Surface of Upstream

Midstream

Illustrated in Figure 7, pipelines require continuous monitoring to maintain the stability of oil and gas transport, whether they are in remote or accessible locations. Remote segments might leverage LEO for sensor data transmission, while other areas predominantly employ gateways that transmit via LTE or MQTT. However, these SOHO (Small Office/Home Office) devices, crucial in the IIoT (Industrial Internet of Things) landscape, often present vulnerabilities due to poor configurations. The 2023 unveiling of the Volt Typhoon group using compromised SOHO devices to infiltrate critical infrastructure was a revelation that illustrates this type of risk. Late detection of oil and gas leaks could culminate in environmental catastrophes, given the challenge of frequent manual pipeline inspections.

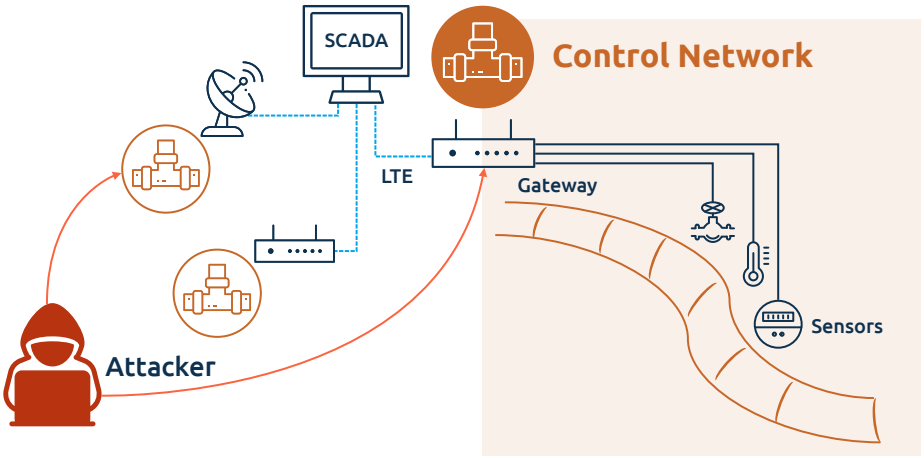

Figure 7: Initial Access Attack Surface of Midstream

Downstream

Highlighted in Figure 8, the digital convergence of IT and OT is increasingly vital in refineries. This includes real-time or historical operational data transmission to business domains or integration with other petrochemical plants. One common approach is using OPC (OLE for Process Control) for standardized IT-OT communication. In attempts to prevent infiltration by external parties, OPC offers a trust list mechanism. However, implementing this in OT presents complexities. Inadequate configurations could grant attackers direct access to field devices, akin to the infamous Stuxnet malware, triggering unsafe operational behaviors and potential shutdowns.

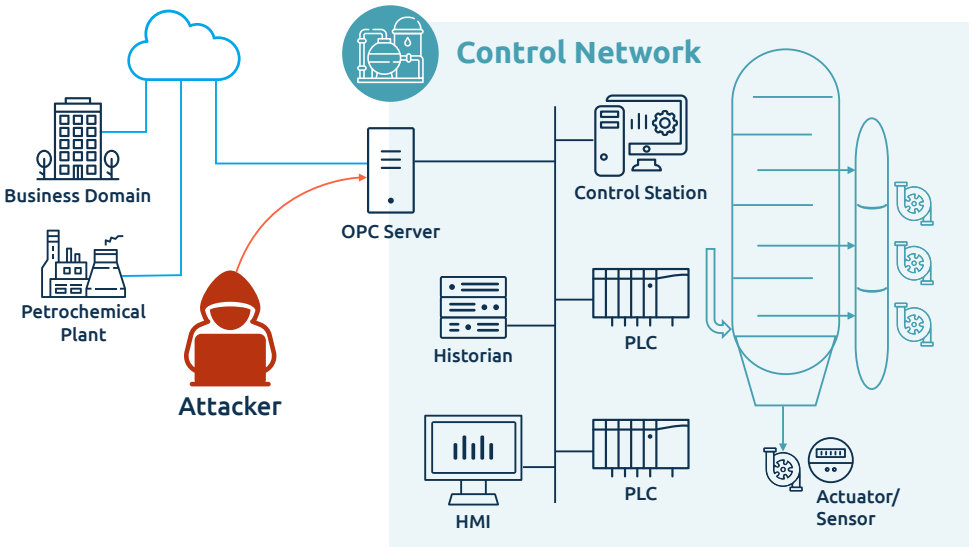

Figure 8: Initial Access Attack Surface of Downstream

In-Depth Asset Analysis

Analysis of LEO Terminal Vulnerabilities

There are seven primary methods of satellite communication available on the market:

- **Inmarsat-C:** Predominantly a maritime communication system, Inmarsat-C facilitates ship-to-shore, shore-to-ship, and ship-to-ship communication. Its versatile store-and-forward mechanism allows telex, fax, data, or email functionalities, which is very useful.
- **VSAT (Very Small Aperture Terminal):** VSAT systems, typically operating at the C-band and Ku-band, are employed for the transmission of data, video, or voice using satellite transponders.
- **BGAN (Broadband Global Area Network):** This global satellite internet and voice network is enhanced with built-in security features, making it apt for sensitive military operations.
- **BGAN-M2M:** Designed for long-term machine-to-machine (M2M) management of fixed assets, this global, two-way IP data service is extensively used in the Industrial Control Systems (ICS) landscape and for SCADA applications, emphasizing its significance in real-time data transmission.
- **FB (FleetBroadband):** An IP-based broadband data and voice maritime satellite system developed by Inmarsat-C or FB, FB is pivotal for both operational and crew communications. Vital navigation systems like the Electronic Chart Display and Information System (ECDIS) often depend on the seamless data connection this service offers.
- **SwiftBroadband:** A broadband data and voice aeronautical satellite system rooted in IP, SwiftBroadband is sanctioned by the International Civil Aviation Organization (ICAO) for aircraft safety services, substantiating its role in Future Air Navigation Systems (FANS).
- **Classic Aero Service:** A comprehensive aeronautical satellite communication system by Inmarsat-3 or Inmarsat-4, it supports voice, fax, and data functionalities. Some of its services include AeroH(+), AeroI, and Mini M Aero, among others.

