



Cyber Attacks Against Oil & Gas Sector



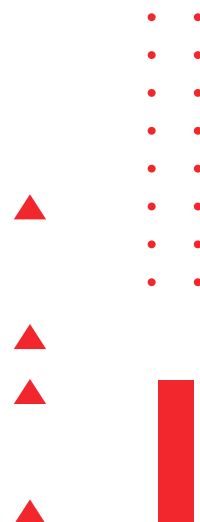
Copyright notice:

This white paper and its content is copyright of Payatu Consulting Pvt. Ltd. Copyright 2023 Payatu Consulting Pvt. Ltd. All Rights Reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following: You may print or download to local hard disk extracts for your personal and noncommercial use only You may copy the content to individual third parties for their personal use, but only if you acknowledge the ebook as the source of the material You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it on any other website or other forms of the electronic retrieval system.

Copyright@ 2023 Payatu Consulting Pvt. Ltd. All Rights Reserved.

Table of Contents

1. Cyber Attacks Against Oil and Gas Sector.....	4
2. Cyber Attacks Evaluation of Oil and Gas Sector	6
3. Threats That Can Compromise Oil and Gas Industries.....	11
4. Malware that Affected Industrial Control Systems (ICS) in the Oil and Gas Sector.....	13
5. How have OEMs, Third-Party Vendors, and Supply Chain Issues Affected ICS in Oil and Gas Sector?.....	14
6. Activity Groups Targeting Oil and Gas Sector.....	16
7. Detailed Analysis of Oil and Gas Infrastructure Attacks.....	17
8. Recommendations to Strengthen ICS/SCADA(OT) Cybersecurity Posture.....	19
9. Few Well-Known Standards/Guidelines to Follow.....	21
About the Authors.....	22



1.0

Cyber Attacks Against Oil and Gas Sector

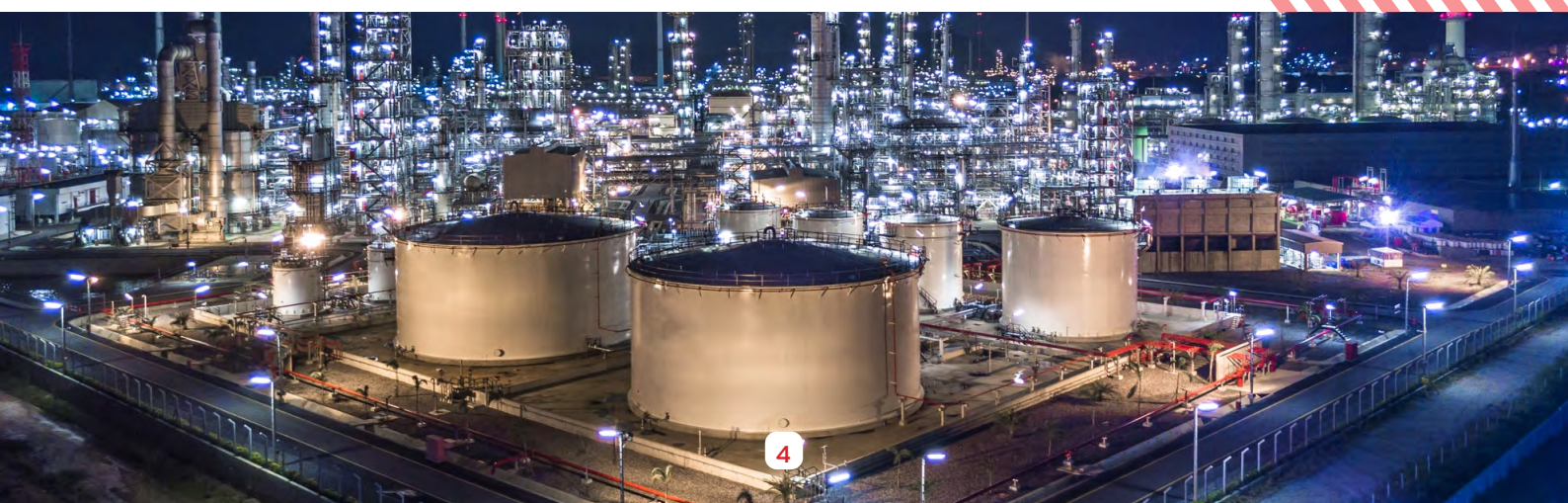
Cyber Threat to Digital Oilfield

Since the beginning of 2010, the frequency of cyberattacks has gradually risen despite the expansion of digitization across the oil and gas industry. Intruders may compromise ICS/SCADA(OT) infrastructure by either launching malware attacks on networked services or by exploiting devices that have security holes that provide them access to the infrastructure. Both methods enable intruders to get access to the infrastructure.

Since the oil and gas industry is increasingly reliant on digitalization and remote operators, unscrupulous attackers are able to penetrate industrial control systems via phishing, malware, ransomware, and supply chain vulnerabilities causing huge impact on operations

All these different devices and computer systems are connected to one another via networks. It is absolutely necessary to gain a better understanding of how to prevent such attacks and then put those understandings into action given the significance of the oil and gas industry to the economy of the entire world as well as the breadth and complexity of the major systems, that are frequently controlled remotely. Given these factors, it is vital to gain a better understanding of how to prevent such attacks.

During an attack on any level of the supply chain for the oil and gas industry, from upstream to the middle to downstream, the most common methods that cyber criminals used to spread malware and gain unauthorized access to user accounts were phishing and intrusions. These methods were also the primary means by which they gained access to user accounts. Following the process of collecting information on real attacks that have been carried out in each domain, we conduct an analysis of the data that we have obtained.



