



# Drilling Deep

A Look at Cyberattacks on the  
Oil and Gas Industry

Feike Hacquebord and Cedric Pernet



#### **TREND MICRO LEGAL DISCLAIMER**

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

**Trend Micro Research**

Written by

**Feike Hacquebord and Cedric Pernet**

Stock image used under license from  
Shutterstock.com

*For Raimund Genes (1963-2017)*

# Contents

## 5

The Infrastructure of a Typical  
Oil and Gas Company

## 7

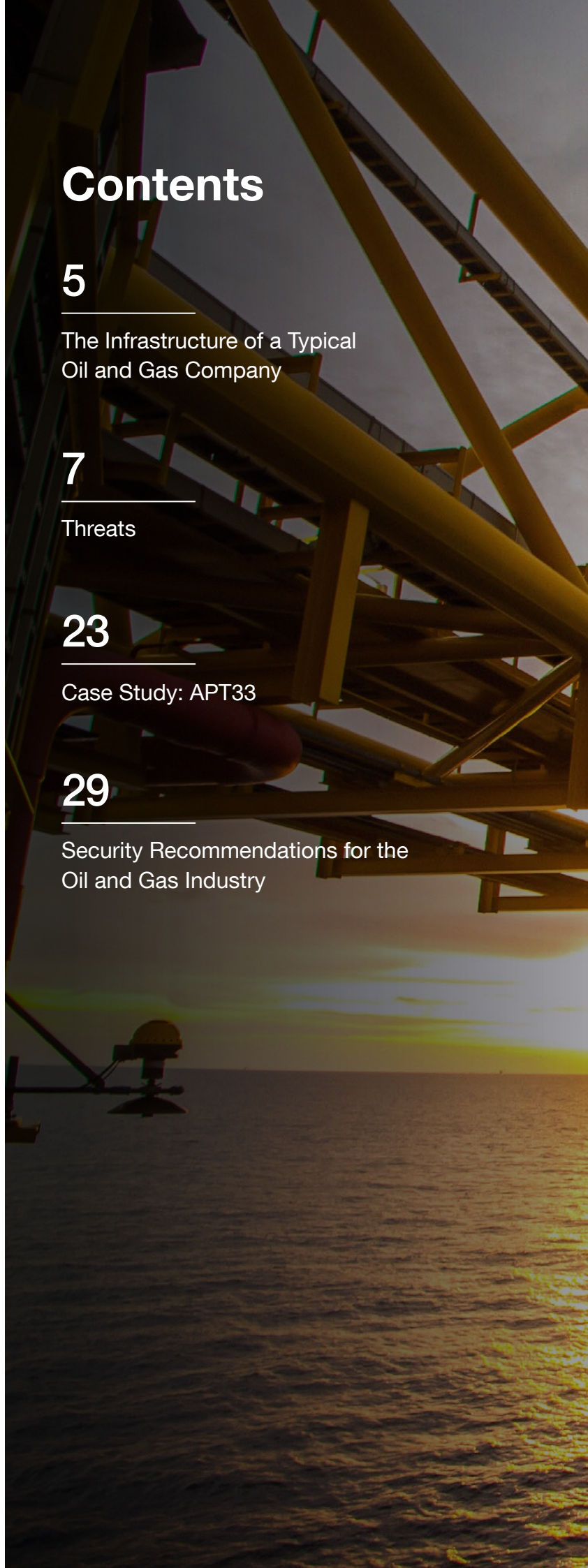
Threats

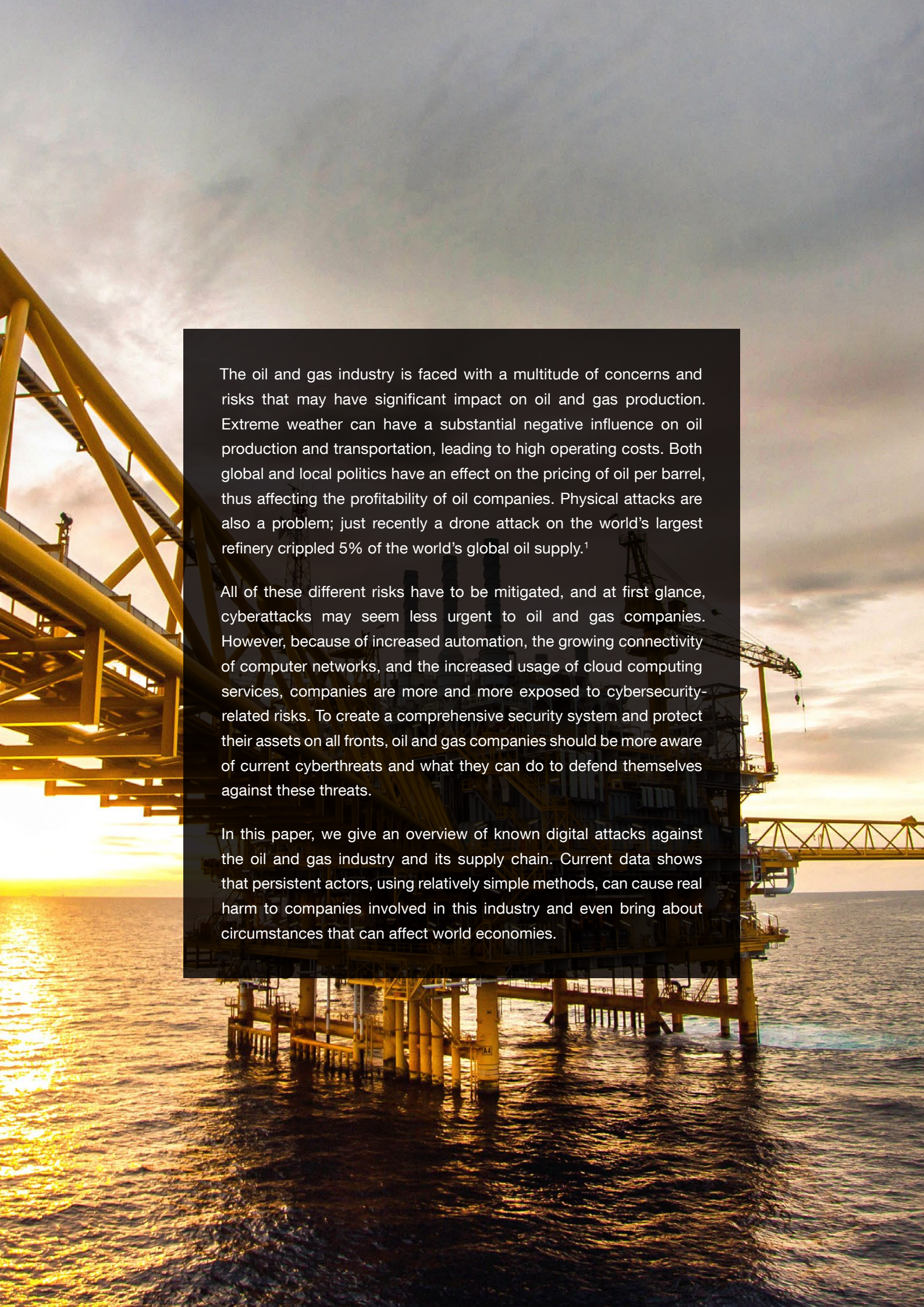
## 23

Case Study: APT33

## 29

Security Recommendations for the  
Oil and Gas Industry



A large offshore oil rig is shown against a dramatic sunset sky. The rig's complex network of yellow pipes and steel structures is silhouetted against the bright orange and yellow light of the setting sun. The ocean below is dark with some whitecaps, reflecting the low light. The overall mood is industrial and serene.

The oil and gas industry is faced with a multitude of concerns and risks that may have significant impact on oil and gas production. Extreme weather can have a substantial negative influence on oil production and transportation, leading to high operating costs. Both global and local politics have an effect on the pricing of oil per barrel, thus affecting the profitability of oil companies. Physical attacks are also a problem; just recently a drone attack on the world's largest refinery crippled 5% of the world's global oil supply.<sup>1</sup>

All of these different risks have to be mitigated, and at first glance, cyberattacks may seem less urgent to oil and gas companies. However, because of increased automation, the growing connectivity of computer networks, and the increased usage of cloud computing services, companies are more and more exposed to cybersecurity-related risks. To create a comprehensive security system and protect their assets on all fronts, oil and gas companies should be more aware of current cyberthreats and what they can do to defend themselves against these threats.

In this paper, we give an overview of known digital attacks against the oil and gas industry and its supply chain. Current data shows that persistent actors, using relatively simple methods, can cause real harm to companies involved in this industry and even bring about circumstances that can affect world economies.

Large-scale cyber intrusions on oil and gas companies are not theoretical scenarios; real-world strikes have been causing damage for years. In August 2012, one of the biggest oil companies in the world suffered from an expansive cyberattack. Tens of thousands of the company's computer servers were rendered unusable by the crippling wiper malware called Shamoon.<sup>2</sup> Although the supply of crude oil to the world was not affected at the time, the Shamoon attack proved to be a real risk to world economies. This watershed event was caused by destructive, yet relatively simple, malware.

Cyberthreats to oil companies seem to become more prevalent and urgent when political tensions rise. Oil companies are targets of cyberattacks that are rooted in political agendas and geopolitical concerns. For example, recent incidents of unrest in the Gulf Region have cascaded into cyberspace, i.e., the internet.<sup>3</sup> There has been increased interest in malware attacks that target not only the military and defense industry but also the oil and gas industry. This activity has been going on for almost a decade already.

Additional destructive attacks on the oil industry continued between 2012 and 2019 with variations of the Shamoon malware and a destructive wiper variant of the so-called StoneDrill malware. In 2018, it was reported that an Italian oil company suffered from a Shamoon wiper attack.<sup>4</sup> This time, a few hundred computer servers were hit. Around the same time, a British oil company reported it had suffered from a security breach caused by a variant of known malware.<sup>5</sup>

There are several advanced actor groups or advanced persistent threats (APTs) that target the oil and gas industry. In this paper, we describe some of the attack methods of an actor group that is commonly referred to as APT33 (also identified as Refined Kitten, Magnallium, and Elfin). APT33 is known to aggressively target the oil and gas and aviation industries and their supply chains.