Different industries deploy various methods tailored to their specific needs. For instance, military operations and government emergency services predominantly utilize BGAN, BGAN-M2M, and VSAT. Public transportation systems, such as GPS, employ IRIS and GNSS. The oil and gas sector, on the other hand, predominantly harnesses BGAN-M2M for its remote operations. In the context of oil and gas, besides the previously mentioned rigs and pipelines, numerous related remote operations also leverage this technology, as illustrated in Figure 9.

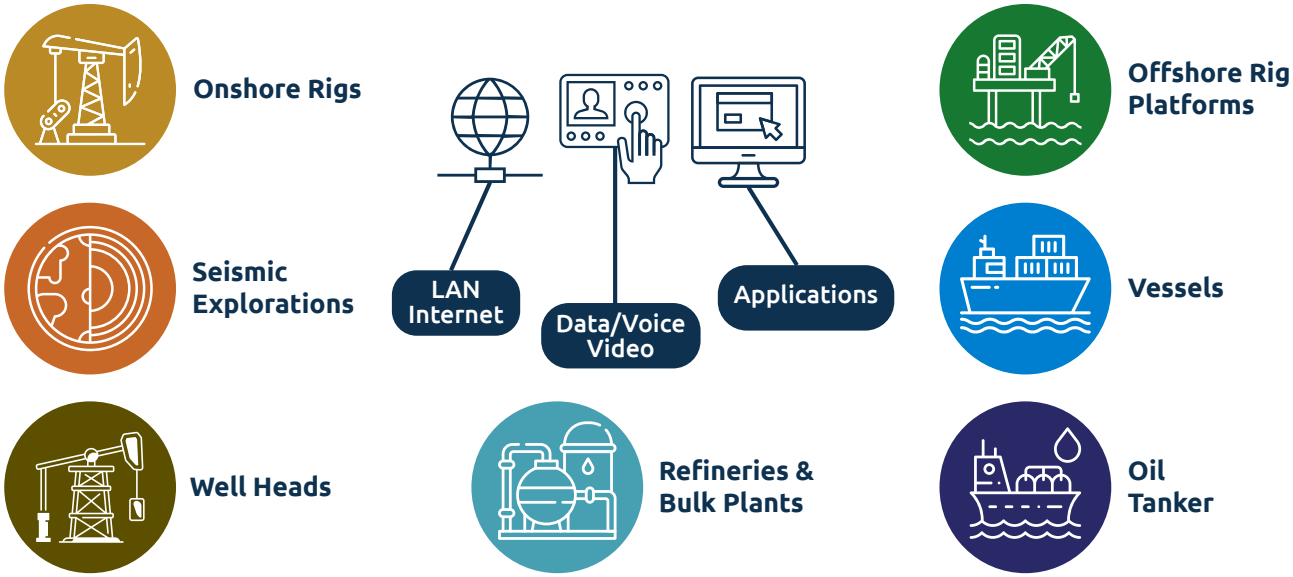

Figure 9: Remote Processes in the Oil and Gas Industry [8]

Table 1 enumerates known vulnerabilities associated with common LEO terminal brands, along with their frequently adopted industries.[9] From this table, one can discover that the vulnerabilities inherent in these products bear similarities to those found in less sophisticated Internet of Things (IoT) devices. Predominant among these vulnerabilities are issues related to authentication, communication protocols, and backdoor access. This implies that the integrity and confidentiality of these terminals, serving as interfaces between the control network and external communication, are severely compromised.

Table 1: Terminal Vulnerabilities by Products

Vendor	Product	Vulnerabilities	Service	Industry
Harris	• RF-7800-VU024 • RF-7800-DU024	• Hardcoded Credentials • Undocumented Protocols • Insecure Protocols • Backdoors	• BGAN	• Military • Emergency Services
Hughes	• 9201/9202/9450/9502	• Hardcoded Credentials • Undocumented Protocols • Insecure Protocols • Backdoors	• BGAN • BGAN M2M	• Military • Emergency Services • Energy
Cobham	• EXPLORER	• Weak Password Reset • Insecure Protocols	• BGAN	• Military • Emergency Services

Vendor	Product	Vulnerabilities	Service	Industry
Cobham	• SAILOR 900 VSAT	• Hardcoded Credentials • Weak Password Reset • Insecure Protocols	• VSAT	• Military • Emergency Services • Media
Cobham	• AVIATOR 700 (E/D)	• Hardcoded Credentials • Weak Password Reset • Insecure Credentials • Backdoors	• SwiftBroadband • Classic Aero	• Aerospace
Cobham	• SAILOR FB 150/250/500	• Weak Password Reset • Insecure Protocols	• FB	• Maritime
Cobham	• SAILOR 6000 Series	• Hardcoded Credentials • Insecure Protocols	• Inmarsat-C	• Maritime
JRC	• JUE-250/500 FB	• Hardcoded Credentials • Undocumented Protocols • Insecure Protocols • Backdoors	• FB	• Maritime

As of research conducted up to 2023, it is evident that most LEO device infrastructures lack rigorous security checks, which can primarily be attributed to lower transmission speeds. The mainstay of their validation is CRC (Cyclic Redundancy Check) for packet integrity. Furthermore, they predominantly utilize network protocols such as POP3, SMTP, Pure HTTP, TCP, and FTP. According to a study by Oxford University,[10] attackers could potentially intercept and alter the transmitted data without needing state-of-the-art-equipment, leading to malicious abuse of the control network, as illustrated in Figure 10.

