Journal of Mines, Metals and Fuels, 71(3): 300-303; 2023. DOI: 10.18311/jmmf/2023/33705

Print ISSN : 0022-2755

Journal of Mines, Metals and Fuels

Contents available at: www.informaticsjournals.com/index.php/jmmf

Jayanta Bhattacharya
Hony. Chief Editor

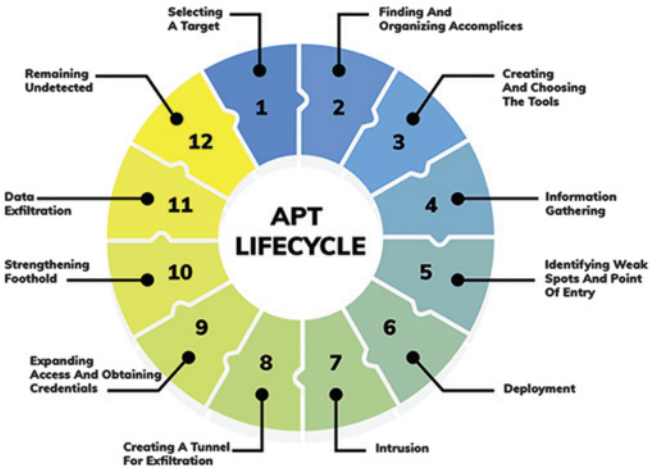
Security™

How to Prepare for Information Security Threats for Systems Connected with Internet in MOGI Companies

Part-II discusses connected threats in the MOGI companies

Advanced persistent threat attacks

An advanced persistent threat (APT) is a targeted cyberattack in which an unauthorized intruder penetrates a network and remains undetected for an extended period of time. Rather than causing damage to a system or network, the goal of an APT attack is to monitor network activity and steal information to gain access, including exploit kits and malware.



Cybercriminals typically use APT attacks to target high-value targets, such as large enterprises and nation-states, stealing data over a long period.

Preventing APT attacks

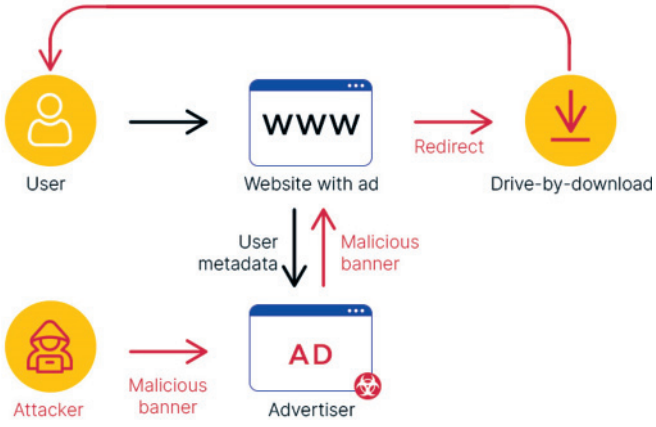
Detecting anomalies in outbound data may be the best way for system administrators to determine if their networks have been targeted.

1. Indicators of APTs include the following:
2. unusual activity on user accounts;
3. extensive use of backdoor Trojan horse malware, a method that enables APTs to maintain access;
4. odd database activity, such as a sudden increase in database operations involving massive amounts of data; and
5. the presence of unusual data files, possibly indicating that data that has been bundled into files to assist in the exfiltration process.

To combat this type of information security threat, an organization should also deploy a software, hardware or cloud firewall to guard against APT attacks. Organizations can also use a web application firewall to detect and prevent attacks coming from web applications by inspecting HTTP traffic.

Malvertising

Malvertising is a technique cybercriminals use to inject malicious code into legitimate online advertising networks and web pages. This code typically redirects users to malicious websites or installs malware on their computers or mobile devices. Users' machines may get infected even if they don't click on anything to start the download. Cybercriminals may use malvertising to deploy a variety of moneymaking malware, including cryptomining scripts, ransomware and banking Trojans. Some of the websites of well-known companies, including Spotify. The New York Times and the London Stock Exchange, have inadvertently displayed malicious ads, putting users at risk.



Preventing Malvertising

To prevent malvertising, ad networks should add validation; this reduces the chances a user could be compromised. Validation could include: Vetting prospective customers by requiring legal business paperwork; two-factor authentication; scanning potential ads for malicious content before publishing an ad; or possibly converting Flash ads to animated gifts or other types of content.

To mitigate malvertising attacks, web hosts should periodically check their websites from an unpatched system and monitor that system to detect any malicious activity. The web hosts should disable any malicious ads.

To reduce the risk of malvertising attacks, enterprise security teams should be sure to keep software and patches up to date as well as install network antimalware tools.

Case Studies in MOGI Companies

As the mining industry continues to embrace emerging technologies, from autonomous vehicles to artificial intelligence, the sector opens itself up to new potential risks alongside the potential improvements in productivity and profitability. One of the most prominent risks is cybersecurity in mining.

The Weir Attack

The latest example is a cyberattack that hit industrial supplier Weir in October, and was described by its chief executive Jon Stanton as "a sophisticated external attack". While the company's own defences were able to shut down the attack before more significant damage was done, the attack is a sobering reminder of the potential for cyberattacks to damage mining operations, with Weir expecting its Q4 revenue to fall by $13.6m-$27m in the wake of the incident.

While details on the Weir attack remain sparse, its impacts are significant. The company experienced ongoing disruptions to its core IT systems, its engineering systems, and its resource planning processes, dealing a significant blow to Weir's administrative capabilities. This is a particular threat in the mining industry, which operates across borders and continents.