Energy Sector Becoming More Vulnerable to Cybercrime

Since 2015, oil-related assets and infrastructure have been the most popular targets for attackers and cyberattacks, accounting for one-third of all occurrences during that time period. Damage to the industrial control systems and operational technology (ICS/OT) business is estimated to be close to \$2.8 million on average, with the oil and gas industry being the most severely affected sector.

Only in the last four years has there been a roughly 78% rise in the financial effect of cybercrime, and the amount of time it takes to settle a cyber assault has more than doubled in that period. It may come as a surprise to find that as much as 40% of all malware generated is deployed and tested in the oil and gas industry. This includes attacks against facilities that store gasoline and pipelines, as well as oil rigs (both onshore and offshore), facilities that store natural gas, and refineries.



The Oil and Gas Industries are Turning Digital. How Serious is the Threat Right Now?

Implementing digital technology in the oil and gas sectors may result in a variety of benefits, including increased productivity, better decision-making, and cost savings. As more infrastructure becomes digital and internet-connected, it becomes more vulnerable to cyber attack. Attackers exploit vulnerabilities in digital systems to steal information, disrupt systems, or even cause bodily injury. Intruders may attempt to disrupt the oil and gas sector's digitization in a variety of methods, for example:

- For the purpose of stealing sensitive information or gaining unauthorized access, attackers may send phishing emails or create spoof websites to deceive workers.
- Attempts may be made by attackers to breach a company's network security by taking advantage of the system or equipment.
- Malware, like viruses or ransomware, may be used by attackers to infiltrate computers, networks, and other systems.
- Damage or interruption to oil and gas operations might result if attackers breach the facilities' industrial control systems.
- In order to compromise an oil and gas firm's systems or data, attackers may go after the firm's suppliers or contractors.

To combat such attacks, oil and gas companies must implement stringent cybersecurity measures, as well as conduct periodic risk assessments, deploy effective prevention and response mechanisms, and keep security advances and best practices updated. Businesses must have an incident response plan in place, in addition to cybersecurity safeguards, to quickly detect and remediate any security breaches that may occur. This may entail activities such as isolating affected systems, restoring backups, and communicating with stakeholders.



2.0

Cyber Attacks Evaluation of Oil and Gas Sector

There is something very unique about the oil and gas sector. The facilities are typically very large. For example, a single refinery has the potential to supply 20% or 30% of the energy requirements of an entire state or a significant portion of a country. Therefore, an attacker can cause significant harm (such as shutting down a region of a country) even by targeting a single large refinery. The following are examples of actual cyber attacks that resulted in significant losses.

European Oil Refineries and Storage Facilities Were Hacked

Year: 2022

Impact: The latest large-scale ransomware attack has targeted oil port terminal software in at least 17 ports in Western Europe, re-routing tankers and significantly disrupting supply chains.

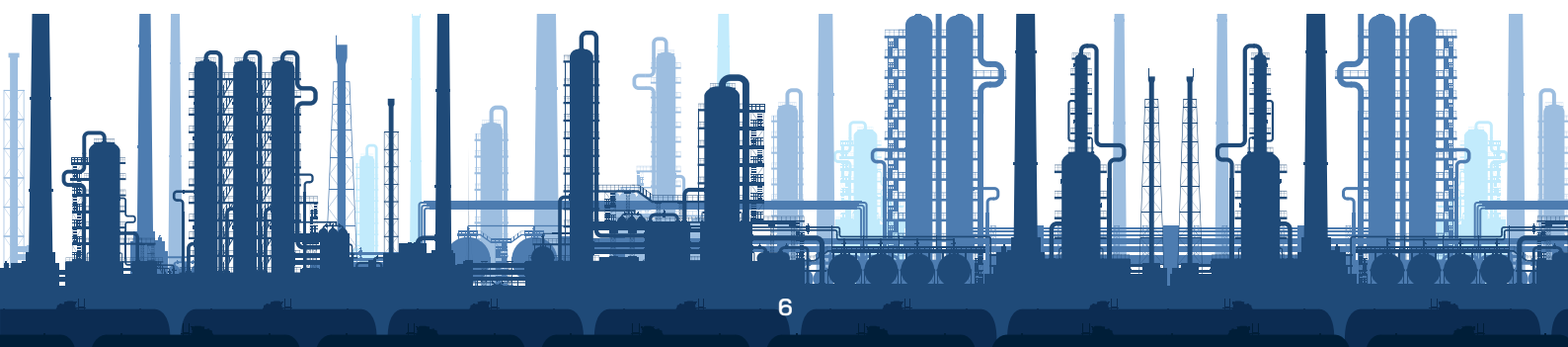
Attack: Ransomware attack

Details: After affecting operations in Germany, cyberattacks on oil loading facilities have spread to important terminals in the Amsterdam-Rotterdam-Antwerp (ARA) refining hub. The attack coincided with escalating tensions before Russia's invasion of Ukraine earlier this year and growing worries about the security of Europe's energy supply. Systems at Oiltanking and Mabanaft in Germany, SEA-Invest in Belgium, and Evos in the Netherlands were the focus of the attack. 17 terminals in all (11 in Germany and 6 in ARA) were impacted.

Operations were clogged as the firms worked to stop the attack, making it impossible to load or unload merchandise from barges. In the wake of the event, which occurred at a time of skyrocketing energy costs and geopolitical unrest, worries about the security of the European energy infrastructure have persisted.