Even with the emergence of Starlink technology (comprising over 5,000 LEO satellites as of August 2023), which offers faster packet transmission speeds enabling users to opt for secure connections like HTTPS, there are challenges. When compared to traditional LEOs, Starlink's cost and locational support limitations pose significant hurdles given the diverse geographic landscape of the oil and gas industry.

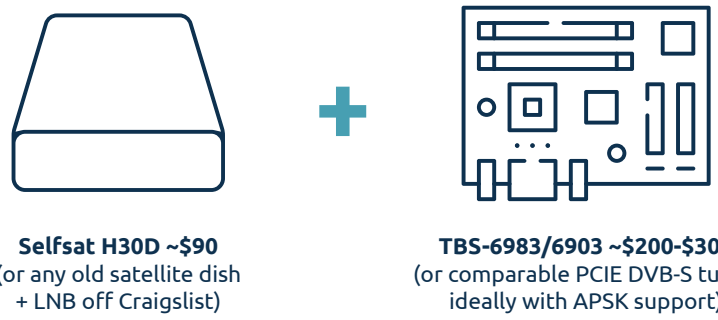

Figure 10: Oxford PhD student James Pavur used a Selfsat satellite dish and a TBS-6983/6903 PCIe card to achieve satellite eavesdropping for around $300

Taking the Hughes BGAN M2M Terminals,[11] which are applicable to the oil and gas sector, official operating documents state that operators can send commands to the device through an IP pipeline. This means that if an attacker manages to access the device due to insecure network configurations, they could potentially exploit vulnerabilities like hardcoded credentials or backdoors mentioned in Table 1. Such unauthorized access grants them control over the device, paving the way for a range of potential outcomes, including data spoofing and physical damage to the control network.

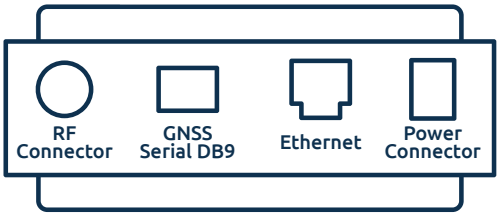

Figure 11: BGAN M2M Terminal

In-Depth Analysis of Asset Security in OPC UA

Let's consider OPC UA, one of the most prominently used standardized protocols that unify IT and OT environments. This protocol embodies both client/server identities and utilizes a publish/subscribe mechanism. The server acts as a management agent for subscriptions between clients. Clients can disseminate data to other clients subscribed to a particular topic by publishing said data. To thwart external intrusions into the control network, OPC UA's standard has devised an authentication mechanism. As illustrated in Figure 12, this includes settings for Anonymous, Password, and Certification.

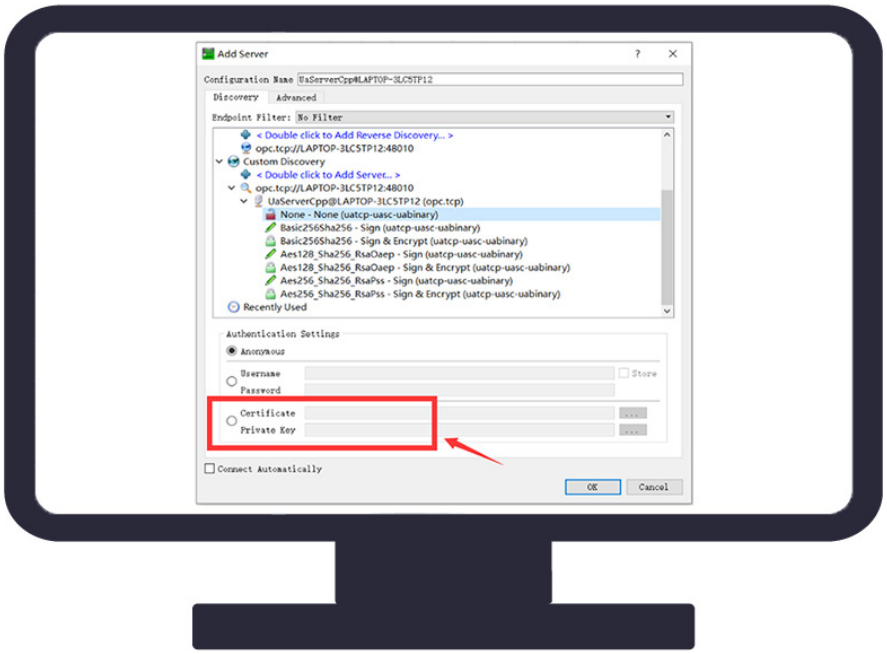

Figure 12: The OPC UA Authentication Mechanism

A trust list only allows clients with legitimate certifications to connect. Though leveraging a trust list offers security, the numerous field devices in OT's control network in combination with network segmentation pose a challenge for administrators in manually updating all machine credentials simultaneously. Recognizing this, administrators might employ the OPC-GDS (Global Discovery Server) for certificate management. By this method, they only need to add/delete certificates on the GDS to update all OPC servers. However, the GDS's need for an internet connection to obtain the root CA conflicts with the traditional OT environment's network isolation principle. As such, not all OPC UA products support this service.

