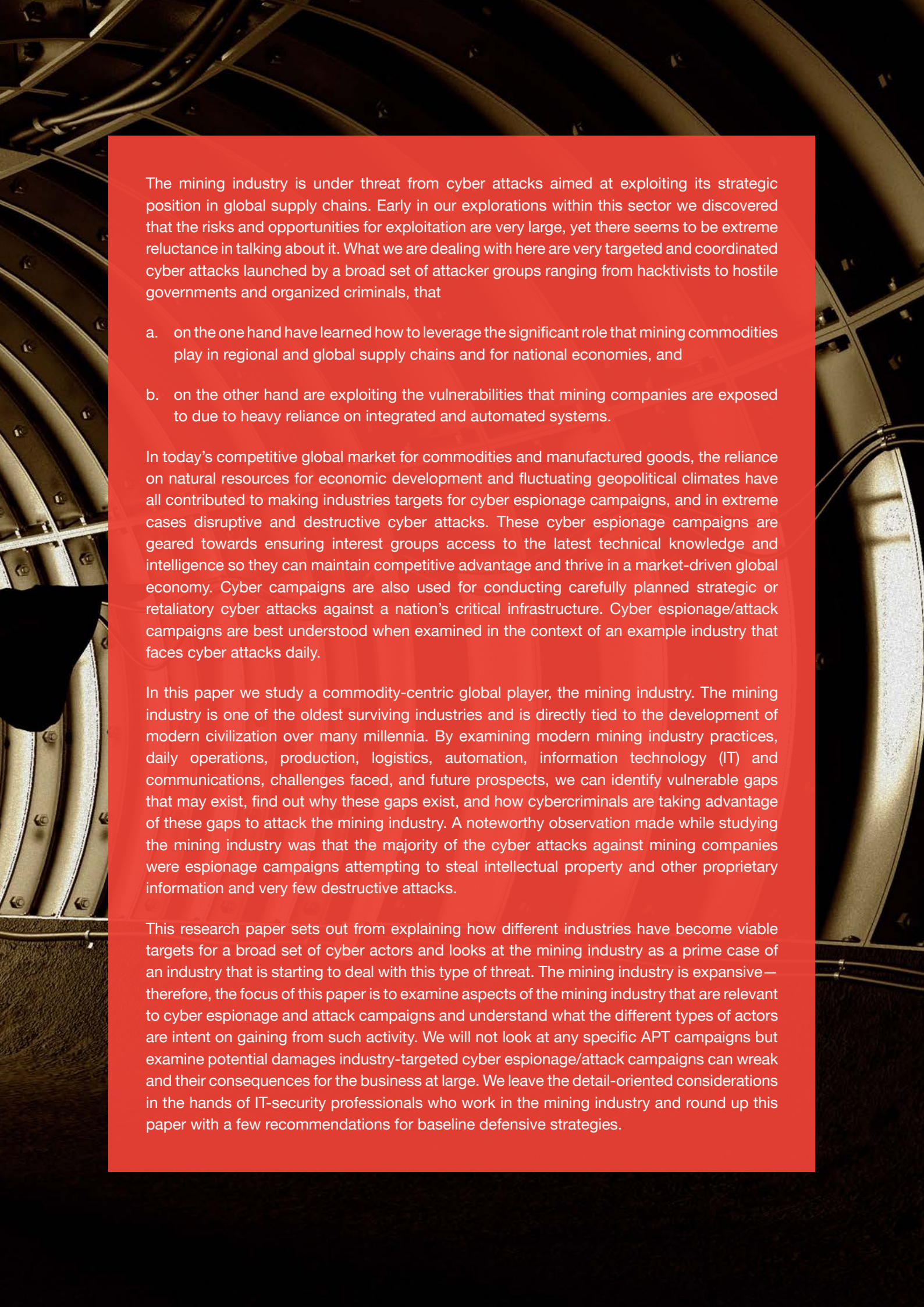
Cyber Threats to the Mining Industry

Numaan Huq

Trend Micro Forward-Looking Threat Research (FTR) Team

A **TrendLabs**SM Research Paper

Contents



The mining industry is under threat from cyber attacks aimed at exploiting its strategic position in global supply chains. Early in our explorations within this sector we discovered that the risks and opportunities for exploitation are very large, yet there seems to be extreme reluctance in talking about it. What we are dealing with here are very targeted and coordinated cyber attacks launched by a broad set of attacker groups ranging from hacktivists to hostile governments and organized criminals, that