Reference Links:

- <https://www.bbc.com/news/technology-60250956>
- <https://www.bankinfosecurity.com/cyberattack-cripples-european-oil-port-terminals-a-18465>
- <https://www.france24.com/en/live-news/20220203-european-oil-port-terminals-hit-by-cyberattack>
- <https://www.bloomberg.com/news/articles/2022-02-02/cyberattack-on-europe-s-fuel-network-hits-germany-and-trade-hub>



India's 2nd Largest Government-owned Hydrocarbon Production Hacked

Year: 2022

Impact: Oil India suffered a significant financial loss as a result of the outages and interruptions to business.

Attack Type: Russian ransomware demands \$75,000 in bitcoin.

Details: On April 10th, a cyber attack was launched against one of the workstations belonging to the Geological and Reservoir department; however, the IT department was not made aware of the incident until April 12th. Because of this, the OIL (Oil India Limited) server, the network, and any other services that were linked to it were affected. Russian malware installed on a computer in Nigeria was used in the cyber attack that brought the PSU's main subsidiary's network to a halt. However, the virus had already spread to other computers, so organizations took the precaution of disconnecting those machines from the primary LAN connection.

Based on the first findings, it appeared that OIL's network, server, and client PCs are all suffered from a network outage. The company claimed in its lawsuit that OIL suffered "substantial financial damage" as a direct result of the Oil India ransomware attack because business interruptions and outages occurred. Because of the hack, the firm and the government treasury have both sustained substantial losses, which may be attributed to the inability of their information technology systems to function properly.

The magnitude of an event can be greatly reduced by resilience and prompt intervention. Otherwise, the cyber-attack can cause disruption within the firm, downtime within the network, and significant monetary loss

Reference Links:

- <https://timesofindia.indiatimes.com/city/guwahati/assam-cyberattack-in-oil-indias-headquarters-attackers-demand-over-rs-57-crore-as-ransom/articshow/91067771.cms>
- <https://economictimes.indiatimes.com/news/india/oil-india-cyber-attack-russian-malware-planted-from-nigeria/articleshow/91010072.cms?from=mdr>

Ransomware on Colonial Pipeline

Year: 2021

Impact: Ransomware attack that forced the U.S. energy company to shut down its entire fuel distribution pipeline, threatening gasoline and jet fuel distribution across the U.S. East Coast.

Attack Type: DarkSide Ransomware Attack

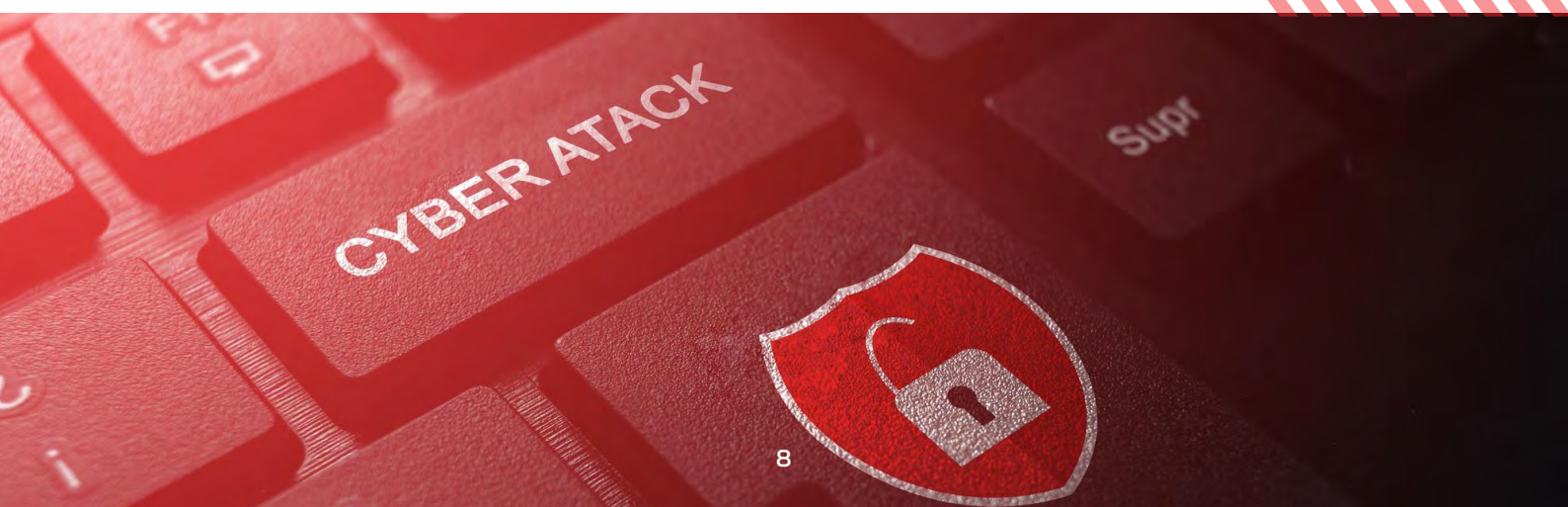
Details: The attack on the facility did not directly impact on any of the control systems; rather, it affected the billing system. It prevented the consumers from being able to get invoices for their purchases. However, just by gaining access to the firm's invoicing system, the attackers were able to force the company to halt all activities because they did not realize at the time how extensive the attack was. The intrusion, which was used to encrypt data on the company's systems, putting Colonial's enormous operational technology (OT) network, which included a pipeline spanning 5,500 miles, at risk of being taken over remotely. Following the hack, the firm ceased all activities involving pipes.