According to research from Saarland University Germany,[12] seen in Table 2, aside from most OPC UA products not supporting the GDS mechanism, there are also glaring security issues related to the trust list in many products.

Table 2. OPC UA Products

Vendor	Platform	OPC Certification	Pub-Sub	GDS	Security	Trust List	Recommended Policy
B&R	ADI OPC UA	●	○	○	●	●	Not specified
Bachmann	OPC UA Client/ Serv.	○	○	○	△	△	Not specified
Beckoff	TC3 OPC UA	○	○	○	△	△	Deprecated protocols
Beijer	iX Developer	○	○	○	○	○	None
Bosch Rexroth	ctrlX CORE	○	○	○	●	△	Security mode not supported
General Electric	iFIX	○	○	●	●	△	Basic256Sha256
Honeywell	ControlEdge Builder	○	○	○	○	○	None
Lenze	Easy Starter	○	○	○	△	△	Deprecated protocols
Mitsubishi	MX Configurator-R	●	○	○	●	●	None
National Instr.	InsightCM	○	○	○	●	●	None
Omron	SYSMAC-SE2	●	○	○	●	●	Not specified
Panasonic	HMWIN Studio	○	○	●	●	△	Not specified
Rockwell	Factory talk linx	○	○	○	●	●	Not specified
Schneider	Control Expert	●	○	○	●	●	Basic256Sha256
Siemens	STEP 7	●	○	●	●	△	Not specified
Weidmüller	u-create studio	○	○	○	●	●	Basic256Sha256
Yokogawa	SMARTDAC+	○	○	○	○	○	None
Codesys-based Platforms							
Codesys	Codesys V3.5	○	●	○	●	△	Not specified
ABB	Automation Builder	○	●	○	●	△	Basic256Sha256
Eaton	XSOFT-CODESYS	○	○	○	●	△	Not specified
Hitachi	HX Codesys	○	○	○	●	△	Not specified
Wago	e!cockpit	●	○	●	●	△	Not specified

Concerning trust list issues, OPC UA products primarily suffer from the following:

Missing Support for Trust List Design:

Products in this category lack operational guidelines for deploying trust lists. Even enabling the trust list in the user interface doesn't result in certificate validation, as seen in Figure 13. This misconception would lead administrators to erroneously believe they are in a secure environment, allowing attackers without valid credentials to directly publish/subscribe to topics and access field device data - a risk far greater than explicitly stating that the product doesn't support this feature.

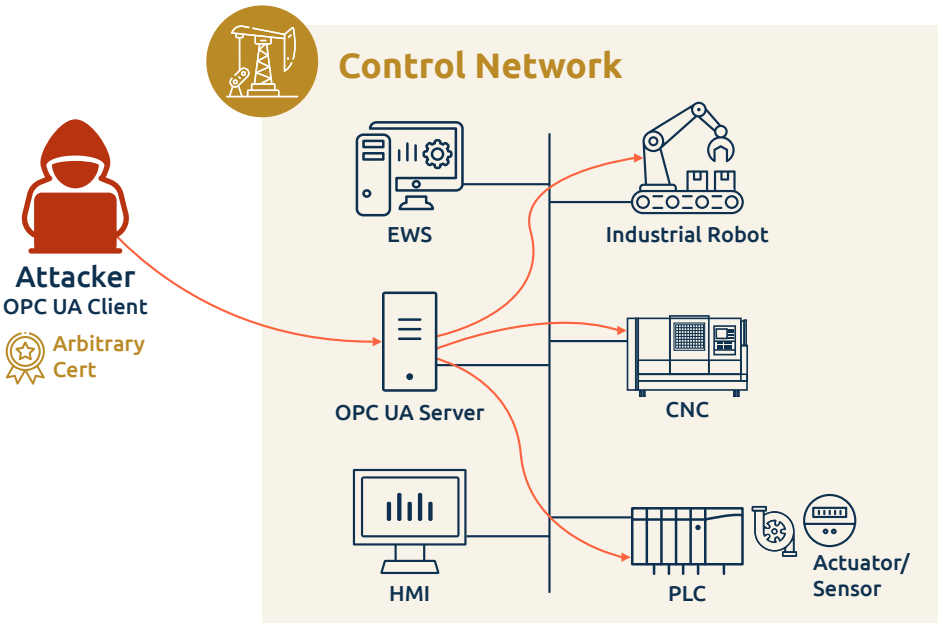

Figure 13: Missing Support for Trust List Design

Trust List Disabled by Default

Products in this group don't treat trust lists as a foundational security feature, but rather as an optional one. If users don't proactively activate this feature, any data sent by clients is deemed trustworthy without verification. For instance, as shown in Figure 14, the SIEMENS S7-1500 OPC UA user guide indicates that administrators need to actively turn off the "Automatically accept client certificates during runtime" to employ the trust list feature.[13]

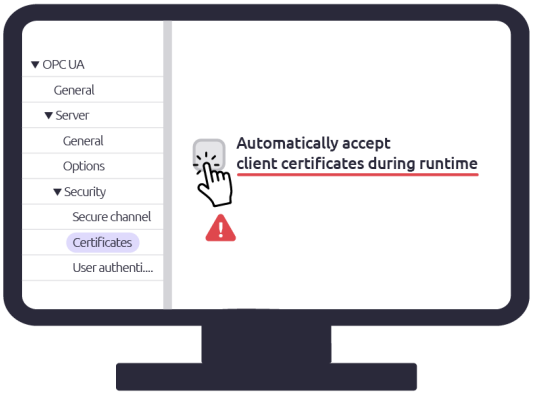

Figure 14: Trust List Disabled by Default

Insecure Trust List Configuration

Products in this category harbor security flaws in certificate trust implementation. This arises as the OPC UA standard permits unauthenticated users to exchange certificates in a secure channel setting. Product manuals instruct users to obtain new certificates by establishing new connections to join the trust list. However, this assumes that only trusted individuals can create a secure channel. If an attacker can perform a man-in-the-middle attack before adding the certificate to the trust list, they can deceive administrators into adding malicious device certificates to the trust list, granting them direct access to field device data, as depicted in Figure 15.