a. on the one hand have learned how to leverage the significant role that mining commodities play in regional and global supply chains and for national economies, and

b. on the other hand are exploiting the vulnerabilities that mining companies are exposed to due to heavy reliance on integrated and automated systems.

In today's competitive global market for commodities and manufactured goods, the reliance on natural resources for economic development and fluctuating geopolitical climates have all contributed to making industries targets for cyber espionage campaigns, and in extreme cases disruptive and destructive cyber attacks. These cyber espionage campaigns are geared towards ensuring interest groups access to the latest technical knowledge and intelligence so they can maintain competitive advantage and thrive in a market-driven global economy. Cyber campaigns are also used for conducting carefully planned strategic or retaliatory cyber attacks against a nation's critical infrastructure. Cyber espionage/attack campaigns are best understood when examined in the context of an example industry that faces cyber attacks daily.

In this paper we study a commodity-centric global player, the mining industry. The mining industry is one of the oldest surviving industries and is directly tied to the development of modern civilization over many millennia. By examining modern mining industry practices, daily operations, production, logistics, automation, information technology (IT) and communications, challenges faced, and future prospects, we can identify vulnerable gaps that may exist, find out why these gaps exist, and how cybercriminals are taking advantage of these gaps to attack the mining industry. A noteworthy observation made while studying the mining industry was that the majority of the cyber attacks against mining companies were espionage campaigns attempting to steal intellectual property and other proprietary information and very few destructive attacks.

This research paper sets out from explaining how different industries have become viable targets for a broad set of cyber actors and looks at the mining industry as a prime case of an industry that is starting to deal with this type of threat. The mining industry is expansive—therefore, the focus of this paper is to examine aspects of the mining industry that are relevant to cyber espionage and attack campaigns and understand what the different types of actors are intent on gaining from such activity. We will not look at any specific APT campaigns but examine potential damages industry-targeted cyber espionage/attack campaigns can wreak and their consequences for the business at large. We leave the detail-oriented considerations in the hands of IT-security professionals who work in the mining industry and round up this paper with a few recommendations for baseline defensive strategies.

Industrial Controls under Attack

Cyber Attacks Targeting Different Industries

News about cyber attacks targeting different industries is becoming more and more commonplace much like daily news stories about data breaches. Advanced persistent threat (APT) campaigns such as BlackEnergy—originally pure industrial espionage campaigns—have been re-purposed to cause physical impact by attacking and damaging industrial assets. BlackEnergy and another APT campaign, Sandworm, were discovered as the likely perpetrators behind outages at two power generation facilities in Ukraine in December 2015.[1] BlackEnergy and KillDisk were discovered in attempted similar cyber attacks against a mining company and a large railway operator also in Ukraine.[2] This shows that BlackEnergy has evolved from being just an energy sector problem to a threat applicable to organizations in all sectors.