In the fall of 2018, we observed that a U.K.-based oil company had computer servers both in the U.K. and India communicating with an APT33 command-and-control (C&C) server. Another European oil company also suffered from an APT33-related malware infection on one of its servers in India for at least three weeks in November and December 2018. We also found that for at least two years, APT33 used the private website of a member of the national defense committee in the senate of a European country to send spear-phishing emails to companies in the supply chain of oil products. Targets also included a water facility that supplied potable water to a U.S. military base.

In this paper, we also include our findings on the multiple layers of obfuscation that APT33 puts up to run C&C servers they use in extremely targeted malware campaigns against targets in the Middle East and the U.S.

Pawn Storm<sup>6</sup> is another threat actor group that has targeted the oil and gas industry. In particular, we have seen reconnaissance attacks on email and VPN servers of oil and gas companies originating from this group.

# The Infrastructure of a Typical Oil and Gas Company

Most of the best understood attacks against the oil industry are initial attempts to break into the corporate networks of oil companies. We will discuss several of these attacks in this paper. At the outset, it is important to understand the complete oil and gas production chain and what risks are involved in those areas. This section will discuss these concerns in detail.

The production chain, from exploring oil to producing end products like gasoline for cars, is oftentimes divided into three parts: upstream, midstream, and downstream. Processes that are related to oil exploration and production are generally referred to as upstream. Transportation and storage of crude oil through pipelines, trains, ships, or trucks are referred to as midstream. And downstream is the production of end products. Cyber risks are present in all three categories, but for midstream and upstream, there are few publicly documented incidents.

A typical oil company has production sites where crude oil is extracted from wells, tank farms where the oil is stored temporarily, and a transportation system to bring the crude oil to a refinery. Transportation may include pipelines, trains, and ships. After processing in the refinery, different end products like diesel fuel, gasoline, and jet fuel are transported to tank farms and the products are later shipped to customers.

A typical gas company also has production sites and a transportation system like pipelines, railroads, and ships. But it also needs compressor stations where the natural gas is compressed to a specific pressure to be ready for transport. The natural gas is transported to a separation plant that separates different hydrocarbon components from natural gas, like LPG and cooking gas. The different gasses are later transported to customers using pipelines, trains, and ships.

In the whole chain — from oil and gas production to refineries to the several hydrocarbon end products — constant monitoring is crucial for performance measurement, performance improvement, quality control, and safety. Monitoring metrics include temperature, pressure, chemical composition, and detection of leaks. Some oil and gas production sites are in very remote locations where the weather can be extreme. In particular for these sites, communication of the monitored metrics over the air, fixed (optic or copper) lines, or satellite is important. Likewise, remote control of on-site equipment such as valves, pumps, hydraulic and pneumatic control systems, safety instrumented systems (SISs), emergency stop systems, and fire detection equipment are crucial. All of the systems are controlled by software and can be compromised by an attacker.

Availability of these systems is key and there is usually no incentive for confidentiality. The communication of both control messages and the monitoring data is oftentimes not encrypted and not even signed for data integrity. This means that there are multiple theoretical attacks possible: sending attacker commands to control systems, injecting commands, changing sensor data, and replay attacks, among others. Fortunately, attackers are not likely to use these methods because the impact is limited by built-in mechanical safety measures that prevent hazardous situations. Also, many of these attacks would require the actor to be close to the oil well or refinery. There are only a few public reports on compromises of industrial control systems (ICSs) in the oil and gas industry, and some that describe attacks against SISs in refineries.<sup>7, 8</sup>

The more urgent threats oil and gas companies are facing come from several advanced attacker groups who are focused on this industry. Among these groups are the same actors who usually attack the military and defense industry. These attackers have geopolitical impact and espionage in mind, and in some cases are aiming to deploy destructive attacks.

Theft of intellectual property and industrial espionage are dangerous threats to oil companies too. Among valuable intellectual property typically held by these companies are the location of new proven oil reserves that are not in production yet, techniques of effective drilling, and the chemical composition of additives in premium car gasoline.

In the succeeding sections, we will discuss the internet-related threats that are relevant to the oil and gas industry. We will also give recommendations for defending oil and gas companies against each threat.

# Threats

The biggest threats the oil and gas industry have to worry about are those that have a direct negative impact on the production of their end products. Aside from these, espionage is something the industry has to defend itself against as well. Actors may steal intellectual property through these compromises, and espionage can also be the starting point of destructive attacks or sabotage that may impact companies' product supply.

## Infrastructure Sabotage

An important threat the oil and gas industry is facing is infrastructure sabotage. The initial action to sabotage infrastructure is the same as that for a usual advanced targeted attack: reconnaissance. The attacker first needs to collect information about the target and then use this information to compromise systems or computer servers on the targeted network. The attacker does not need to maintain access to the system. The attacker may also try to remove all evidence of compromise while proceeding with the sabotage.

Sabotage in this context can be done via different actions:

- Altering the behavior of software
- Deleting or wiping off specific content to disrupt the activity of the company
- Deleting or wiping off as much content as possible on every accessible machine

Some examples of these kinds of sabotage operations have been reported broadly, the most famous being the Stuxnet case.<sup>9</sup> Stuxnet was a piece of self-replicating malware that contained a very targeted and specific payload. Most infections of the worm were located in Iran and analysis revealed that it was designed to exclusively target the centrifuge in the uranium enrichment facility of the Natanz Nuclear Plant in the country. The malware targeted Siemens' WinCC/PCS 7 SCADA control software specifically, and only when it fit certain precise parameters in their configuration. It destroyed several nuclear enrichment centrifuges, which lowered the productivity of the nuclear plant. Despite the fact that Stuxnet was developed with one particular goal in mind, it did spread further within the oil industry (even without launching its dedicated payload).<sup>10</sup>

Another example is the malware Industroyer (aka Crashoverride).<sup>11</sup> This malware contains specific payloads for ICSs used in electric substations, although it can be refitted to target other types of critical infrastructure. In addition to these payloads, it contains a data wiper part that can be triggered to erase data and make systems unbootable.

The BlackEnergy malware is also of note. This malware evolved through time, from being a trojan to being a new piece of malware delivering a payload known as KillDisk. It targeted the power facility Prykarpattya Oblenergo and other electricity distribution companies in Ukraine. Research by Trend Micro also revealed that it targeted a large Ukrainian mining company and a large Ukrainian railway operator,<sup>12</sup> showing that such modular malware could be used against different industries.

There is also the Triton malware, which was built to interact with Triconex SIS controllers and could, among other features, shut them down.<sup>13</sup>

The Shamoon (aka Disttrack) campaigns, which had at least three known waves of attack from 2012 to 2018,<sup>14</sup> on oil and gas companies have been incredibly aggressive. The biggest target of these attacks, a Saudi oil company, had about 30,000 computers rendered unbootable by the destructive malware. The impact was significant since a lot of the oil company's computer servers were disrupted for weeks. However, the world oil supply was essentially not affected by these attacks.

While these examples show strong developer skills in terms of building specific malware, special malware is not always needed for attacks to be successful. Any remote access tool that could allow an attacker to gain access to a human-machine interface (HMI) for equipment would work. Also, there are cases when no outside attack is needed, as when the threat comes from within the company. The next section deals with that danger: the insider threat.

## Insider Threat

An insider — in most cases, a disgruntled employee seeking revenge or merely wanting to make easy money selling valuable data to competitors — can commit sabotage operations. Although there are several factors that can motivate a person to turn against their employer, revenge is the more dangerous type since the individual could not care less which part of the company is targeted. Blackmail can also be a motivation for an inside job.

An insider may do the following:

- Altering data to create problems, misuse access, or cause damage
- Deleting or destroying data from corporate servers, shared project folders, or any location the insider has access to
- Stealing intellectual property for the insider's own use or for a competitor's
- Leaking sensitive corporate documents to third parties or competitors, or even uploading them to the internet

Defense against insider threats is very complex, since insiders generally have access to a lot of data. In addition, unlike an external attacker, an insider does not need months to know the internal network of the company — the insider probably already has knowledge of the inner workings of the organization. With that knowledge, the insider probably knows how to inflict damage to the company's business more than any external attacker.

Careful monitoring of user activity can bring this kind of activity to light, but the task is still very difficult. It might be difficult to distinguish the usual daily operations from sabotage actions — for example, simple actions like modifying a document or deleting a file could be part of a sabotage attempt.

## Espionage and Data Theft

While sabotage of the daily operations is among the most damaging attacks on the oil and gas industry, data theft and espionage are important threats the industry needs to be aware of as well. As mentioned above, data theft and espionage can be the starting point of a larger destructive attack. Attackers often need specific information before attempting further action. Obtaining sensitive data like well drilling techniques, data on suspected oil and gas reserves, and special recipes for premium products can also translate to monetary gain for attackers.

In the next sections, we will discuss some of the advanced espionage and theft techniques and security concerns that affect the oil and gas industry.

## DNS Hijacking

DNS hijacking is a particularly dangerous attack used by a limited set of advanced attackers. The aim of DNS hijacking may include getting access to the corporate VPN network or corporate emails of governments and companies. This is particularly relevant for the oil industry, as we have seen a number of oil companies being targeted by advanced attackers who probably have certain geopolitical goals in mind.