"We responded quickly and comprehensively to what was a sophisticated external attack on our business," said Stanton in a press release following the incident, highlighting the fact that many of the systems were shut down and control regained before lasting damage could be done.

"The robust action to protect our infrastructure and data has led to significant temporary disruption but our teams have responded magnificently to this challenge and have managed to minimise the impact on our customers.

Collateral Damages

Victoria Gold (TSXV: GCX) warned investors in its annual report last month that the military invasion of Ukraine could lead to "heightened cybersecurity disruptions and threats" in 2022, even though the company doesn't have any operations in Russia or Ukraine. In the same month, Endeavour Mining (TSX: EDV; LSE: EDV) listed cyber security as one of its principal risks and said that companies were becoming "more vulnerable to cyber threats" due to the increasing reliance on digital technology.

"Although Endeavour invests heavily to monitor, maintain, and regularly upgrade its systems, there remains a risk that we may be unable to prevent, detect, and respond to cyber-attacks in a timely manner," it said in its annual report. According to Ernst & Young's Global Information Security Survey published in mid-2021, about 55% of mining executives are worried about their ability to manage a cyber threat with nearly 70% witnessing an increase in the number of disruptive attacks in the previous 12 months. Almost half of the respondents said that the industrial control systems were most frequently attacked.

Analysts say that the impacts of these attacks can range

from company stocks being shorted or the lives of workers being put in danger when crucial operating systems are hacked to something as simple as assay results getting delayed.

In another instance, in the last five months British Columbia-based PJX Resources (TSXV: PJX) and Getchell Gold (US-OTC: GGLDF) in Nevada reported delays in receiving their assays as the Bureau Veritas Laboratory in Nevada was recovering from a cyber-attack that hit the company in November last year.

Nadine Miller, an engineer who has worked in mining for over two decades and is currently vice-president of project development at JDS Energy & Mining, notes that the industry has a tradition of being late adaptors to new technologies and is now also lagging behind in cyber security.

"We are always in a race to be the first ones to be last in new technologies," Miller told The Northern Miner, adding that mining companies generally do not want to be early adaptors of any technology. "There are a few that will do it," she said, adding they are usually larger companies.

Miller says that while the mining industry has done a good job in securing its information technology (IT) systems, which include network infrastructures, file shares or employee laptops and computers, the operational technology (OT) – which, for example, involves systems responsible for process plants, refineries, heating or ventilation in underground mines – are not secure.

Bryan Tan, an Associate partner at EY's cyber security practice says that ransomware, a type of malicious software designed to block access to a computer system until a sum of money is paid, is one of the "key threats" in the industry right now.

"A lot of organizations... put the OT systems on the same network as the IT systems," he told The Northern Miner. "That starts to spread on the environment in the IT side, but because it can touch the OT systems, it can potentially impact those as well. From more of a business impact, your OT comes to a standstill and that may lead to life-threatening issues as well," he explained.

Oil and Gas Cybersecurity

The oil and gas industry is no stranger to major cybersecurity attacks, attempting to disrupt operations and services. Most of the best understood attacks against the oil industry are initial attempts to break into the corporate networks of oil companies. A survey also found that oil and gas companies have experienced disruptions with their supply due to cyberattacks. On average, the disruption lasted six days. The financial damage amounts to approximately $3.3 million. Due to long disruption, the oil and gas industry has a much larger damage, too.

It is important to have an in-depth analysis at cyberattacks than can disrupt oil and gas companies because they affect operations and profit in a major way. By looking closer at the infrastructure of an oil and gas company and identifying threats that can disrupt operation, a company can seal off loopholes and improve their cybersecurity framework.

An expert team at Trend Micro identified the following threats that can compromise oil and gas companies:

1. **Sabotage**
   In the context of the oil and gas industry, sabotage can be done by changing the behaviour of software, deleting or wiping specific content to disrupt company activity or deleting or wiping 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. Stuxnet was a piece of self-replicating malware that contained a very targeted and specific payload. Most infections of the worm were 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.
2. **Insider threat**
   In most cases, an insider is a disgruntled employee seeking revenge or wanting to make easy money by selling valuable data to competitors. This person can sabotage operations. They can alter data to create problems, delete or destroy data from corporate servers or shared project folders, steal intellectual property, and leak sensitive documents to third parties.
   Defense against insider threats is very complex since insiders generally have access to a lot of data. An insider also does not need months to know the internal network of the company — the insider probably already knows the inner workings of the organization.
3. **Espionage and data theft**
   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.
4. **DNS hijacking**
   DNS hijacking is a form of data theft used by advanced attackers. The objective is to gain access to the corporate VPN network or corporate emails of governments and companies. We have seen several 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 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.

5. **Attacks on Webmail and Corporate VPN Servers**

While webmail and file-sharing services have become a vital tool for accessing emails and important documents on the go, these services can increase the possibility of a cyberattack on the surface. For instance, a webmail hostname might get DNS-hijacked or hacked because of the 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 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.

6. **Data leaks**

Data leaks have always been problematic. But the oil and gas industry is more susceptible to these threats because leaked information can be quite beneficial to a competitor. Data leaks can also cause substantial damage to a company's reputation.

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.

7. **External emails**

In general, emails are well-protected inside companies. However, external emails cannot be controlled the same way. Employees regularly send emails to external addresses, hence some sensitive internal content ends up outside the company's purview. Even worse, sensitive information can be copied to unsecured 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.