In order to avoid the consequences, the ransom demand of \$4.4 million was paid within a few hours. After that, the attackers offered tools to decrypt the files, a process that took several hours but ultimately assisted in bringing the systems back online in a timely manner. The active gang that was behind the hack was known as DarkSide, and prior to the malware attack, they had already taken 100 GB of data from the servers of the firm.

The potential risk rises when an organization uses insecure hardware or software across a network, which might result in the firm having to suspend all operations if they are unaware of the

Reference Link:

- <https://www.sans.org/newsletters/newsbites/xxiii-37/>
- <https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html>
- <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>
- <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>



German Gasoline Provider Goes Offline After Cyber Attack

Year: 2022

Impact: Shutdown of different plants causing major business loss

Attack: Ransomware Attack

Details: Oiltanking, a multinational gasoline transportation company based in Germany, was the victim of a hack that caused thirteen of its distribution sites to become inaccessible. In response to what seems to have been a cyber attack on Oiltanking, operational technology (OT) systems at gasoline distribution sites across Germany were deactivated. According to the gasoline providers, the cyber attack caused harm to their information technology systems in general; however, the most urgent concern was with the automated tank loading and unloading systems, which were wholly dependent on the computer systems that were compromised. The resources of Oiltanking and Mabanaft, another subsidiary of the same parent firm, were affected, nevertheless.

Reference Link:

- [German fuel supplier declares force majeure after a cyberattack | Cybernews](#)
- <https://www.hazardexonthenet.net/article/189225/German-fuel-supplier-hit-by-cyber-attack--13-oil-terminals-affected.aspx>
- <https://www.cpomagazine.com/cyber-security/critical-infrastructure-hit-again-as-german-fuel-suppliers-victimized-by-cyber-attack-oil-shipments-forced-to-use-alternative-depots/>
- <https://www.bbc.com/news/technology-60215252>

Triconex Controller Attack at Saudi Aramco

Year: 2017

Impact: The hard drives inside the company's computers were destroyed and their data wiped clean, replaced with an image of Alan Kurdi, the small Syrian child.

Attack: W32.Disttrack/Shamoon Malware

Details: An employee in the IT department of Aramco fell for a phishing email and clicked on a link, which made it possible for the W32.Disttrack/Shamoon Malware to conduct a successful breach against the Saudi Arabian oil and gas company Aramco. This allowed the malware to spread to more than 30,000 computers, corrupt the company's Master Boot Records (MBRs), and rendered numerous internal networks inactive for up to 2 weeks.

2 weeks of business interruption left this multinational corporation's computer networks susceptible to intrusions. Due to the infrastructure attack, certain drilling and production data may have been destroyed. Not only did the Shamoon ransomware infect their computer network, but it also wreaked havoc on the computer systems of a number of other companies working in the oil and gas business. Due to Ramadan, most Saudi Aramco workers were not present during the initial stages of the assault, therefore few people noticed anything unusual happening on their devices.

On the panels there appeared to be a flickering pattern, and the information was progressively lost. Some computers would abruptly power off without providing any kind of warning.

Reference Links:

- <https://www.cnbc.com/2021/07/22/saudi-aramco-facing-50m-cyber-extortion-over-leaked-data.html>
- <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>
- <https://www.eenews.net/articles/the-inside-story-of-the-worlds-most-dangerous-malware/>
- <https://www.cyberscoop.com/trisis-investigator-saudi-aramco-schneider-electric-s4x19/>

3.0

Threats That Can Compromise Oil and Gas Industries

- **Phishing Attack**
Phishing includes sending fake emails or text messages that look like they're from a reputable source to fool recipients into exposing personal information or clicking on a malicious link. A phishing attack steals login credentials or financial information or infects the recipient's device with malware. Phishing attacks are hard to detect because they utilize social engineering and resemble authentic brands and language. They may utilize bogus websites or other internet tools to trick victims.
 - **External Emails**
Businesses safeguard email. External email, however, can't be controlled. Employees routinely email external addresses, exposing firm data. Sensitive information can be duplicated to unprotected backup systems or kept locally on personal devices without usual enterprise security controls, making it easier for attackers to access the data. After compromising a computer, an attacker can use the emails to harm the organization.
 - **Supply Chain Attack**
Supply chain assaults are difficult to notice and avoid because they include reputable sources like software or hardware vendors. Supply chain attacks are possible from manufacturing to distribution. Malware can be inserted into software updates or altered before reaching consumers. An organization might unwittingly provide an attacker access to its internal systems and data by installing or utilizing compromised software or hardware.
 - **Advanced Persistent Threat (APT)**
A threat actor, such as an attacker or a group of attackers, gains unauthorized access to a network and goes undetected for a long time. APTs often steal critical data or disrupt network operations. APTs are harmful because they're well-planned and organized and employ advanced methods and technologies to prevent detection. APTs target specific companies or individuals and use malware, phishing, and other tactics to infiltrate their systems.
 - **Cloud Attack**
Cloud attacks target cloud computing systems. Cloud computing includes storage, networking, software, analytics, and intelligence. Cloud attacks can take numerous forms, but they always aim to steal critical data or impair service. Server breaches, malware injection, DoS attacks, insider threats, and misconfigured systems are prevalent cloud attacks.
- **Phishing Attack**
 - **External Emails**
 - **Supply Chain Attack**
 - **Advanced Persistent Threat (APT)**
 - **Cloud Attack**
 - **Data Theft**
 - **Insider Threat**
 - **Sabotage**