In DNS hijacking, the DNS settings of a domain name are modified by an unauthorized third party. The third party can, for instance, add an additional entry to the zone file of a domain or alter the resolution of one or more of the existing hostnames. The simplest things the attacker can do are committing vandalism (defacement), leaving a message on the hijacked website, and making the website unavailable. This will usually be noticed quickly and the result may just be reputational damage. However, there are more dangerous attacks possible, with a much bigger impact: theft of corporate credentials, interception of emails, VPN access to the corporate network, and launching a watering hole attack. Ultimately, these may even lead to lasting access to the victim's network by an unauthorized third party. An actor can, for example, use the (short) time window of the DNS hijack to send internal malware-ridden emails using credentials intercepted during the hijack.

DNS hijacking attacks can happen by targeting registrants of a domain name. But many registrars and DNS providers have two-factor authentication in place for their customers. Two-factor authentication raises the bar significantly for a successful attack. More dangerous actors may use different tactics that the domain owner cannot easily repel.

One possible scheme involves an actor not attacking the registrant of a domain directly, but instead the registrar of the domain or even registries. More specifically, the actor can try to compromise the registrar's credentials for the management system that is used to push changes on domains to Whois registries and DNS root servers. Once the registrar is compromised, the actor can push specific changes for the domains that are under control of the registrar. For example, the actor can change the legitimate authoritative nameservers to other nameservers under the actor's control. Once that has succeeded, the actor can point domains to a foreign IP he controls.

We have seen these attacks targeting mail servers of government agencies in particular, and there are serious possible compromise scenarios. When the attacker is also able to create a valid, new SSL certificate of the hijacked domain, the attacker can even intercept SSL connections to the corporate servers and potentially intercept corporate credentials that are sent to a hijacked version of the IMAP server. To create an SSL certificate of a domain the attacker doesn't own, the attacker usually has to show ownership of the domain. When the attacker is able to intercept emails to the domain owner, the attacker may be able to fool a certificate authority and pose as the legitimate owner of a domain. With that, a valid SSL certificate may be issued.

There are ways to raise the bar for DNS hijack attacks. First of all, the use of multi-factor authentication will make attacks more difficult, though not impossible. As explained in a talk by Bill Woodcock, the executive director of Packet Clearing House,<sup>15</sup> using Domain Name System Security Extensions (DNSSEC) validation for all email clients also helps. In the event that the IMAP server domain gets hijacked, the email clients won't make a connection to the foreign IP address as the DNSSEC validation fails. In his talk, Woodcock says the use of mobile device management (MDM) is advised as well, to force mobile users who are not in the office to use the right recursive DNS servers that implement DNSSEC validation.

While most DNS hijacking attacks<sup>16</sup> have happened against government organizations, some oil companies have been affected too. Most likely, these oil companies fell victim to politically motivated attacks such as the incidents that happened in 2018 and 2019 in the Middle East. These attacks might have resulted in interception of emails, interception of corporate credentials, temporary access to the corporate VPN, and even semi-persistent access to the corporate network.

The risk of DNS hijacking can be further reduced by a couple of additional measures. First, a script can check the DNS records of the critical domains and hostnames of an organization frequently — every minute or as often as may be desired. By walking down the whole DNS hierarchy for crucial domain

names starting from the root servers, the script can quickly notice any unauthorized changes in the chain. If this monitoring is done frequently enough, the potential damage can be limited significantly.

Once an organization has become a victim of a DNS hijack attack and the DNS settings have been restored to normal, it is important to note that crucial information might have been stolen, such as corporate credentials. Obviously, passwords should be reset. Also, if, for example, the webmail or mail domain was hijacked, that might have just been a way for the attacker to get into systems and get persistent access to the network with malware or gain unauthorized VPN access. In that case, a full security sweep of the corporate network will be necessary.

DNS hijack attacks can also be used to plant an exploit on a hijacked website with an audience the attacker is interested in. For example, we saw that during an attack in 2019 the personal blog of a prolific member of an American think tank was hijacked. While we were unable to reproduce what happened exactly on the hijacked domain, an obvious case scenario would be a watering hole attack. This watering hole could then infect the readers of the blog during the DNS hijack.

## Attacks on Webmail and Corporate VPN Servers

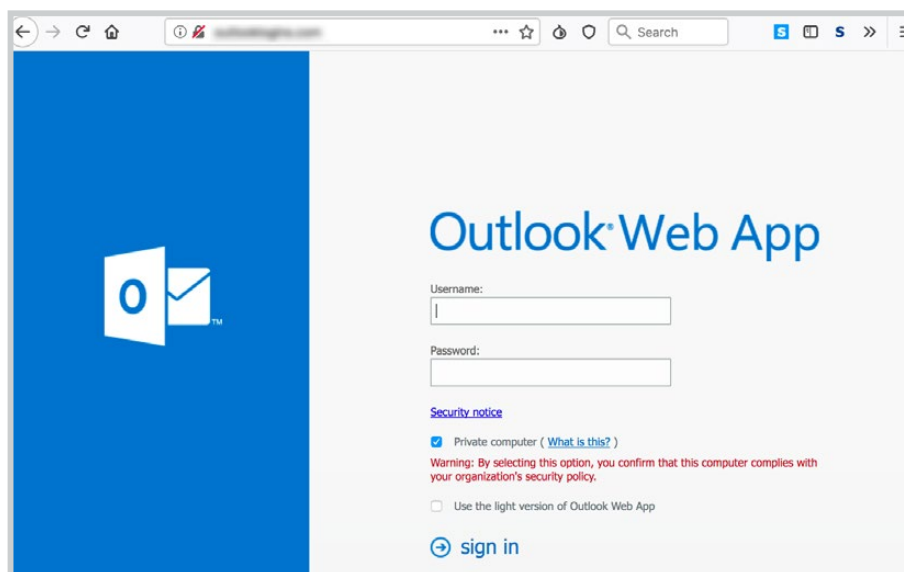


Figure 1. An example of a phishing site of APT33

Webmail is a very useful tool for individuals who want to have access to their emails while on the road. The same holds for file-sharing services from third-party service providers with which employees can work together on a project. However, these services increase the attack surface. For example, a webmail hostname might get DNS-hijacked or hacked because of a vulnerability in the webmail software. Webmail and file-sharing and collaboration platforms can be compromised in credential-phishing attacks. A well-prepared credential-phishing attack can be quite convincing, as when an actor registers a domain name that resembles the legitimate webmail hostname, or when an actor creates a valid SSL certificate and

chooses the targets within an organization carefully. The risk of webmail and third-party file-sharing services can be greatly reduced by requiring two-factor authentication (preferably with a physical key) and corporate VPN access to these services.

However, VPN credentials and one-time passwords can be phished as well. There have also been critical vulnerabilities in VPN software and some webmail software that could give third parties unauthorized access. It is very important to patch these vulnerabilities as soon as security updates are ready to be installed. We have seen that advanced attackers scan VPN servers and webmail servers, hunting for exploitable vulnerabilities. In September 2019, an APT actor scanned servers running specific VPN software, including those in a state-owned oil company. And in October 2019, Pawn Storm (aka APT28 or Sofacy) scanned the mail servers of several oil companies in the U.K.

## Data Leaks

Data leaks have always been problematic for companies across industries. The oil and gas industry, in particular, is very competitive and almost any kind of leaked information can be beneficial to a competitor. Data leaks can also cause substantial damage to a company's reputation. It has been said for decades that data should be carefully handled inside companies, yet this is not enough. Outside monitoring should be put in place as well.

What happens when data that is carefully handled internally is sent to an outside partner? What happens when a company uses unfamiliar tools and software? What happens when a company does not know that the software shares files on remote servers? And what happens when those files are stored on unsecure external networks, in some cases becoming freely accessible even to anyone who knows the data is there? Needless to say, these are serious issues that should be considered by all companies.

In the course of our research, we easily found dozens of sensitive documents related to the oil industry online. One way of finding these documents is by using specially crafted Google queries, called Google Dorks. We will not show any of these search engine queries in this research paper since the matter is very sensitive and we do not want to help cybercriminals. Some redacted examples of data we could retrieve are below.

Another way to find such content is to hunt for data on public services like Pastebin, an online service that allows anyone to copy and paste any text-based content and store it there, privately or publicly. Another source of data is public sandboxes meant for analysis of suspicious files. Users can mistakenly send legitimate documents to these sandboxes for analysis. Once uploaded, these documents can be parsed or downloaded by third parties.

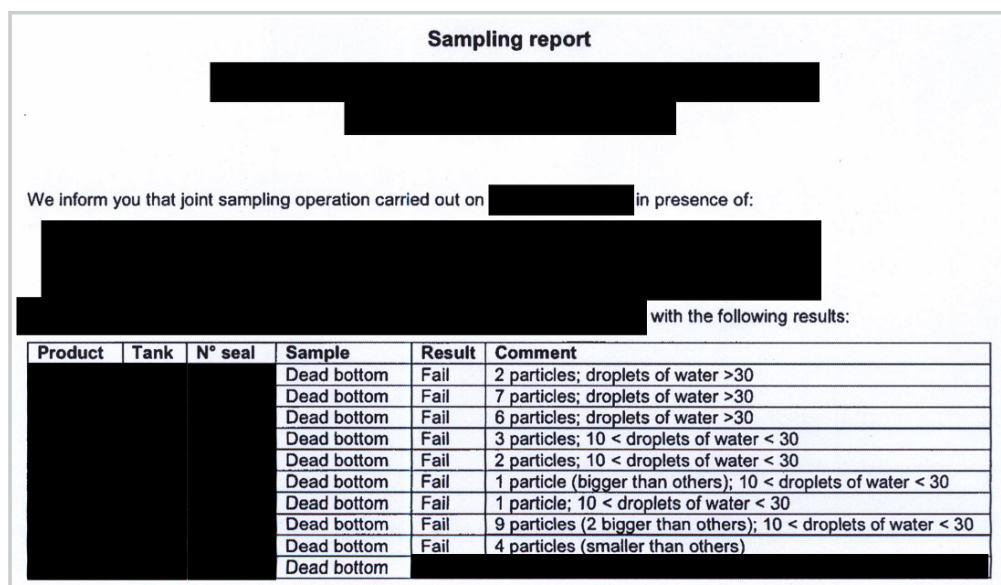
These are several common security lapses that companies should correct in regard to document storage:

- Documents are stored on a web server in a folder that is world-readable.
- Documents are stored on a file server without proper access control.
- Documents are backed up on an unsecure server accessible to anyone.