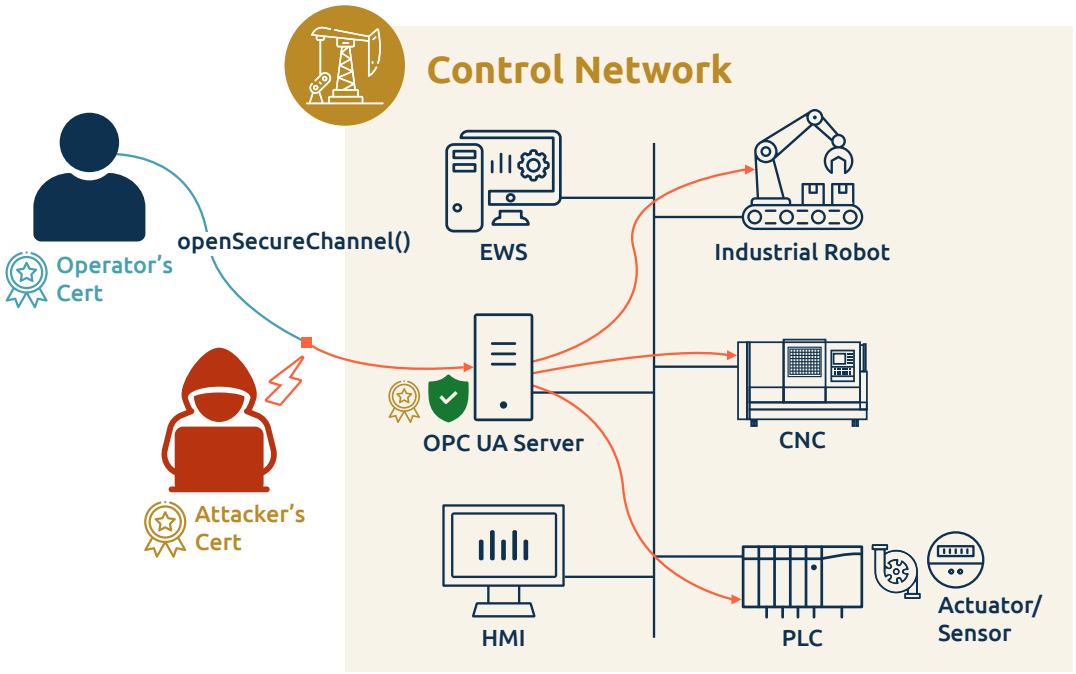

Figure 15: Insecure Trust List Configuration

SOHO

SOHO (Small Office/Home Office) devices often dwell on the perimeter of intricate network architectures, leaving them critically exposed without the advantage of sophisticated Intrusion Prevention Systems (IPS) to safeguard them. A longstanding issue with SOHO network devices is their notorious lack of security-centric designs, coupled with prolonged use of outdated models. This oversight leaves them vulnerable to exploits that might have been public knowledge for years. As a result, adversaries find it particularly enticing to target these low-hanging fruits to orchestrate attacks.

The Mirai botnet serves as a chilling testament to this vulnerability. This malware capitalized on multiple susceptibilities in IP cameras and home routers, embedding its malicious code to transform these devices into zombies in its botnet army. These 'infected' devices were then leveraged for Distributed Denial of Service (DDoS) assaults. Even more concerning is the evolution of Mirai, with newer variants exploiting fresh vulnerabilities in an array of SOHO devices from well-known manufacturers. Command injection and remote code execution are the primary attack vectors in these cases.

In a more OT-specific context,[14] the VPNFilter malware is known to have impacted a range of network devices from brands such as Linksys, MikroTik, NETGEAR, and TP-Link, with capabilities that extend to monitoring Modbus communication protocols.

By 2023, the Volt Typhoon organization leveraged vulnerable SOHO devices as stepping stones, exploiting firewall vulnerabilities for initial breach attempts, and subsequently nesting in critical infrastructure internal networks. This raises alarming questions: in the wake of the VPNFilter debacle, does this mean there is still a high chance that attackers targeting the OT environment can exploit SOHO devices for initial breaches?

Recognizing the growing trend of SOHO devices becoming primary targets, the Pwn2Own competition, hosted by Trend Micro, incorporated a SOHO category from 2022 onwards. Contestants were tasked with infiltrating SOHO devices from the WAN, transitioning to the LAN, and then cracking devices like smart speakers, NAS systems, or printers. In the 2022 edition, where the competition utilized contemporary SOHO devices, the NCCGroup unearthed the vulnerabilities shown in Table 3.[15]

Table 3. SOHO Vulnerabilities by Product[15]

Vendor	Product	Vulnerabilities
NetGear	RAX30 AX2400	• Undocumented protocol • Unprotected firmware update • Insecure protocol implementation
TP-Link	Archer AX21	• Undocumented protocol • Hardcoded encryption key
Synology	RT 6600ax	• Insecure protocol implementation • Insecure password reset
Ubiquiti Network	EdgeRouter X SFP	• Insecure protocol implementation

Taking the NetGear RAX30 AX2400 as a prime example, researchers identified a vulnerability that could grant shell access. Attackers could send specially crafted packets to the 23/udp service, subsequently adding a custom IP to gain access to the device's telnet service (23/tcp). This essentially handed them full control over the device on a silver platter, as illustrated in Figure 16. Translating this to the context of an oil and gas pipeline, should an attacker gain full control of the SOHO device, it could disrupt the smooth transmission of field device information to SCADA systems. This would potentially hinder timely detection of pipeline damage, heightening the risk of environmental catastrophes.