- **Data Theft**

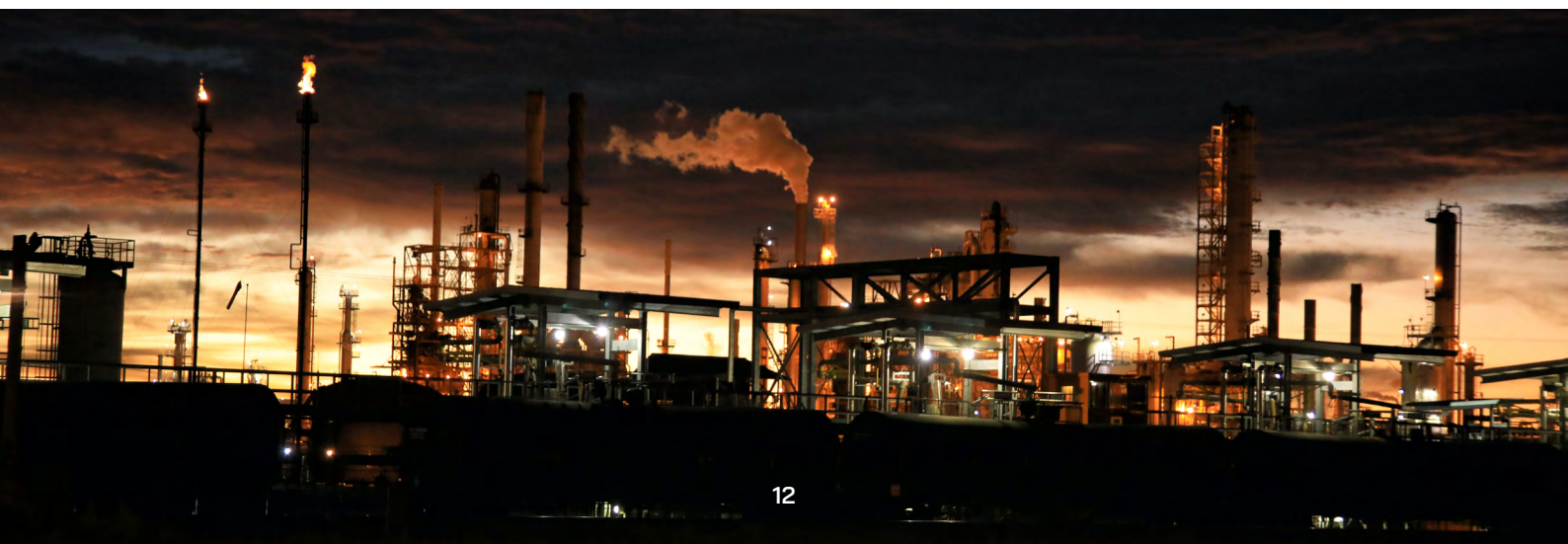
Potentially lethal attacks on a larger scale could be sparked by espionage. A precise understanding of the situation is necessary for attackers before taking any further action. Financial gain may be possible for attackers if they obtain sensitive data such as drilling techniques, knowledge of suspected oil and gas resources, and exclusive recipes for high-end commodities.

- **Insider Threat**

An insider leaker may be a former employee who is out for revenge or wants to make quick cash by selling confidential company information to a rival company. This individual is a security risk because of their potential to cause problems for the business, alter data in ways that lead to problems, delete material from company servers or shared project files, steal intellectual property, and leak sensitive information.

- **Sabotage**

In the oil and gas industry, sabotage can be carried out via modifying the functioning of software, erasing, or wiping certain files to disrupt corporate activities, or erasing as much data as possible from every available equipment.

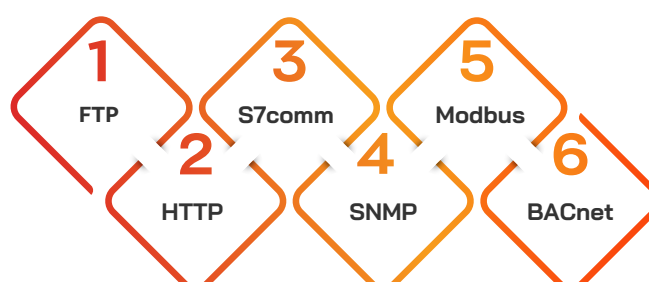


4.0

Malware that Affected Industrial Control Systems (ICS) in the Oil and Gas Sector

- Triton/Trisis**
 The malware known as Triton has been around since at least August of 2017, and its primary method of operation involves infecting a Windows machine that is presumed to be linked to a SIS device. After that, the malware injects code into the system, changing the way the SIS device operates. Trisis, is programmed to interface with a particular category of industrial control systems (ICS), known as safety instrumented systems (SIS), and to deploy alternative logic to these devices, which means that they may not operate in the proper manner.
- Flame**
 Flame is a very advanced piece of malware that is also called Flamer or SkyWiper or Skywiper. It has a number of add-on modules that allow it to attack, gather information, spread itself, scan networks, leak files, and remove itself from a system that it has infected. It uses 5 different kinds of encryption, many zero-day exploits, and fake security certificates to make itself look like real Microsoft software.
- Havex**
 Havex is a RAT focused on industrial control systems (ICS). Havex is transmitted using phishing emails with malicious attachments or URLs to infect a target's PC and provide remote access. Havex may accomplish many tasks once it's installed, like collecting system and network information, executing more harmful files, and creating a remote shell to issue commands to the infected systems. It's been used in "Energetic Bear" and "Dragonfly" advertisements targeting energy and industrial industries in the US and Europe.
- Industroyer**
 Industroyer, also known as CrashOverride, is meant to disrupt normal ICS operation by overwriting important system files and causing equipment to malfunction. It can also turn off the safety relays that prevent equipment damage and outages.