While it is not a problem to see official documents that were meant for publication online in different locations, it becomes problematic when the documents are internal only or require a security clearance. Those document leaks can affect the “victim” company in several ways:

- Affects one or several company employees
- Affects the company’s public image
- Leaks nondisclosure agreements (NDAs) or contracts signed between a company and a third party
- Leaks information that can be leveraged by competitors
- Leaks information that can be used legally against the company
- Leaks information that can harm long-term projects or road maps

This is particularly significant in the energy industry, where most information is usually kept internal.



**Sampling report**

[Redacted]

We inform you that joint sampling operation carried out on [Redacted] in presence of:

[Redacted]

[Redacted] with the following results:

Product	Tank	N° seal	Sample	Result	Comment
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	2 particles; droplets of water >30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	7 particles; droplets of water >30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	6 particles; droplets of water >30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	3 particles; 10 < droplets of water < 30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	2 particles; 10 < droplets of water < 30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	1 particle (bigger than others); 10 < droplets of water < 30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	1 particle; 10 < droplets of water < 30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	9 particles (2 bigger than others); 10 < droplets of water < 30
[Redacted]	[Redacted]	[Redacted]	Dead bottom	Fail	4 particles (smaller than others)
[Redacted]	[Redacted]	[Redacted]	Dead bottom	[Redacted]	[Redacted]

Figure 2. A sampling report sent from a private laboratory to an oil company

An example is a full document we recently found sent from a laboratory to an oil company, providing the exact location, ship name, and results for particular oil particles (SN100, SN150) hunting. Information on a potential contamination is confidential and sensitive for any company in the oil and gas industry and should not be publicly available.

## External Emails

While emails are generally well protected inside companies, external emails cannot be controlled the same way. Employees regularly send emails to external addresses, hence some sensitive internal content ending up outside the company's purview. Even worse, sensitive information can be copied to unsecure backup systems or stored locally on personal computers without standard corporate security protocols, which makes it easier for attackers to get hold of the information. Once a computer is compromised, an attacker can get the emails and use them in different ways to harm a company. For example, an actor could leak them on public servers or services like Pastebin.

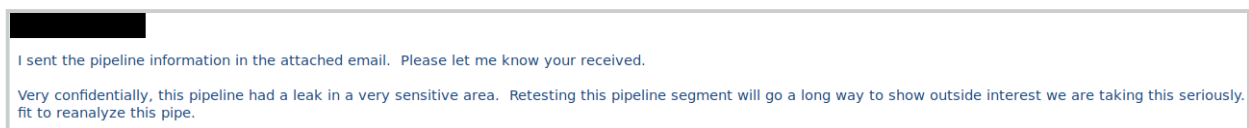


Figure 3. Sample content from an email found in the wild, sent from an oil company employee to a third-party service provider

Even to someone not knowledgeable about the industry, it becomes clear that interesting information is found when an email starts by mentioning a level of confidentiality.

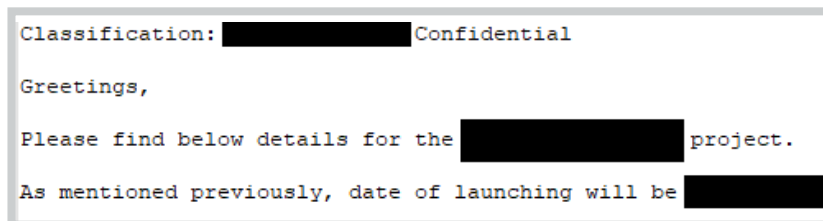


Figure 4. Sample content from an email found in the wild indicating a "confidential" level of information

## Defending Organizations Against Data Leaks

A company can identify leaked documents only if it has solid knowledge of all internal documents. Therefore, any important document inside the company should be watermarked in a way that makes it discoverable on the internet, since constantly monitoring for specific marks makes finding leaked documents easier.

Google Dorks based on documents' characteristics and contents — it can be as simple as searching for specific names associated with the word "confidential," for example — and searches on online services like Pastebin<sup>17</sup> should be done daily. The frequency is necessary since companies should be as reactive as possible when a document appears in public or somewhere where it should not be.

Data leaks will happen at some point, whether by "bad handling or mistakes" or by malicious exposure. The important thing is to find them before someone with bad intentions does, and have them removed quickly.

One of the first steps in mitigating the risk of data leaks is to make a list of keywords that are critical to a company. Specific watermarks of sensitive documents should also be collected. Automated search queries for these keywords and watermarks on the internet can then be set up with a script. Even better, a company can outsource all monitoring and data leak prevention to an external service provider that specializes in preventing and mitigating data leaks.

## Ransomware

In the past, cybercriminals were spreading ransomware wherever they could, mostly using spam botnets to try to infect as many machines as possible. While it remains a serious threat to any individual who stores data on their computer, ransomware has become an even larger threat as ransomware actors have been targeting companies specifically, with attacks that may have a big impact on daily operations.

Targeting individuals is fairly easy for cybercriminals, even for those with a low level of computer knowledge. The easiest business model consists of subscribing to ransomware-as-a-service (RaaS) offers on underground cybercrime marketplaces.<sup>18</sup> Any fraudster can buy such a service and start delivering ransomware to thousands of individuals' computers by using exploit kits or spam emails.

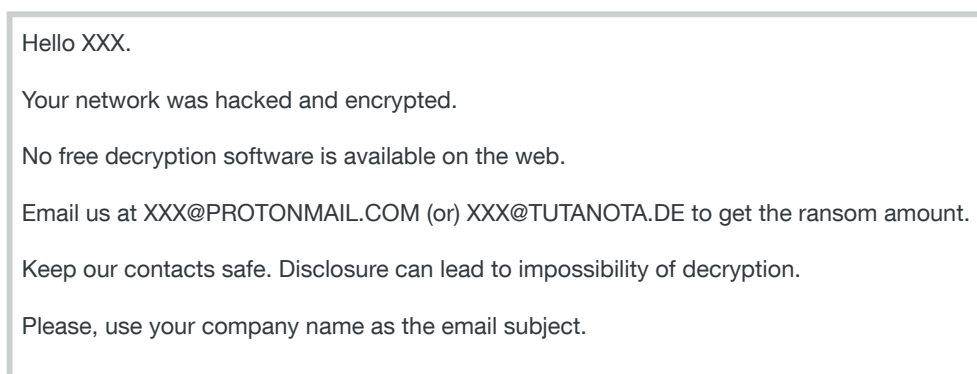
Targeting companies and organizations takes more effort. Infecting a company with ransomware the same way it is done with individuals is inefficient because the goal is not about infecting a few computers. Typically, an actor will try to disrupt a whole company. To this end, the attacker needs to spend time “profiling” its target entity, collecting information about it, much in the same way as the attacker would do in a targeted attack.

That reconnaissance phase is necessary for the attacker to get to the next stage: compromising one or several of the target computers, generally via specially tailored spear-phishing emails or by exploiting an unsecure Remote Desktop Protocol (RDP) connection. Once inside a network, the attacker will try to move laterally and then carefully choose a moment to drop ransomware either on selected servers or massively across the network. The end goal is to render the company unable to operate its normal business or unable to recover its lost data (for example, by tampering with the backup system), so that it is more likely to pay the ransom.

We found that a U.S. oil and natural gas company was hit by ransomware, infecting three computers and its cloud backups. The computers that were targeted contained essential data for the company, and the estimated total loss was more than US\$30 million. While we do not have additional details on this case, we believe the attackers did plan this attack carefully and were able to target a few strategic computers rather than hitting the company with a massive infection.

More recently, we discovered a variant of the ransomware family BitPaymer<sup>19</sup> that had targeted a U.S. company specializing in providing services for oil well drilling. The actors behind BitPaymer typically use spear phishing to infect their targets with initial malware, before spending time moving laterally and compromising the network further. They plant the ransomware in specific spots in the network and launch the malware, for example, on a Saturday night. They are efficient and dangerous, and they know how to take advantage of the absence of IT people during weekends or holidays to infect selected machines and encrypt the contents.

The ransom message of BitPaymer is the same for every target, except for the first line, where the company name is written, and the email addresses for reaching the fraudsters.



Hello XXX.

Your network was hacked and encrypted.

No free decryption software is available on the web.

Email us at XXX@PROTONMAIL.COM (or) XXX@TUTANOTA.DE to get the ransom amount.

Keep our contacts safe. Disclosure can lead to impossibility of decryption.

Please, use your company name as the email subject.

Figure 5. The ransom message from the latest variants of BitPaymer (company name and email addresses of fraudsters removed)

## Ever-changing Malware

Malware is an important part of targeted threat actors' arsenal. Different kinds of malware serve different purposes and have different ways of functioning and communicating between the infected computers and the C&C servers.

Threat actors targeting oil and gas companies for cyberespionage definitely want to stay undetected inside their target's network. Compromising and planting malware inside a target network is just the initial stage for attackers. Yet for a number of reasons, these actions can be detected after a while or even just deleted automatically by any antivirus or security solution.

To avoid being kicked off from the network when the only available access is via their malware, attackers generally choose to regularly update their malware. And if possible, they use different malware families so that they have more than one way to access the compromised network.

Malware updates can be functionality or code updates, or sometimes just slight modifications for avoiding detection.

Cybercriminals working with malware often use online testing platforms like VirusTotal to check whether their files are detected by different security products. Some threat actors run their own testing platforms for better operational security reasons. They do not send their files to any third party and they want to be sure the files are not known to security companies before a campaign starts to spread them in the wild. Trend Micro has successfully collaborated with law enforcement to take some of these platforms down (such as Scan4You<sup>20</sup> and Refud.me<sup>21</sup>) and help catch the cybercriminals behind them.