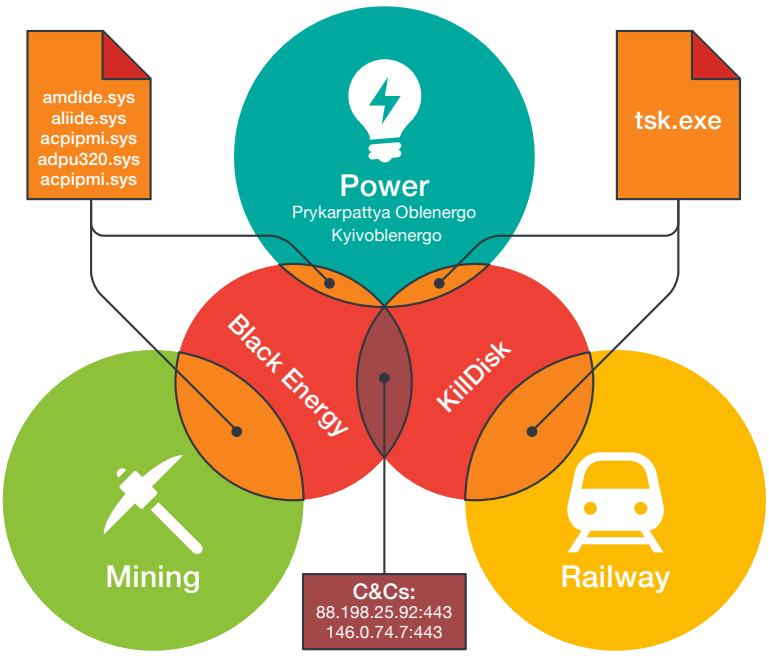


Figure 1: Overlap between sectors, campaigns, malware, and C&C servers[3]

Victims of cyber attacks tend to not publicly disclose that they were attacked. In part this is because there is no legal requirement for disclosure, but also due to other dissuasive factors such as negative effect on company stock prices or company reputation, decline in short-term sales, etc. The BlackEnergy case shows that APTs are now not only penetrating deeper inside organizations but can actually be weaponized to cause asset damage. At risk is the entire supply chain of the targeted organization: raw materials, manufacturing and production, logistics, inventory, distribution, etc. A cyber attack against any part of the supply chain is easily able to cause substantial asset, capacity, and monetary damage to the organization. The new reality of weaponized APTs is something that can no longer be ignored.

Looking back at past campaigns we can trace a broad spectrum of different actors from hacktivists, to nation-state actors, business competitors and criminal syndicates that all have varying and sometimes overlapping interests. These campaigns have targeted a variety of industries as well, ranging from data and intelligence theft (Red October), deletion of data on hard drives in energy facilities (Shamoon), to disruption of nuclear facilities (Stuxnet) and most recently, disruptive attacks against power generation facilities (BlackEnergy).

Why Are Industries Vulnerable?

Cyber attacks are not an exclusive IT problem—they have a deep impact on daily business operations such as: operational shutdowns, equipment damage, reputation damage, financial loss, intellectual property loss, competitive advantage loss, health and safety risks, etc. The classic modus operandi and primary goal for cybercriminals has been the theft of money, financial information, and PII in the past—and not surprisingly this first affected the financial sector. Today's cybercriminals, however, are evolving not only in terms of their technical ability and sophistication but are increasingly understanding the value of stolen sensitive data from all kinds of sectors in monetizing it and influencing business dynamics.

As an example, one group stole market-sensitive information from 100+ companies, while another group stole pre-release information from financial newswires. In both cases the stolen information was traded for profits in the stock market.[4] Another recent trend is the rise of extortive cyber attacks against organizations using ransomware and DDoS (distributed denial of service) attacks against IT infrastructure. The Deep Web marketplace and underground forums together form a massive virtual organized crime group. They allow criminals with limited technical knowledge to purchase malware, bulletproof hosting services, technical support, expertise, money laundering services, etc.[5] Cybercrime has moved from being a niche business to mainstream activity and has greatly increased the threat against organizations.[6]

One of the central weaknesses found throughout different industries is the way operations are set up and increasing levels of centralization. “Operational Technology (OT) is hardware and software that detects or causes a change through direct monitoring and/or control of physical devices, processes, and events in the enterprise.”[7] To be competitive in the market-driven global economy, organizations need a better overview of the supply chain. “This need for a better view of the supply chain is reflected in the shift towards greater integration, visibility, and intelligence within and amongst the OT production control systems and IT that companies use to manage their critical assets, logistics, planning, and operations.”[8]