Most Attacked Protocol





5.0

How have OEMs, Third-Party Vendors, and Supply Chain Issues Affected ICS in Oil and Gas Sector? – Few Scenarios

An organization's network may be dependent on OEMs, third-party vendors, or the supply chain for critical products or services. If these external parties experience disruptions or outages, it can have a significant impact on the organization's network and operations.

To mitigate these risks, it is important for organizations to establish clear agreements and contracts with OEMs, third-party vendors, and supply chain partners that outline expectations for security, quality, and integration. Organizations should also consider implementing monitoring (OT visibility).

Vulnerabilities in Vendors' Products : Few Examples



Schneider

Industrial giant Schneider claims that in 2015, Triton malware exploited a zero-day vulnerability in Triconex SIS controllers to attack a critical infrastructure organization. Schneider Electric's software, managing a building's temperature had been determined to contain security flaws. By tricking a user into running a malicious file or visiting a malicious URL, threat actors could execute arbitrary code on the victim's PC.

ABB

Researchers in the field of cybersecurity have released details on a newly discovered flaw in a system widely employed by the oil and gas industry. CVE-2022-0902, a path-traversal vulnerability in ABB Totalflow (CVSS score: 8.1), is a critical flaw. MAGNALLIUM continues to focus mostly on front-end Information technology incursions since it lacks the ICS-specific capacity.

Advantech

Vulnerabilities were discovered at a higher rate in 2016, with the majority being in products made by Advantech. Recently, 109 flaws in its Web Access SCADA software were discovered. Threat actors may be able to execute arbitrary code due to a lack of validation in one of its components.

Wecon's LeviStudioU

LeviStudioU is used to build HMI solutions in energy, critical industrial, water, and wastewater systems. Numerous severe flaws in WECON LeviStudioU have been discovered. Successful exploitation of these vulnerabilities might allow an attacker to execute remote code.

Dell

Dell has issued a series of critical and high-priority solutions to address continuing Log4j vulnerabilities before they are discovered and exploited by malicious actors. One software patch resolves two major Log4j remote code vulnerabilities in the Dell EMC VxRail systems, which are hyper-converged infrastructure systems using VMware Vcenter software on Dell EMC hardware. It addresses CVE-2021-44228 and CVE-2021-45046, although Dell warned that a workaround is required and directed customers to visit VMware for guidance.

6.0

Activity Groups Targeting Oil and Gas Sector

These are some of the ICS/OT Activity Groups reaching Stage 2 of the ICS Cyber Kill Chain, meaning they gained access directly into ICS/OT networks.

XENOTIME

In August 2017, Xenotime interrupted a Saudi Arabian oil and gas plant using the damaging TRISIS architecture. TRISIS's possibly catastrophic impact increased ICS assaults. In 2018, XENOTIME included electric utilities in North America and APAC, other devices besides Triconex controllers, and oil and gas corporations in Europe, the US, Australia, and the Middle East. This group compromised ICS manufacturers and vendors, endangering the supply chain.

MAGNALLIUM

Magnesium has been actively targeting the petrochemical and aerospace industries since at least 2013. After targeting a Saudi Arabia-based aircraft holding firm and energy companies, the activity group widened its aim to include organizations in Europe and North America. MAGNALLIUM still lacks the ICS-specific functionality, and it continues to be primarily concerned with early IT intrusions.

CHRYSENE

Chrysene originated from an intelligence gathering operation that originally attracted attention following the devastating Shamoon cyberattack in 2012 that hurt Saudi's Aramco. The petrochemical, oil and gas, and power generation sectors are the focus of the activity group. The group's initial focus on the Gulf region has expanded, and its target has changed accordingly. The group is still active and constantly changing in a variety of contexts.

HEXANE

The oil and gas industry as well as the telecommunications sector are Hexane's primary targets throughout Africa, the Middle East, and Southwest Asia. Although this newly recognized activity group was discovered in May of 2019, there is little information that is currently accessible to the public at this time.

DYMALLOY

Dymalloy is a very aggressive activity group that may get long-term, persistent access to IT and operational environments in order to gather intelligence and prepare for future disruption activities. The criminal group has targeted utilities, oil and gas firms, and hi-tech manufacturers in Turkey, Europe, and the Americas.

7.0

Detailed Analysis of Oil and Gas Infrastructure Attacks

Attack Technique	Oil & Gas Stream	Attack Type	Attack Impact	Business Loss
Internet Accessible Device	Upstream	External - Malware Attack	<ul style="list-style-type: none"> Damage to property Loss of Availability Denial of Services 	In 2010, a computer virus was discovered on a rig travelling from South Korea to Brazil. The breadth of the infection was such that it took IT personnel 19 days to restore functioning.
User Execution	Upstream, Midstream, Downstream	Internal - Injection, Jamming attack	<ul style="list-style-type: none"> Change program state Damage to property Modify control logic 	A chevron oil employee was dismissed after he modified the computers in the company's New York and San Jose offices—which oversaw the alerts systems—to crash whenever the system was powered on. Richmond, California experienced a toxic material leak, however the system did not issue the appropriate notice.
Internet Accessible Device User Execution	Upstream	External - Injection attack	<ul style="list-style-type: none"> Modify control logic Change program state Denial of service Damage of property 	An oil rig off the coast of Africa was tilted by an assault in 2012, shutting it off. The attack was blamed for equipment failure due to manipulation of the ballast control, most likely via PLC-actuator command and control. 89 construction workers who were working on the rig were hurt in the attack.
Replication through removable media technique	Upstream, Midstream, Downstream	Internal - USB attack	Theft of Operation Information	Critical systems in the Middle East were compromised by the virus Copperfield through USB. Windows script host was used in a malware attack using scripts. For the goal of reconnaissance, an attack stole data.
Internet Accessible Device	Upstream, Midstream, Downstream	External - Malware Attack	Modify control logic	The xenotime hacking organization launched an attack against the Saudi oil business Petro Rabigh using the Triton/Trisis virus. Triton was created with the intention of disrupting operations and setting off an explosion. The controller was forced into entering a failsafe mode, which caused all processes to be automatically terminated.