Once a file has a “close to zero” or even zero detection rate, it becomes “FUD” (fully undetectable) and it can be used in an attack. In order to alter the malware well enough to become undetectable, attackers often use crypter software, which refers to programs that modify and obfuscate binaries to escape detection. Attackers can also note the exact security products used by the target, and only consider bypassing that one and not care about others.

In the next sections, we will discuss some of the most common malware types and tools that are used against the oil and gas industry.

## Webshells

Webshells are tiny files, generally written in PHP, ASP, or JavaScript language, that have been fraudulently uploaded to a web server belonging to a targeted entity. An attacker just needs to browse to it to get access to the web server. Most common options for webshells provide upload or download file operations, command line (shell), and dump databases.

Webshells can also be tiny files connecting back to a server that listen for communications.

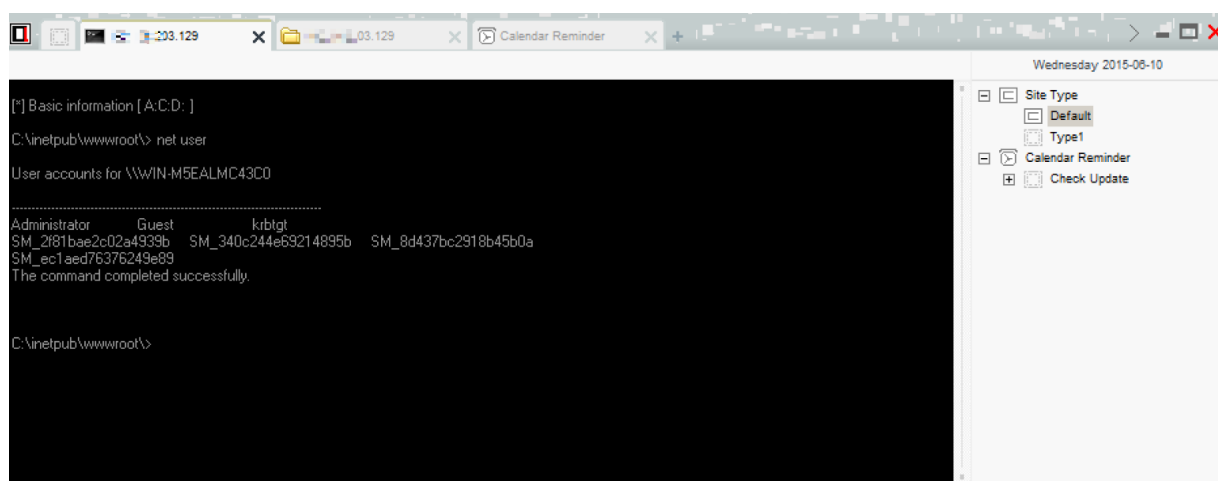


Figure 6. Webshell example: A shell window opened in the China Chopper webshell GUI

Threat actors sometimes use webshells to ease their operations, generally at an early infection stage. They can use webshells to:

- Download or upload files to the compromised web server.
- Run other tools (such as credential stealers).
- Maintain persistence on the compromised infrastructure.
- Bounce to other servers and move on with more compromises.
- Steal information.

Threat actors that target the oil industry, like OilRig, have typically used webshells (TwoFace, DarkSeaGreenShell, possibly more) to serve most of these purposes.

## Cookies

Cookies are small files sent from web servers and stored in the browser of an internet user. They serve different legitimate purposes, such as allowing a browser to know if the user is logged in or not (as in the case of authentication cookies) or storing stateful information (like items in shopping carts).

Some variants of the backdoor BKDR64\_RGDOOR<sup>22</sup> used cookies<sup>23</sup> to handle communications between the malware and its C&C server. They used the string “RGSESSIONID=” followed by encrypted content. Careful cookie field monitoring in HTTP traffic can help detect this kind of activity.

## DNS Tunneling

While the most common way for malware to communicate with its C&C server is by using the HTTP or HTTPS protocol (usually to evade firewall rules or filtering), some attackers allow their malware to communicate via DNS tunneling. The technique is not new and has its limitations, which is why it is not seen quite often in APT attacks. But some actors do like using it, such as OilRig and GreenBug.

DNS tunneling in this context exploits the DNS protocol to transmit data between the malware and its controller, via DNS queries and response packets.

The DNS client software (the malware) sends data, generally encoded in some ways, prepended as the hostname of the DNS query. As an example, the malware might want to send a username “prouser1” to the controller. The malware encodes this username in Base64 format:

```
prouser1 => cHJvdXNlcjE
```

The malware then sends the following DNS query:

```
cHJvdXNlcjE.c2serverdomainname.com
```

In this fictional example, the domain `c2serverdomainname.com` is owned and controlled by the attacker, and points its nameserver (NS) records toward the server where DNS tunneling server software (the controller) is running.

The server can then reply to the DNS query with different kinds of answers. Data can, for example, be sent to the malware in the answered query via the CNAME record, or in the TXT field, or others.

Real examples from the wild have affected the oil and gas industry. The Alma communicator DNS tunneling trojan<sup>24</sup> used by OilRig uses encryption to send data back and forth via DNS tunneling. The ISMDoor malware also uses similar techniques.<sup>25</sup>

The limitation of the DNS tunneling technique resides in the length of data that can be transmitted per request. In the best case, via the TXT record, for example, only 255 bytes can be sent at a time. If the attacker needs to send more, the attacker needs to use several DNS queries.

Careful examination of the DNS requests sent from an infrastructure can be very effective in detecting DNS tunneling.

## Email as a Communication Channel

It is possible for an attacker to use email as a communication channel between the attacker's malware and its controller. While it might sound very amateurish for senior computer security professionals because this method has typically been used by novice malware writers, it can still be seen in the wild.

An APT attacker might want to use this method mostly for two reasons: email services, especially external online services, might be less monitored than other services in the compromised network, and it might provide an additional level of anonymity depending on the email service provider that is used.

In a typical scenario, the malware logs on the email service and reads emails from the inbox, which contain instructions from the malware controller. It can also use the service to send data back.

One example of this modus operandi from a threat actor targeting the oil and gas industry is Kimsuky. This threat actor actively used this method with the malware `BKDR_KIMSUK.A`,<sup>26</sup> which used a free email service to communicate.

It is difficult to detect such behavior on the network, since legitimate users are generally allowed to use free email services and traffic is often SSL-encrypted.

## Zero-day Exploits

It is still a popular thought that all advanced targeted attacks use zero-day exploits and sophisticated code to infect corporate computers and gain full access to the network infrastructure of a company. But this is not what usually happens in the real world of targeted attacks. Oftentimes, attackers limit themselves to the use of known exploits, and they use zero-day exploits only when really necessary.

It actually does not take much effort to compromise most networks, gain access, and exfiltrate information with standard malware and tools. Of course, some threat actors have more weapons than others, and those weapons may include zero-day exploits.

The Stuxnet case has been an interesting one in this respect, with the use of four different zero-day exploits. No other known attack has been seen exploiting so many unpatched and unknown vulnerabilities — it has shown an extraordinary level of sophistication.

Two years before Stuxnet, another malware from the Equation group<sup>27</sup> was using two of the four zero-day exploits that Stuxnet used. The Equation group targeted many different sectors, including oil and gas, energy, and nuclear research. It showed advanced technical capabilities, including infecting the hard drive firmware of several major hard drive manufacturers, which had seemed impossible without the firmware source code.

Other cases affecting the oil and gas industry have been reported by the media. The Reaper threat actor, for example, used a zero-day exploit abusing Adobe Flash, and also sometimes exploited recently patched vulnerabilities. Also, just recently, an actor group was actively scanning for vulnerable VPN servers, including VPN servers of oil companies.

## Mobile Phone Malware

The use of mobile phone malware has increased slowly in recent years. While it is mostly used for cybercrime, it can also be used for espionage.

The Reaper threat actor has developed Android malware,<sup>28</sup> which we detect as AndroidOS\_KevDroid. This malware has several functionalities, including starting video or audio recording, downloading the address book from the compromised phone, fetching specific files, and reading SMS messages and other information from the phone.

The MuddyWater APT group<sup>29</sup> has used several variants of Android malware (AndroidOS\_Mudwater.HRX, AndroidOS\_HiddenApp.SAB, AndroidOS\_Androrat.AXM and .AXMA) posing as legitimate applications. These malware variants have the capability to completely take control of an Android phone, spread infecting links via SMS, and steal contacts, SMS messages, screenshots, and call logs.

```

public class AppProtocol {
    public static final int DELETE_CLIENT = 210;
    public static final int DO_BRUTE_FORCE = 102;
    public static final int DO_PORT_SCAN = 103;
    public static final int GET_ALL_CONTACT = 206;
    public static final int GET_ALL_SMS = 205;
    public static final int GET_ALL_SMS_SENT = 212;
    public static final int GET_ALL_SYSTEM_INFO = 204;
    public static final int GET_CLIENT_DONE = 105;
    public static final int GET_CLIENT_NUM = 209;
    public static final int GET_COMMAND = 214;
    public static final int GET_CONTACT = 203;
    public static final int GET_PERSONAL_INFO = 213;
    public static final int GET_SMS = 202;
    public static final int GET_SMS_RECEIVED = 211;
    public static final int GET_SYSTEM_INFO = 201;
    public static final int IS_CLIENT_CONNECTED = 106;
    public static final int IS_SERVER_ALIVE = 299;
    private static final int PRE_INDEX = 200;
    private static final int ROBOT_PRE_INDEX = 100;
    public static final int SEND_SMS = 207;
    public static final int SEND_SMS_TO_ALL = 208;
}

```

Figure 7. A list of commands supported by the Android malware AndroidOS\_Mudwater.HRX

In most cases, mobile phone malware poses as known legitimate software as a lure to infect unsuspecting users. For example, users may think they are downloading the latest version of Signal or Telegram while they are in fact being infected by malware.