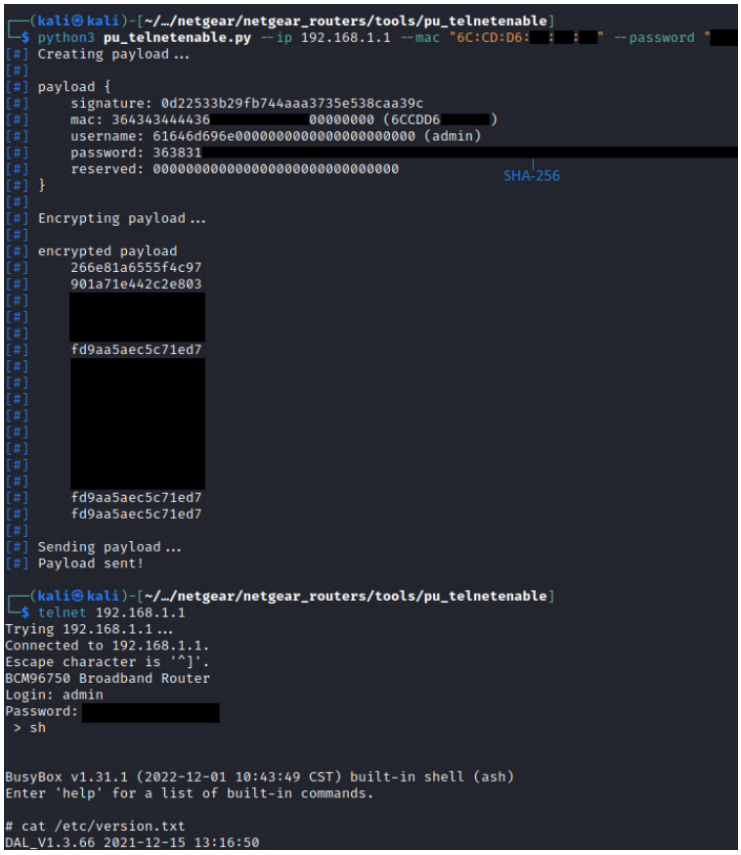

Figure 16: Attack on NetGear RAX30 AX2400 [15]

Legacy Assets

Historical incidents targeting Industrial Control Systems (ICS) serve as stark reminders of the vulnerabilities these systems possess. Once attackers breach the control network, they can easily exploit inherent service vulnerabilities to escalate their attacks. Ransomware, which continues to plague various industries, often proliferates by exploiting known 1-day vulnerabilities. Case in point, notorious ransomware variants like Bad Rabbit, LockerGoga, Revil, Ryuk, and WannaCry predominantly propagated through the SMB (Server Message Block) service, as illustrated in Figure 17. Many oil and gas facilities, built in earlier epochs, epitomize the looming threats to these legacy assets.

ICS	T0817	Drive-by Compromise	Bad Rabbit ransomware spreads through drive-by attacks where insecure websites are compromised. While the target is visiting a legitimate website, a malware dropper is being downloaded from the threat actor's infrastructure.
ICS	T0866	Exploitation of Remote Services	Bad Rabbit initially infects IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability), spreads to industrial networks.
ICS	T0867	Lateral Tool Transfer	Bad Rabbit can move laterally through industrial networks by means of the SMB service.
ICS	T0828	Loss of Productivity and Revenue	Several transportation organizations in Ukraine have suffered from being infected by Bad Rabbit, resulting in some computers becoming encrypted, according to media reports.
ICS	T0863	User Execution	Bad Rabbit disguises itself as an Adobe Flash installer. When the file is opened, it starts locking out the infected computer.

Figure 17: Bad Rabbit Exploits SMB Vulnerabilities to Infect Transportation Organizations [17]

Furthermore, our extensive research highlights the vulnerability of programmable assets commonly found in digital OT environments.[16] These assets, defined by their capability to autonomously execute physical operations based on compiled programs, become tempting targets for malicious actors. Given their unique ability to impact the physical realm, successful breaches can have direct repercussions on OT operations.

- **PLC (Programmable Logic Controllers):** Both open-source and proprietary service vulnerabilities offer assailants potential gateways to directly manipulate PLCs.
- **CNC (Computer Numerical Control):** Remote interaction services coupled with antiquated legacy Windows systems may grant attackers unmediated control over CNC machines.
- **Industrial Robots:** Assailable services and legacy components can potentially allow attackers to take over robot controllers directly, leading to manufacturing defects or even presenting tangible threats of bodily harm to human operators.

Revisiting Windows-based assets reveals that even contemporary oil and gas installations aren't immune to these threats. As illustrated in Figure 18, we executed a vulnerability exploit against the current up-to-date Windows Server 2022 using an MS-RPC (Microsoft Remote Procedure Call) breach. The diagram portrays a successful reverse connection from the victim machine (Windows Server 2022) to the attacker's system, demonstrating the feasibility of replicating attacks akin to the infamous Stuxnet, which notoriously exploited MS-RPC vulnerabilities.