The convergence of OT and IT is exactly what allows greater access to two components that are prime targets for cybercriminals. In many organizations OT infrastructure is at best poorly protected against cyber attacks. They are secured with IT solutions that are ill-adapted to legacy control systems such as Supervisory Control and Data Acquisition (SCADA). In addition to that, new and emerging technologies such as cloud computing, big data analytics, and Internet of Things (IoT) have made security challenges faced by today’s organizations more complex, and more critical. Simply put, centralization introduces new and unknown vulnerabilities into the cyber ecosystem. But ultimately the centralization of business functions across the supply chain is driven by cost rationalizations that seem to outweigh the risks. This thought process will have to change in light of cyber risks.

Industrial Control and Automation Systems and Their Pitfalls

To compete in today’s market-driven global economy, businesses need to have efficient production processes to reduce costs, increase output, and improve quality. The solution is automation. Automation improves workplace safety, reduces operational costs, brings production consistency, increases production capacity, increases the level of control at each stage of production, limits operational variance, improves precision, allows for accurate process modeling, etc. For these reasons automation of industrial systems has been steadily gaining momentum, helping businesses become competitive global players.

Most Industrial Control Systems (ICS) in use today were developed decades ago. With new requirements for corporate connectivity and remote access, ICS has been adopting IT solutions for ease of integration and reduced development costs. The operational priorities for ICS are: **i**ntegrity (ensuring that correct commands are issued), **a**vailability (limiting interruptions), and **c**onfidentiality (protecting the data). The operational priorities for IT systems are: **c**onfidentiality (protecting the data), **i**ntegrity (ensuring that correct commands are issued), and **a**vailability (limiting interruptions). IT administrators need to manage two different systems, ICS and IT, with conflicting operational priorities, I-A-C vs C-I-A. ICS was originally designed with performance, reliability, safety, and flexibility in mind and to operate in isolated environments.

With ICS incorporating everyday IT solutions, network connectivity, and different operational priorities, it has introduced a whole new set of exploitable vulnerabilities. In FY2015, ICS-CERT responded to 295 cyber incidents, a 20 percent increase over FY2014.[9] Attacks against the Critical Manufacturing Sector nearly doubled to a record 97 incidents, the Energy Sector was the second most targeted with 46 incidents, and the Water and Wastewater Systems Sector was third with 25 incidents.

Malware and targeted cyber attacks are not the only causes of ICS disruptions; operator error, system failures, and software bugs also contribute to ICS disruptions. The Stuxnet worm attacked and damaged ICS in five industrial facilities in Iran that were suspected of enriching uranium.[10] The attacks were speculated to have originated from nation states that wanted to deter Iran's nuclear ambitions. While this was not the first cyber attack against ICS, it was the first to infect a Programmable Logic Controller.[11] The attack against Iran's secretive nuclear program made Stuxnet a widely reported news story. The Stuxnet incident brought ICS security considerations to the forefront and demonstrated just how vulnerable industries are in the face of targeted attacks against their ICS environments.

The Mining Industry

Introduction to the Mining Industry

The mining of metals was a key driver in the advancement of civilization and is used as a yardstick measure of progress. The world is rapidly becoming urbanized with more people relocating to cities. This urban migration has increased the demand for basic infrastructure such as roads, houses, schools, etc. Furthermore, wealth generation in urban centers has increased the demand for everyday essentials such as consumer appliances, cars, computers, etc. With urbanization comes a greater demand for metals and minerals, particularly base metals like iron, copper, and aluminum. Modern society's existence depends on the products of mines.