## Bluetooth

Bluetooth can also be exploited by threat actors. And one of the most interesting recent discoveries in this regard is the USB Bluetooth Harvester.<sup>30</sup> It is very uncommon, but it highlights the need for organizations to stay up to date on threat actor developments.

Reaper has deployed malware (TrojanSpy.Win32.BLUEHARV.A) that steals Bluetooth devices' information. When it is run, it collects basic information on connected Bluetooth devices, such as the device names, addresses, classes, and a few additional status flags.

## Cloud Services

There are many ways for attackers to try to render the traffic between their malware and the C&C server undetectable. One of these is to use legitimate cloud services to handle the communications between the malware and the controller. The Slub malware,<sup>31</sup> for example, has been used for APT attacks. While it has not affected the oil and gas industry yet, it bears mentioning here as its use of GitHub, a software development platform, and Slack, a collaborative messaging service, for C&C communication can easily be copied by other threat actors.

More interestingly, MuddyWater has used Telegram, a messaging service with end-to-end encryption, to exfiltrate data from one of its Android malware variants.<sup>32</sup> Another of MuddyWater's malware variants has used the API for the online storage service Dropbox. The malware stores all commands from the controller and their results in the cloud.<sup>33</sup>

C&C connections to cloud services are difficult to detect since they are using normal services that any employee can use for legitimate purposes. One way to prevent attacks that take advantage of cloud services is to blacklist all of these services. However, this is likely to reduce the company's efficiency and generate discomfort for employees.

## Case Study: APT33

In this section, we will focus on some aspects of an actor group called APT33. APT33 is generally considered to be responsible for many spear-phishing campaigns targeting the oil industry and its supply chain. A lot has been published about APT33 already, but we will highlight some facts that were not published before the release of our earlier blog post.<sup>34</sup> In particular, we will describe what measures APT33 takes to obscure a dozen live C&C servers that have been used in extreme narrow targeting since about 2016. We will also list IP addresses that have been used by APT33 to do reconnaissance and botnet management since 2018.

APT33 is known to target not only the oil supply chain but also the aviation industry and military and defense companies. We have observed that the group has had some limited success in infecting targets related to oil, the U.S. military, and U.S. national security. For example, we found that in 2019 APT33 was able to infect a U.S. company providing supporting services to national security.

APT33 has also compromised oil companies in Europe and Asia. A large oil company with a presence in the U.K. and India had concrete APT33-related infections in the fall of 2018. Some of the IP addresses of the oil company communicated with the C&C server *times-sync.com*, which hosted a so-called Powerton C&C server from October to December 2018, and then again in 2019. A computer server in India owned by a European oil company communicated with a Powerton C&C server used by APT33 for at least three weeks in November and December 2019. We also observed that a large U.K.-based company offering specialized services to oil refineries and petrochemical installations was likely compromised by APT33 in the fall of 2018.

APT33 has attacked the supply chain of the oil industry broadly. For about two years, multiple spear-phishing campaigns of APT33 were sent from a compromised private website of a politician who had a seat in the defense committee of the senate in a European country. The targets of these campaigns included companies that operated oil tankers, IT companies that specialized in the oil industry, a publisher of an online magazine that covered news on oil, and several manufacturers of valves and other industrial equipment. APT33 has also been targeting a water facility that supplies potable water to a U.S. military base for several years. But recent attack waves of APT33 indicate that the actor group has been targeting companies more narrowly.

APT33's best-known infection technique has been using social engineering through emails. It has been using the same type of lure for several years: a spear-phishing email containing a job opening offer that may look quite legitimate. There have been campaigns involving job openings in the oil and aviation industries.

Date	From Address	Subject
Dec. 31, 2016	recruitment@alsalam.aero	Job Opportunity
April 17, 2017	recruitment@alsalam.aero	Vacancy Announcement
July 17, 2017	careers@ngaaksa.com	Job Openning
Sept. 11, 2017	jobs@ngaaksa.ga	Job Opportunity
Nov. 20, 2017	jobs@dyn-intl.ga	Job Openning
Nov. 28, 2017	jobs@dyn-intl.ga	Job Openning
March 5, 2018	jobs@mail.dyn-corp.ga	Job Openning
July 2, 2018	careers@sipchem.ga	Job Opportunity SIPCHEM
July 30, 2018	jobs@sipchem.ga	Job Openning
Aug. 14, 2018	jobs@sipchem.ga	Job Openning
Aug. 26, 2018	careers@aramcojobs.ga	Latest Vacancy
Aug. 28, 2018	careers@aramcojobs.ga	Latest Vacancy
Sept. 25, 2018	careers@aramcojobs.ga	AramCo Jobs
Oct. 22, 2018	jobs@samref.ga	Job Openning at SAMREF

Table 1. Known job offering campaigns of APT33

The emails contain a link to a malicious .hta file. This .hta file will attempt to download a PowerShell script, which may download additional malware from APT33 so that the group can gain persistence in the network of the target. Some of the malware is quite generic in nature, while the others seem to be used by APT33 alone. Table 1 lists some of the campaigns we were able to recover from data based on feedback from the Trend Micro™ Smart Protection Network™ infrastructure. The company names in the campaigns are not necessarily targets in the campaign, but they are usually part of the social lure used in the campaigns.

**MAILER INBOX SENDER #2014**

**SMTP SETUP**

SMTP Login: <input type="text"/>	SMTP Pass: <input type="password"/>
Port : <input type="text"/> (optional)	SMTP Server Smtip: <input type="text"/>
SSL Server: <input type="checkbox"/> (yes)	Reconnect After: <input type="text"/> EMAILS

" If you dont have SMTP login, leave blank queries above "

**MESSAGE SETUP**

Your Email: <input type="text"/>	Your Name: <input type="text"/>
Reply-To: <input type="text"/>	Email Priority: - Please Choose - <input type="button" value="v"/>
Subject: <input type="text"/>	

Encode sending information ? ☒ yes

☐ Plain
☒ HTML

Figure 8. PHP mailer script probably used by APT33. The script was hosted on the personal website of a European senator who had a seat on his nation's defense committee.

The job opening social engineering lures are used for a reason: Some of the targets actually get legitimate email notifications about job openings for the same companies used in the spear-phishing emails. This means that APT33 has some knowledge of what their targets are receiving from legitimate sources.

APT33 is known to be related to the destructive malware called StoneDrill and is possibly related to attacks involving Shamoon, although we don't have solid evidence for the latter.

Besides the relatively aggressive attacks of APT33 on the supply chain, we found that APT33 has been using several C&C domains, listed in Table 2, for small botnets composed of about a dozen bots each. It appears that APT33 has taken special care to make tracking more difficult.

The C&C domains are hosted on cloud-hosted proxies. These proxies relay URL requests from the infected bots to back-ends at shared web servers that may host thousands of legitimate domains. These back-ends are protected with special software that detects unusual probing from researchers. The back-ends report bot data back to a dedicated aggregator and bot control server that is on a dedicated IP address. The APT33 actors connect to these aggregators via a private VPN with exit nodes that are changed frequently. Using these VPN connections, the APT33 actors issue commands and retrieve data from the bots. In the fall of 2019, we counted 10 live bot data-aggregating or bot-controlling servers, and we tracked a couple of these servers for months. These aggregators get data from typically very few C&C servers (around one or two). For every unique C&C domain, there are usually only a dozen or fewer victims.

Domain	Date created
oorgans.com	May 28, 2016
suncocity.com	May 31, 2016
zandelshop.com	June 1, 2016
simsoishop.com	June 2, 2016
zeverco.com	June 5, 2016
qualitweb.com	June 6, 2016
service-explorer.com	March 3, 2017
service-norton.com	March 6, 2017
service-eset.com	March 6, 2017
service-essential.com	March 7, 2017

Table 2. APT33 C&C domains for extreme narrow targeting

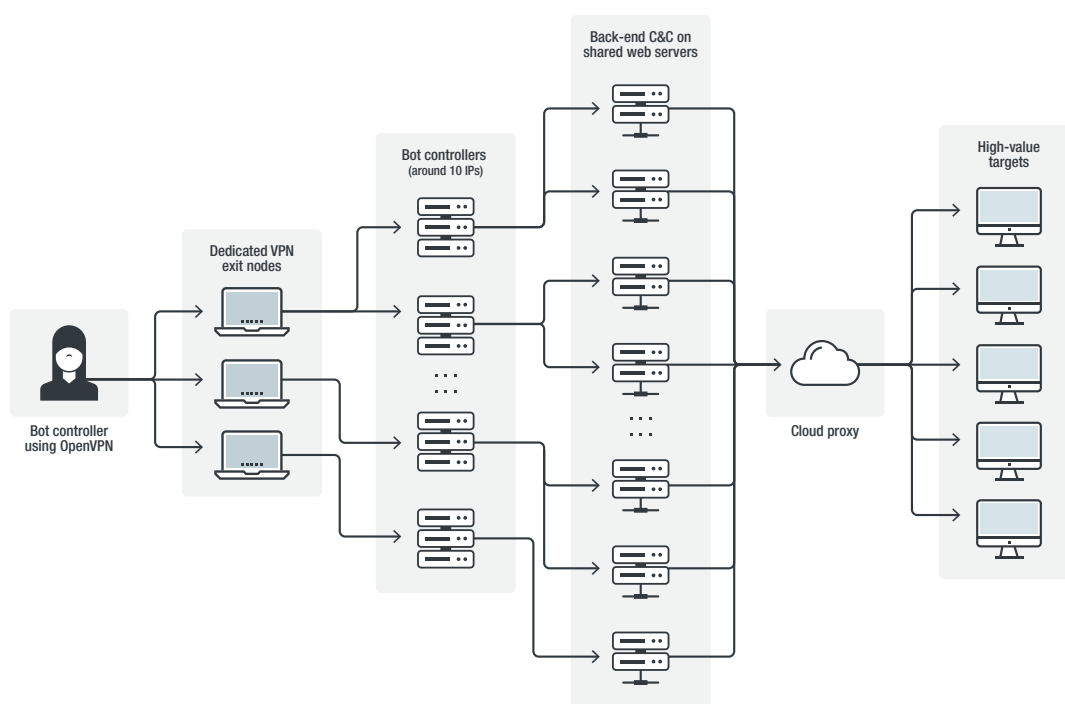


Figure 9. Schema showing the multiple obfuscation layers used by APT33

Actors often use commercial VPN services to hide their whereabouts when administering C&C servers and doing reconnaissance. Aside from VPN services that are available to anyone, we also see that actors use private VPNs they set up for themselves. Setting one up can be easily done by renting a couple of servers in data centers around the world and using open-source software like OpenVPN. Although the connections from private VPNs still come from seemingly unrelated IP addresses around the world, this kind of traffic is actually easier to track. Once we know that an exit node is mainly being used by a

particular actor, we can have a high degree of confidence about the attribution of the connections that are made from the IP addresses of the exit node. For example, besides administering C&C servers from a private VPN exit node, an actor might also be doing reconnaissance of targets' networks.