Attack Technique	Oil & Gas Stream	Attack Type	Attack Impact	Business Loss
User Execution Modify Control Logic	Upstream, Midstream, Downstream	Internal - Injection attack	<ul style="list-style-type: none"> Change program state Denial of services 	Electromagnetic pulses and clock blips were created by test attacks upon machinery and equipment utilized by O&G plants. Attacks have the potential to interrupt operations and result in various unintended consequences.
Spear phishing attachment	Midstream	External - Phishing attack	Supply chain compromise	The APT33 attack group targeted the oil supply chain among other things in order to infiltrate oil firms in Europe and Asia. Targets of spear phishing efforts included many Oil and Gas equipment manufacturers and oil tanker firms. Facilities' supply chains were the focus of attacks.
Spear phishing attachment	Upstream	External - Phishing attack	Theft of operational information	Attacks by the Gaza cybergang against the oil and gas sector led to the identification of its opponents throughout the MENA area. Using the CVE 2017-0199 vulnerability, attackers constantly retrieved data for more than a year. Using a vulnerability, attackers constantly retrieved data for a year.
Internet Accessible Device	Downstream	External - Injection attack	<ul style="list-style-type: none"> Loss of availability. Loss of productivity and revenue 	Energy services group - ESG attack handled client transactions for various energy companies that owned natural gas pipelines. Customers were unable to access transactions for a sizable portion of the ESG assault. Gas interruptions were caused by collateral damage.
Spear phishing attachment	Midstream Downstream	External - Phishing attack	Theft of Operational information	Attacks using hexane targeted oil and gas telecommunications in Southwest Asia, the Middle East, and Africa. Attack spread malware via infected papers gathering information on ICS entities.

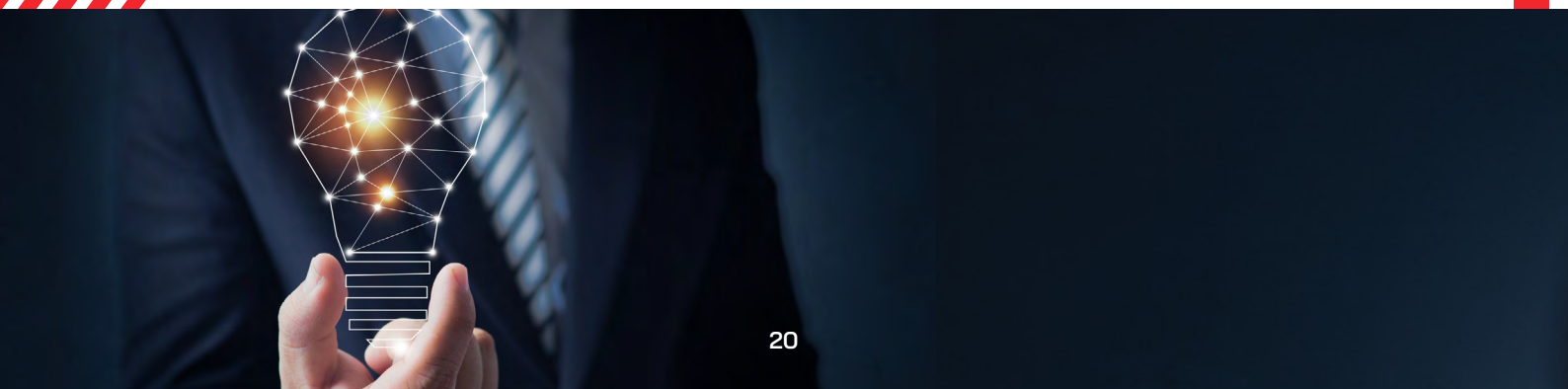
8.0

Recommendations to Strengthen ICS/SCADA(OT) Cybersecurity Posture

- Define the specific OT systems and integrated OT system designs that are thought to be essential for ensuring safety both inside the company and on the company vessel. Create a system architecture diagram as per Purdue model, for the system (or systems) that may be used in cyber risk assessment.
- Segmenting networks and systems as per the Purdue model (Perimeter Network, Demilitarized Zone, Internal Network, and Secure Zone), to limit the spread of a potential cyber attack and make it easier to identify and isolate the source of the attack. Whenever possible, ICS should not share the same network with internet - accessible devices.
- A perimeter-level firewall is recommended for defending against cyber attack by filtering incoming traffic, inspecting traffic, providing a single point of protection, and performing other functions.
- It is recommended to have IDS and IPS solutions to provide real-time visibility and protection for industrial control systems (ICS) and operational technology (OT) networks. This can involve restricting traffic or quarantining compromised systems.
- It is recommended to regularly monitor and log activity on your systems to detect and respond to any suspicious activity.
- Use secure communication channels, such as virtual private networks (VPNs), to protect data transmitted between different locations or devices.
- To safeguard user information, digital certificates, passwords, access to confidential data, and safety-critical systems, a robust password policy in conjunction with MFA should be developed.
- Enforce a password reset policy in the event of a compromise, especially for VPNs and administrative accounts.
- Employees' access rights and credentials should be tailored to their specific roles. All user accounts must adhere to the principle of least privilege and require administrator credentials for program installation.
- To respond to and recover from a cyber attack, implement an incident response plan that includes recognizing and minimizing the attack, recovering systems, and communicating with stakeholders.
- Implement secure coding practices to reduce the risk of vulnerabilities in custom applications.
- Conduct regularly audit on your systems and networks to identify vulnerabilities and implement controls to mitigate them.
- Use secure protocols, such as HTTPS, SFTP, TLS, etc., to protect against man-in-the-middle attacks.
- Harden Microsoft Windows 10 with latest version Workstations. Before implementing recommendations, thorough testing should be undertaken to ensure the potential for unintended negative impacts on business processes is reduced as much as possible.



- Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Disable local administrator accounts or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.
- Implement a patch management process to keep your systems up to date with the latest patches and updates to reduce the risk of vulnerabilities being exploited.
- As the owner of an asset, you should have an OT cybersecurity risk management plan in place that delegates responsibility to stakeholders, including integrators, operators, and vendors.
- Conduct regular security assessments to identify vulnerabilities and weaknesses in your network systems.
- Implement access controls, such as user authentication and permissions, to control who has access to which systems and data.
- It is recommended to have application whitelisting to allow only approved applications to run on endpoints/systems.
- Use asset management to track and monitor your assets, including hardware and software, to ensure that they are secure and up to date.
- It is recommended to have end-to-end encryption to protect data in transit and ensure that it can only be accessed by authorized individuals.
- To stop physical manipulation, field equipment must have hardware security controls.
- Critical OS and ICS software upgrades must be installed as soon as possible following proper testing by the support team. All hosts should have antivirus and anti-malware software installed and kept up to date. Turn down unnecessary RDP/remote access ports and keep an eye on the logs.
- All personnel working on critical systems must have training or certifications to support their roles' high danger level. Human error and phishing attempts are best avoided by staff knowledge.
- Regular vulnerability assessment and penetration testing audits must be conducted at all sites to guarantee continuous examination of operating systems.
- To limit the number of vulnerable assets, implemented ICS should make use of hardware and software from different manufacturers. Although it adds complexity to management, this approach is essential for protecting essential systems from failure.
- Data should be backed up on a regular basis, air gaps should be used, and offline backup copies should be password protected. Make sure that copies of crucial data are not stored in a way that would allow them to be altered or removed from the system in which they are stored.
- Maintain and store multiple copies of servers and data that include sensitive or proprietary information in a safe, isolated area (i.e., hard drive, storage device, the cloud). Build, test, and maintain continuity of operations.
- It is important for organizations to establish clear agreements and contracts with OEMs, third-party vendors, and supply chain partners that outline expectations for security, quality, and integration. Organizations should also consider implementing monitoring and audit processes to ensure that these partners are meeting their obligations.
- Use threat intelligence to stay informed about the latest cyber threats and how to protect against them.
- Implement physical security measures such as security cameras and access controls, to help prevent unauthorized access to your facilities and systems.



9.0

Few Well-Known Standards/Guidelines to Follow

- ISA/IEC 62443 (Industrial Automation and Control Systems Security) Standard of Good Practice for Information Security (Published by the Information Security Forum (ISF)).
- National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).
- API 1164 Pipeline Supervisory Control and Data Acquisition (SCADA) Security standard
- IEC 27019 Security Management for Process Control
- Interstate Natural Gas Association of America (INGAA) – Control Systems Cybersecurity Guidelines for the Natural Gas Pipeline Industry
- ISO 10855-1 Offshore containers design, manufacture and marking, ISO 10855-2 Offshore containers lifting sets, and ISO 10855-3 Offshore containers periodic inspection.



About the Authors



Anand Papad

Senior SCADA
Security Consultant

Papad Anand is a senior scada security consultant cybersecurity professional with over 7 years of experience. He is currently working with Payatu as a Senior SCADA Security Consultant and is implementing his relevant experience in ICS/SCADA(OT) vulnerability assessment and compliance testing.

Papad Anand has worked with Siemens and during his tenure, he audited OT environment of companies like Reliance, Amul, JSW, Aditya Birla, and etc.

Amit Musale is the Director of ICS/SCADA(OT) Security at Payatu. In his vast experience in OT Security, Amit has made significant contributions towards Industrial Cyber Security, Cyber Security for Products in OT/IoT, Embedded Software Development for Networking Products Technology / Security Management for Products in ICS/SCADA, IoT, and Automotive Embedded.

He has worked with organizations like Kuwait Oil Company, Deloitte, Emerson, and a few MNCs.



Amit Musale

Director,
ICS/SCADA(OT) Security
Payatu

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.



Critical Infrastructure Assessment [↗](#)

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure. pipeline to increase the visibility of security threats.



Product Security [↗](#)

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.



Mobile Security Testing [↗](#)

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.



Cloud Security Assessment [↗](#)

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared responsibility to secure the information stored in their cloud. Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.



Code Review [↗](#)

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.



Red Team Assessment [↗](#)

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.



DevSecOps Consulting [↗](#)

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.



Web Security Testing [↗](#)

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

IoT Security Testing



IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.



CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

More Services Offered by Payatu

- AI/ML Security Audit 
- Trainings 

More Products Offered by Payatu


- EXPLIoT 
- CloudFuzz 



Payatu Security Consulting Pvt. Ltd.

 www.payatu.com

 info@payatu.com

 +91 20 41207726