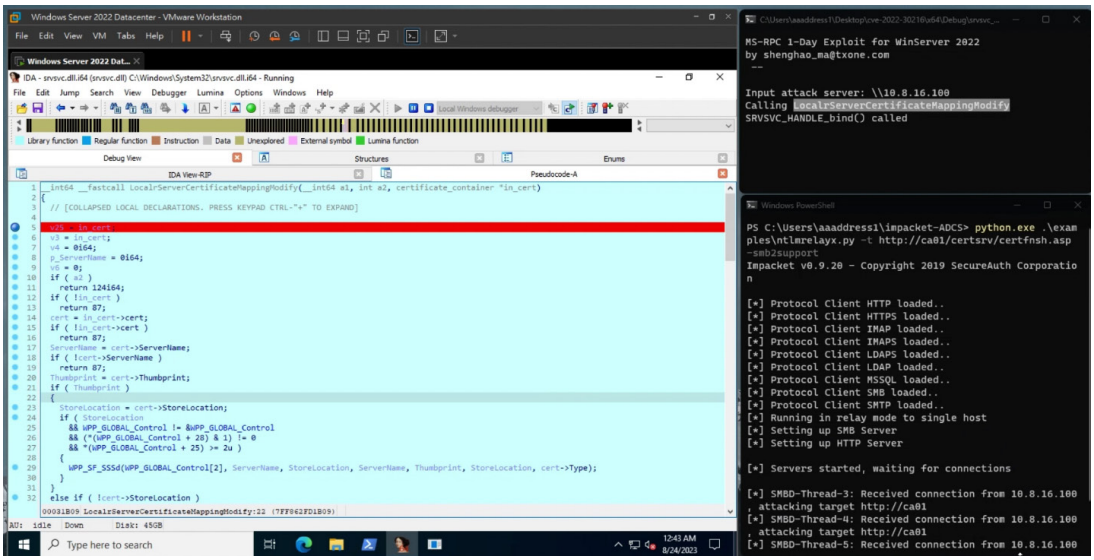

Figure 18: Exploiting Up-to-date Windows Server 2022 Through MS-RPC Vulnerability

Repelling Threats Against the Oil and Gas Industry

When we analyze digital adoption within the oil and gas industry, it becomes evident how potential adversaries might exploit control networks, as illustrated in Figure 19. Here, we'll delve into countermeasures addressing Initial Access, Lateral Movement, and Impair and Impact phases of attacks.

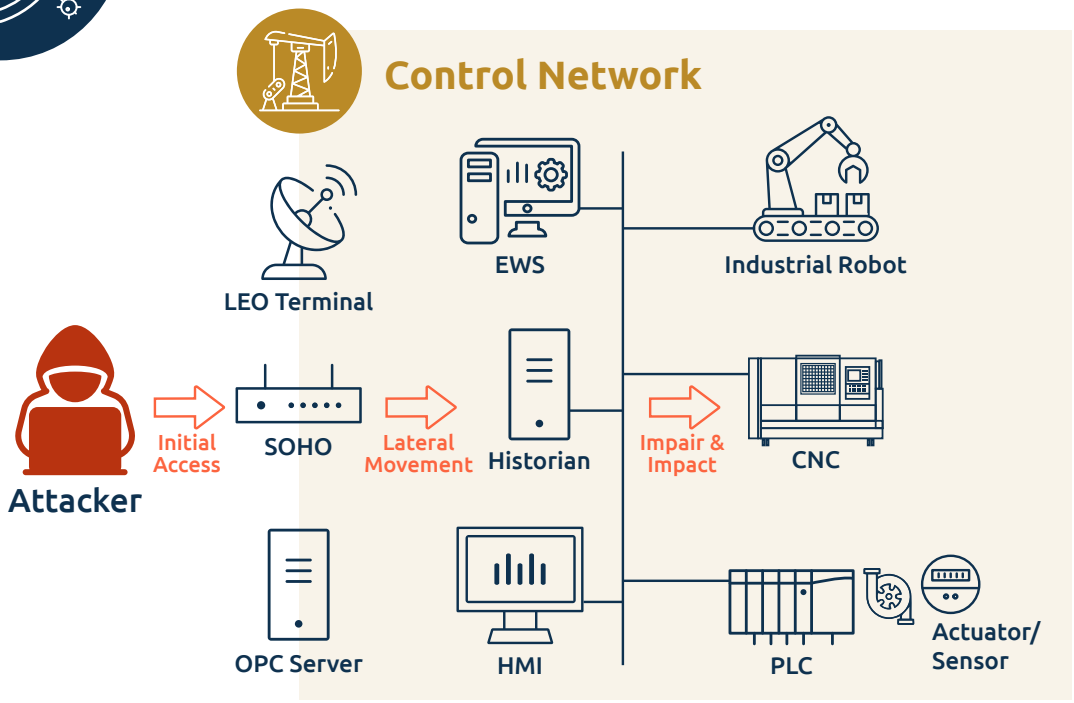

Figure 19: Attack Path to Control Network

Initial Access

Initial access techniques allow attackers entry points into ICS environments. These methods target operational technology assets, IT resources in OT networks, remote services, and websites. Privileged third parties, such as suppliers, maintenance crews, engineers, external integrators, and entities involved in ICS operations, are potential targets. Assets maintained by these third parties, including physical devices and operational equipment, may be vulnerable. Attackers can also exploit external devices, like radios or controllers, to remotely disrupt and potentially infect OT operations.

- **LEO Terminal:** Many Terminal devices inherently possess Ethernet-level vulnerabilities, such as hardcoded credentials and backdoor entry points. Asset owners should rigorously evaluate their network exposure and implement effective network segmentation strategies where necessary. For mitigating low-speed wireless RF hijacking, allowing only specific traffic patterns could be beneficial. As a long-term solution, the adoption of QPEP technology [as discussed in "QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit - NDSS Symposium"], an open-source encrypted hybrid of PEP/VPN, can encrypt satellite traffic without ISP involvement.