In regard to APT33, we were able to track private VPN exit nodes for more than a year. We could cross-relate the exit nodes with admin connections to servers controlled by APT33. It appears that these private VPN exit nodes are also used for reconnaissance of networks that are relevant to the supply chain of the oil industry. More concretely, we witnessed IP addresses that we believe are under the control of APT33 doing reconnaissance on the networks of an oil exploration company in the Middle East, an oil company in the U.S., and military hospitals in the Middle East.

APT33 used its private VPN to access websites of penetration testing companies, webmail services, websites on vulnerabilities, and websites related to cryptocurrencies, and to read hacker blogs and forums. The group also has a clear interest in websites that specialize in the recruitment of employees in the oil and gas industry.

Table 3 shows a list of IP addresses that have been used by APT33. The IP addresses are likely to have been used for a longer time than the time frames indicated in the table. The data can be used to determine whether an organization was on the radar of APT33 for, say, reconnaissance or concrete compromises.

IP address	Date first seen	Date last seen	IP address	Date first seen	Date last seen
5.135.120.57	Dec. 4, 2018	Jan. 24, 2019	137.74.80.220	Sept. 29, 2018	Oct. 23, 2018
5.135.199.25	March 3, 2019	March 3, 2019	137.74.157.84	Dec. 18, 2018	Oct. 21, 2019
31.7.62.48	Sept. 26, 2018	Sept. 29, 2018	185.122.56.232	Sept. 29, 2018	Nov. 4, 2018
51.77.11.46	July 1, 2019	July 2, 2019	185.125.204.57	Oct. 25, 2018	Jan. 14, 2019
54.36.73.108	July 22, 2019	Oct. 5, 2019	185.175.138.173	Jan. 19, 2019	Jan. 22, 2019
54.37.48.172	Oct. 22, 2019	Oct. 31, 2019	188.165.119.138	Oct. 8, 2018	Nov. 19, 2018
54.38.124.150	Oct. 28, 2018	Nov. 17, 2018	193.70.71.112	March 7, 2019	March 17, 2019
88.150.221.107	Sept. 26, 2019	Oct. 31, 2019	195.154.41.72	Jan. 13, 2019	Jan. 20, 2019
91.134.203.59	Sept. 26, 2018	Dec. 4, 2018	213.32.113.159	June 30, 2019	Sept. 16, 2019
109.169.89.103	Dec. 2, 2018	Dec. 14, 2018	216.244.93.137	Dec. 10, 2018	Dec. 21, 2018
109.200.24.114	Nov. 19, 2018	Dec. 25, 2018			

Table 3. IP addresses associated with a few private VPN exit nodes connected to APT33

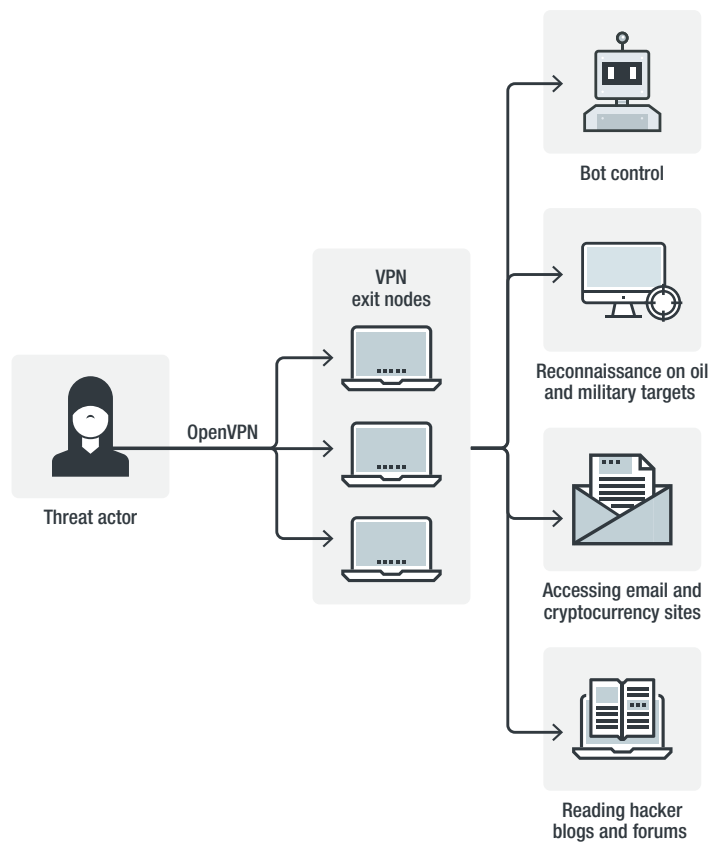


Figure 10. APT33's usage of a private VPN

For any company in the oil and gas industry, it might be a good idea to cross-relate these IP addresses with log files.

# Security Recommendations for the Oil and Gas Industry

In this section, we give general advice that can help companies in the oil and gas industry combat threat actors.

## **Perform data integrity checks.**

While there may not be an immediate need for encrypting all data communications in an oil and gas company, there is some merit in taking steps to ensure data integrity. For example, with regard to the information from the different sensors at oil production sites, the risk of tampering with oil production can be reduced by at least making sure that all data communication is signed. This can greatly decrease the risk of man-in-the-middle attacks where sensor values could be changed or where a third party could alter commands or inject commands without authorization.

## **Implement DNSSEC.**

We have noticed that many oil and gas companies don't have Domain Name System Security Extensions (DNSSEC) implemented. DNSSEC means digitally signing the DNS records of a domain name at the authoritative nameserver with a private key. DNS resolvers can check whether DNS records are properly signed. This checking can be done both on the corporate recursive DNS resolvers and at the clients. It is preferred to do DNSSEC validation at the clients as this ensures that DNSSEC checks are also done when employees use their corporate computing device while traveling or while working from home. DNSSEC helps to combat DNS spoofing and hijacking. As explained earlier in this paper, DNSSEC validation for all email clients in an organization can help raise the bar of an attack in case mail-related domains of the organization are DNS-hijacked.

## **Lock down domain names.**

Domain names can potentially be taken over by a malicious actor, for example, through an unauthorized change in the DNS settings. To prevent this, it is important to use only a DNS service provider that requires two-factor authentication for any changes in the DNS settings of the domains of an organization.

## **Monitor SSL certificates.**

For the protection of a brand name and for early warnings of possible upcoming attacks, it is important to monitor newly created SSL certificates that have certain keywords in the Common Name field. For example, a company can monitor for SSL certificates that have one of its brand names in the Common Name field. These SSL certificates could be used in credential-phishing attacks or malware attacks where the C&C server domain would not ring a bell immediately in log files.

## **Look out for business email compromise.**

Protection against business email compromise (BEC) is possible through spam filtering, user training for spotting suspicious emails, and AI techniques that will recognize writing styles of individuals in the company. Most individuals have a particular style of writing, and a writing DNA profile can be defined from a set of emails written by a specific person. Using the profiles of individuals in the company, an AI algorithm can potentially recognize BEC emails that attempt to mimic users (usually high-profile executives) within a company.

## **Require at least two-factor authentication for webmail.**

A webmail hostname might get DNS-hijacked or hacked because of a vulnerability in the webmail software. And webmail can also be attacked with credential-phishing attacks; a well-prepared credential-phishing attack can be quite convincing. The risk of using webmail can be greatly reduced by requiring two-factor authentication (preferably with a physical key) and corporate VPNs for webmail access.

## **Hold employee training sessions for security awareness.**

It is important to have regular training sessions for all employees. These sessions may include awareness training on credential phishing, spear phishing, social media use, data management, privacy policies, protecting intellectual property, and physical security.<sup>35</sup>

## **Monitor for data leaks.**

Any important document should be watermarked in a way that makes it discoverable on the internet. Watermarks make it easier to find leaked documents since the company can constantly monitor for these specific marks. There are also companies that specialize in finding leaked data and compromised credentials; through active monitoring for leaks, potential damage to the company can be mitigated earlier.

## **Keep VPN software up to date.**

Several weaknesses in VPN software were found in recent years.<sup>36,37</sup> For various reasons, some companies do not update their VPN software immediately after patches become available. This is particularly dangerous since APT actors start to probe for vulnerable VPN servers (including those of oil companies) as soon as a vulnerability becomes public.

## **Review the security settings of cloud services.**

For companies that use cloud services, a review of all security settings and proper risk assessment are necessary. Cloud services can boost efficiency and reduce cost, but companies sometimes forget to effectively use all security measures offered by the cloud services. There are also services that help companies with cloud infrastructure security.<sup>38</sup>

# References

- 1 Stephen Kalin, Rania El Gamal, and Dmitry Zhdannikov. (14 September 2019). *Reuters*. "Attacks on Saudi oil facilities knock out half the kingdom's supply." Last accessed on 22 November 2019 at <https://www.reuters.com/article/us-saudi-aramco-fire/attacks-on-saudi-oil-facilities-knock-out-half-the-kingdoms-supply-idUSKCN1VZ01N>.
- 2 Jim Finkle, Tom Finn, and Jeremy Wagstaff. (1 December 2019). *Reuters*. "Shamoon virus returns in Saudi computer attacks after four-year hiatus." Last accessed on 22 November 2019 at <https://www.reuters.com/article/us-cyber-saudi-shamoon-targets/shamoon-virus-returns-in-saudi-computer-attacks-after-four-year-hiatus-idUSKBN13Q4AX>.
- 3 Idrees Ali and Phil Stewart. (16 October 2019). *Reuters*. "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials." Last accessed on 4 December 2019 at <https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-us-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-say-idUSKBN1WV0EK>.
- 4 Stephen Jewkes and Jim Finkle. (13 December 2019). *Reuters*. "Saipem says Shamoon variant crippled hundreds of computers." Last accessed on 22 November 2019 at <https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA>.
- 5 David McPhee. (19 December 2018). *Energy Voice*. "Petrofac reassures operators after IT breach." Last accessed on 22 November 2019 at <https://www.energyvoice.com/oilandgas/188750/petrofac-confirms-system-security-breach/>.
- 6 Feike Hacquabord. (25 April 2017). *Trend Micro Security News*. "Two Years of Pawn Storm: Examining an Increasingly Relevant Threat." Last accessed on 22 November 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm>.
- 7 National Cybersecurity and Communications Integration Center. (18 December 2017). *U.S. Department of Homeland Security CISA Cyber + Infrastructure*. "MAR-17-352-01 HatMan—Safety System Targeted Malware." Last accessed on 22 November 2019 at <https://www.us-cert.gov/ics/MAR-17-352-01-HatMan%E2%80%94Safety-System-Targeted-Malware>.
- 8 National Cybersecurity and Communications Integration Center. (17 February 2019). *U.S. Department of Homeland Security CISA Cyber + Infrastructure*. "MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B)." Last accessed on 22 November 2019 at <https://www.us-cert.gov/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B>.
- 9 Trend Micro. (1 October 2010). *Trend Micro Threat Encyclopedia*. "STUXNET Malware Targets SCADA Systems." Last accessed on 22 November 2019 at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems>.
- 10 Science X. (9 November 2019). *Phys Org*. "Chevron says hit by Stuxnet virus in 2010." Last accessed on 22 November 2019 at <https://phys.org/news/2012-11-chevron-stuxnet-virus.html>.
- 11 Trend Micro. (23 June 2017). *Trend Micro Threat Encyclopedia*. "TROJ\_INDUSTROYER.B." Last accessed on 22 November 2019 at [https://www.trendmicro.com/vinfo/ph/threat-encyclopedia/malware/troj\\_industroyer.b](https://www.trendmicro.com/vinfo/ph/threat-encyclopedia/malware/troj_industroyer.b).
- 12 Kyle Wilhoit. (11 February 2016). *Trend Micro Security Intelligence Blog*. "KillDisk and BlackEnergy Are Not Just Energy Sector Threats." Last accessed on 22 November 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/>.
- 13 Trend Micro. (22 December 2017). *Trend Micro Security News*. "TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems." Last accessed on 22 November 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/>.
- 14 Trend Micro. (12 December 2018). *Trend Micro Security News*. "New Version of Disk-Wiping Shamoon/Distrack Spotted: What You Need to Know." Last accessed on 22 November 2019 at <https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/new-version-of-disk-wiping-shamoon-distrack-spotted-what-you-need-to-know>.
- 15 Bill Woodcock. (28 March 2019). *A Conference for Defense - ACoD*. "Ops Track 01/30/19 - Briefing on Dec 18 - Jan 19 DNS/IMAP Prepositioning Attacks - Bill Woodcock." Last accessed on 22 November 2019 at <https://www.youtube.com/watch?v=oNF6TE75mzg&t=1136s>.
- 16 Brian Krebs. (18 February 2019). *Krebs on Security*. "A Deep Dive on the Recent Widespread DNS Hijacking Attacks." Last accessed on 4 December 2019 at <https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/>.

- 17 Jake Creps. (8 May 2019). *Jake Creps*. "OSINT Collection Tools for Pastebin." Last accessed on 22 November 2019 at <https://jakecreps.com/2019/05/08/osint-collection-tools-for-pastebin/>.
- 18 Trend Micro. (n.d.). *Trend Micro Security News*. "Cybercriminal Underground Economy Series." Last accessed on 25 November 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series>.
- 19 Gilbert Sison and Ryan Maglaque. (15 April 2019). *Trend Micro Security Intelligence Blog*. "Account With Admin Privileges Abused to Install BitPaymer Ransomware via PsExec." Last accessed on 25 November 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec/>.
- 20 Trend Micro. (16 May 2018). *Trend Micro Security News*. "The Rise and Fall of {Scan4You}." Last accessed on 25 November 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-rise-and-fall-of-scan4you>.
- 21 Trend Micro Forward-Looking Threat Research Team. (23 November 2015). *Trend Micro Security Intelligence Blog*. "Trend Micro, NCA Partnership Leads to Arrests and Shutdown of Refud.me and Cryptex Reborn." Last accessed on 25 November 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-nca-partnership-lead-to-arrests-and-shutdown-of-refud-me-and-cryptex-reborn/>.
- 22 Trend Micro. (24 September 2019). *Trend Micro Threat Encyclopedia*. "BKDR64\_RGDOOR.ZIFB-A." Last accessed on 25 November 2019 at [https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr64\\_rgdoor.zifb-a](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr64_rgdoor.zifb-a).
- 23 Robert Falcone. (25 January 2019). *Unit 42*. "OilRig uses RGDoor IIS Backdoor on Targets in the Middle East." Last accessed on 25 November 2019 at <https://unit42.paloaltonetworks.com/unit42-OilRig-uses-rgdoor-iis-backdoor-targets-middle-east/>.
- 24 Robert Falcone. (8 November 2017). *Unit 42*. "OilRig Deploys "ALMA Communicator" – DNS Tunneling Trojan." Last accessed on 25 November 2019 at <https://unit42.paloaltonetworks.com/unit42-OilRig-deploys-alma-communicator-dns-tunneling-trojan/>.
- 25 Dennis Schwarz. (1 May 2017). *Netscout*. "Greenbug's DNS-isms." Last accessed 25 November 2019 at <https://www.netscout.com/blog/asert/greenbugs-dns-isms>.
- 26 Trend Micro. (8 October 2013). *Trend Micro Threat Encyclopedia*. "BKDR\_KIMSUK.A." Last accessed on 25 November 2019 at [https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr\\_kimsuk.a](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr_kimsuk.a).
- 27 Bernadette Irinco. (18 February 2015). *Trend Micro Threat Encyclopedia*. "Equation Group Takes Precise Calculations." Last accessed on 25 November 2019 at <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3153/equation-group-takes-precise-calculations>.
- 28 Ruchna Nigam. (5 April 2018). *Unit 42*. "Reaper Group's Updated Mobile Arsenal." Last accessed on 25 November 2019 at <https://unit42.paloaltonetworks.com/unit42-reaper-groups-updated-mobile-arsenal/>.
- 29 Daniel Lunghi and Jaromir Horejsi. (10 June 2019). *Trend Micro Security Intelligence Blog*. "MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools." Last accessed on 25 November 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/>.
- 30 GReAT. (13 May 2019). *SecureList*. "ScarCruft continues to evolve, introduces Bluetooth harvester." Last accessed on 25 November 2019 at <https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/>.
- 31 Cedric Pernet, Daniel Lunghi, Jaromir Horejsi, and Joseph C. Chen. (7 March 2019). *Trend Micro Security Intelligence Blog*. "New SLUB Backdoor Uses GitHub, Communicates via Slack." Last accessed on 25 November 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/>.
- 32 Daniel Lunghi and Jaromir Horejsi. (10 June 2019). *Trend Micro Security Intelligence Blog*. "MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools." Last accessed on 25 November 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/>.
- 33 Doug Olenick. (11 June 2019). *SCMagazine UK*. "MuddyWater, Fin8 and Platinum threat actors back in action." Last accessed on 12 December 2019 at <https://www.scmagazineuk.com/muddywater-fin8-platinum-threat-actors-back-action/article/1587131>.
- 34 Feike Hacquebord, Cedric Pernet, and Kenney Lu. (13 November 2019). *Trend Micro Security Intelligence Blog*. "More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting." Last accessed on 4 December 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/>.

- 35 Trend Micro. (14 November 2018). *Trend Micro Simply Security*. "The Importance of Employee Cybersecurity Training: Top Strategies and Best Practices." Last accessed on 25 November 2019 at <https://blog.trendmicro.com/the-importance-of-employee-cybersecurity-training-top-strategies-and-best-practices/>.
- 36 Fortinet. (28 August 2019). *Fortinet*. "FortiOS and SSL Vulnerabilities." Last accessed on 25 November 2019 at <https://www.fortinet.com/blog/business-and-technology/fortios-ssl-vulnerability.html>.
- 37 PulseSecure. (n.d.) *PulseSecure*. "SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX." Last accessed on 25 November 2019 at [https://kb.pulsesecure.net/articles/Pulse\\_Security\\_Advisories/SA44101/](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/).
- 38 Trend Micro. (n.d.) *Trend Micro*. "Cloud Conformity Security." Last accessed on 4 December 2019 at [https://www.trendmicro.com/en\\_us/business/products/hybrid-cloud/cloud-one-conformity.html](https://www.trendmicro.com/en_us/business/products/hybrid-cloud/cloud-one-conformity.html).



## **TREND MICRO™ RESEARCH**

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)