- **OPC:** Depending on the network security implementation by different OPC product vendors, it's imperative to choose products that correctly implement their security features. Employing a DMZ (Demilitarized Zone) structure with external devices like firewalls can fend off various unknown attacks.
- **SOHO:** Ensure the safe use of SOHO equipment with advanced security features, continuously monitor for security patches, and limit connection permissions.

Lateral Movement

Drawing upon the unique characteristics of control networks, strategies like Lock Down, Segment, and Reinforce can deter attackers from escalating their intrusion once they've infiltrated control networks.

- **Lock Down:** Establish trust lists for endpoints and networks, allowing only trust listed programs or traffic to function.
- **Segment:** Network segmentation for unrelated areas helps prevent attackers from expanding their reach after initial access.
- **Reinforce:** Protect assets at the network level, rendering vulnerabilities in legacy assets and unpatched devices remotely inaccessible without disrupting their continuous operation.

Impair and Impact

The impair and impact phase on process control involves methods that adversaries use to disrupt control systems, thereby affecting the targeted environment. This includes tampering with active procedures, control logic, or reporting mechanisms. While such disruptions might initially go undetected, their impact often manifests in the product or surrounding environment. These manipulations can endanger the safety of operators and downstream users, prompting response mechanisms. In conjunction, adversaries might employ techniques to suppress these responses, amplifying the overall damage.

- **Network Segmentation and Advanced Analysis:** Segment operational assets and their management devices based on their functional roles within the process. In the control environment, prioritize stringent isolation for more critical control and operational data. Additionally, monitor parameter changes in ICS management protocols, especially for anomalies, drastic deviations from the norm, or unexpected parameter modifications (e.g., via new functions or at unusual times).
- **Authorization for Execution:** All field controllers should restrict program modifications to specific users, like engineers or field technicians. Ideally, this should be achieved through role-based access control mechanisms.
- **CPS Asset Detection and Response:** It's optimal to enhance anomaly detection for endpoint operational behaviors, safeguarding against malicious software attacks. Implementing operational lockdown can ensure operational integrity, minimize downtime, and reduce service interruptions. This is particularly valuable for "non-patchable" systems. At times, there's also a need to strengthen trusted controls for portable media (like USB devices) to prevent unauthorized access.

Conclusion

With the oil and gas sector increasingly leveraging digital technologies to bolster management and production efficiency, the flip side is an escalation in cyber threats. We've evaluated potential initial attack vectors based on common technologies across upstream, midstream, and downstream segments. Besides delving deep into LEO Terminal, OPC, and SOHO technologies, we've detailed how they might potentially serve as breach points in control networks. Furthermore, by implementing a MS-RPC 1-day vulnerability attack on Windows Server 2022, we've illustrated the feasibility for attackers to replicate events akin to the Stuxnet incident. Finally, based on potential attack paths adversaries might employ against the oil and gas industry, we've outlined countermeasures, ensuring sustained operations within a secure environment.

Reference

[1] CISA of DHS, DoE, *"Energy Sector-Specific Plan 2015"*, The U.S. Department of Energy, October 2, 2015.

[2] EQUINOR, *"Strategies for Data-Driven Digital Transformation In The Plant"*, EQUINOR, 2023.

[3] Jeff Foust, *"Advance GEO/LEO For Oil & Gas"*, eutelsat, September 2023.

[4] Kranthi Kumar Buddha, *"Digital Twins in the Oil & Gas Industry"*, Acuvate, December 21, 2022.

[5] Simon Sierra, *"Digital Twins in Refining: Breaking Down the Coking Process"*, Akselos, April 10, 2023.

[6] FANUC America Corporation, *"Successful Robotic Solution for Oil Drilling Risers"*, FANUC America Corporation, February 22, 2023.

[7] Tatsiana Tsiukhai, *"The Use of Drones in the Oil and Gas Industry: 3 Examples"*, Softeq Development Corp, April 26, 2023.

[8] satelliteevolution, *"Will LEO constellations change the connectivity game for the oil and gas industry?"*, satelliteevolution, May 2023.

[9] Ruben Santamarta, *"SATCOM Terminals: Hacking by Air, Sea, and Land"*, IOActive, 2014.

[10] James Pavur, *"Introduction to Cybersecurity for Commercial Satellite Operations"*, Oxford University, Department of Computer Science, August 5, 2020.

[11] Hughes Network Systems, *"Hughes 9502 User Guide"*, Hughes Network Systems, Aerospace Corporation, September 14, 2022.

[12] Alessandro Erba, Anne Müller, Nils Ole Tippenhauer, *"Security Analysis of Vendor Implementations of the OPC UA Protocol for Industrial Control Systems"*, Saarland University Germany, November 8, 2021.

[13] SIEMENS, *"OPC UA .NET Client for the SIMATIC S7-1500 OPC UA Server"*, SIEMENS, October 2016.

[14] William Largent, *"New VPNFilter malware targets at least 500K networking devices worldwide"*, Cisco Talos, May 23, 2018.

[15] Alex Plaskett, McCaulay Hudson, *"Your not so "Home Office" - SOHO Hacking at Pwn2Own"*, NCC Group, April 2023.

[16] TXOne Networks, *"Threat Terrain of the Modern Factory: Survey of Programmable Assets and Robot Software"*, TXOne Networks, Aug 22, 2023.

[17] MITRE ATT&CK, *"Bad Rabbit Techniques Used"*, MITRE, February 09, 2021.

txone.com