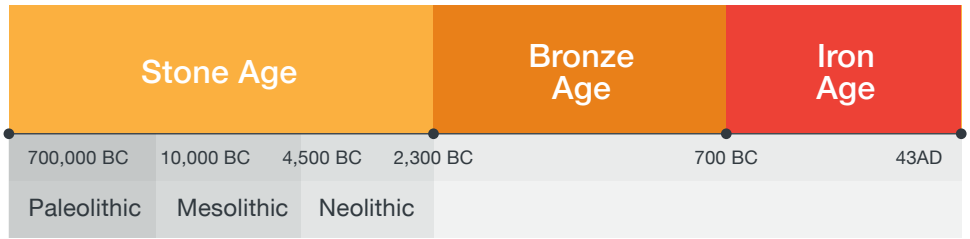


Figure 2: The three-age system periodization of human prehistory and history[12,13]

In the United States, mining is considered an essential or primary industry but not a critical infrastructure sector. The critical infrastructure sectors are those whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[14] Primary metal manufacturing such as iron and steel mills, ferroalloy, alumina (aluminum oxide) and aluminum, and non-ferrous metals are part of critical infrastructure—the mining industry supplies them with processed metal concentrates. The question of whether the mining industry is a critical infrastructure or not is debatable in the energy sector. In countries like Canada and Venezuela, oil sands are surface-mined, processed, and converted into petroleum products. Mines producing oil sands are thus part of the critical infrastructure of those countries.

Modern Mining Operations

Mining operations comprise two major activities:

1. Mining (ore extraction)
2. Mineral Processing (upgrading and recovering metals and/or minerals from ores)

Modern mining companies do more than dig a hole in the ground to excavate rocks and process them to extract metals and minerals. The modern mining company is a transnational corporation running highly coordinated production operations across multiple sites, in multiple countries with varied geopolitical climates, all the while responding to the supply and demand needs of a market-driven global economy. The following diagram provides a high-level overview of the modern mining company:

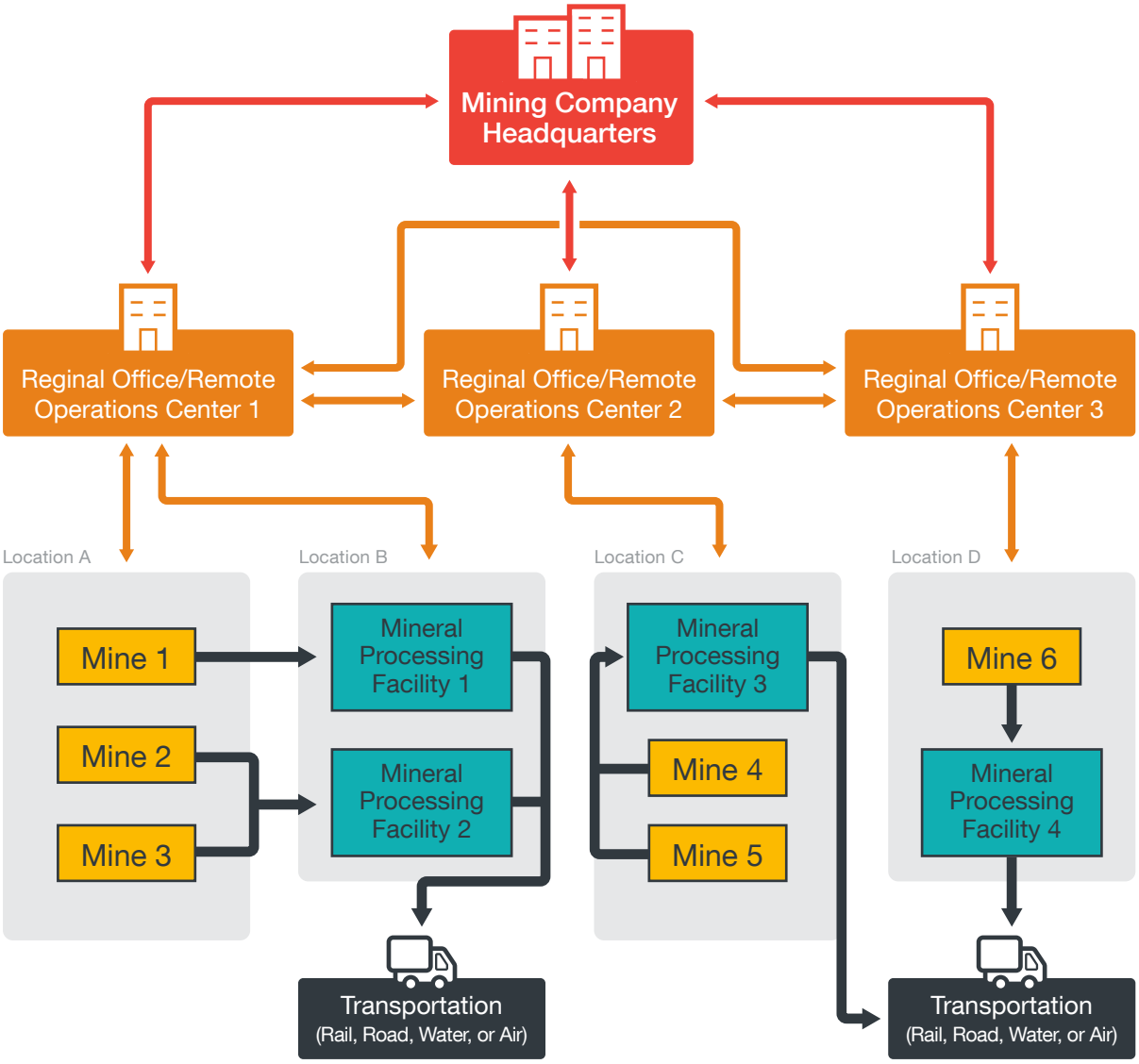


Figure 3: Operations of a modern mining company

In this constructed example the mining company operates six mines, of varying sizes and production capacities, in three international locations (A, C, and D). Mines 1, 2, and 3 produce iron ore, Mines 4 and 5 produce copper, and Mine 6 produces gold. The mining company also operates four mineral processing facilities in three locations. The mineral processing facilities don't need to be located at the mining sites and are typically built in central locations that can aggregate feeds from multiple mines. Two of the mineral processing facilities (3 and 4) are located in the same vicinity as the mines they serve, while the remaining two (1 and 2) are located some distance away from the mines.

The mines crush the excavated ore rocks and rail transports them to the mineral processing facilities. Processed metal or mineral concentrates are transported from the processing facilities to the customers via rail, road, water, or air depending on the type, demand, and volume of the final product (e.g., uncut gem-quality diamonds are transported by air to diamond-cutting facilities). A regional office, located in a nearby urban center, oversees the operations of each location. Regional offices also house the Remote Operations Center (ROC) to manage equipment at the sites. Regional offices communicate with the corporate headquarter and with each other to coordinate production and other functions.

Developing a Mine

Selecting and developing a mining site is a long and expensive process that involves exploration, discovery, feasibility studies, and construction. The following value chain diagram shows all the stages of project development starting from conception to the end-of-life of a mine:

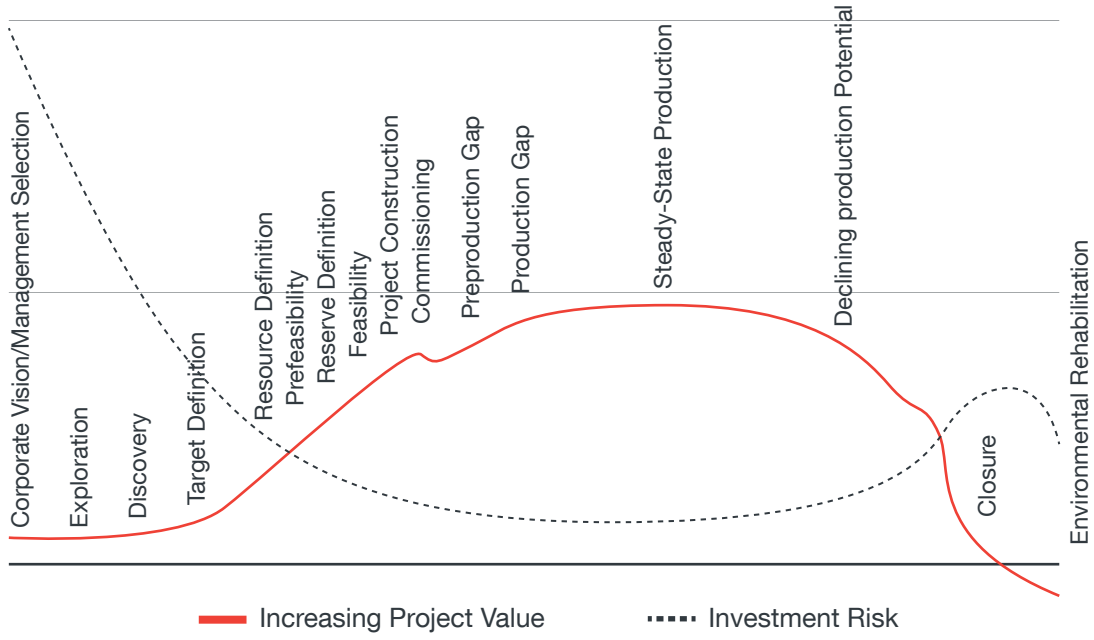


Figure 4: Stages of mine development[15]

Mining companies invest billions of dollars every year exploring potential new mining sites in the hopes of "hitting pay dirt" (i.e., discover an ore-rich area that can be successfully mined). Technological improvements have made exploration more accurate and include geophysical exploration methods such as: gravimetric, magnetic, electrical (electrical resistivity, induced polarization, self potential), electromagnetic (coil sensors, superconductive quantum interference device sensors), radioactive, seismic, and remote sensing techniques. The exploration phase generates big data sets that geologists analyze to identify new ore deposit locations. The exploration data is very expensive to generate and is key to the company's future growth and success, which makes this data a lucrative target for cyber espionage campaigns.

The mining industry is moving towards low-grade, super-large, high-tonnage, and ultra-mechanized operations. This is partly because high-grade/high-quality ore sites are being depleted or are cost prohibitive to mine. Advancements in technology and the production process have improved yields from lower-grade ores, which ultimately makes mines profitable over their lifetimes. This has turned smaller mining operations economically unfeasible leading to closures, mergers, and takeovers. The fundamental source of a mine's value is its potential ore reserve. Ore reserve and production data are targets in cyber espionage campaigns especially when a merger or takeover bid is in the works—the goal is to deflate the mine's value if possible, or to collect insider information and mount a successful bid.

From the start of exploration until the new mine becomes operational roughly takes 10 years. On average, it takes another 10 years of production before the initial investment is recovered, after which the mine starts generating profit. The high capital cost and long lifetime of a mining operation leads to lower rates of technological changes. This means mining operations are using equipment and communications protocols that are vulnerable to crippling cyber attacks because standards and equipment upgrades are deemed unnecessary for continued production. A mining company in British Columbia, Canada privately told us that downtime in their mines costs them north of $6,000 per minute and the general managers in charge of operating the mines will not allow any downtime that will affect production.

Everyday Mining Operations

The modern-day mine is a hive of activity; the basic operations of a mine can be summarized as:

1. Drilling blast holes in the rock
2. Controlled detonation of the rock
3. Excavating and loading the blasted rock
4. Hauling the excavated rock to the rock crushing facility
5. Crushing and transporting the ore rock to a mineral processing facility

The following diagram gives an operational overview of an open pit mine; underground mines have similar operations:

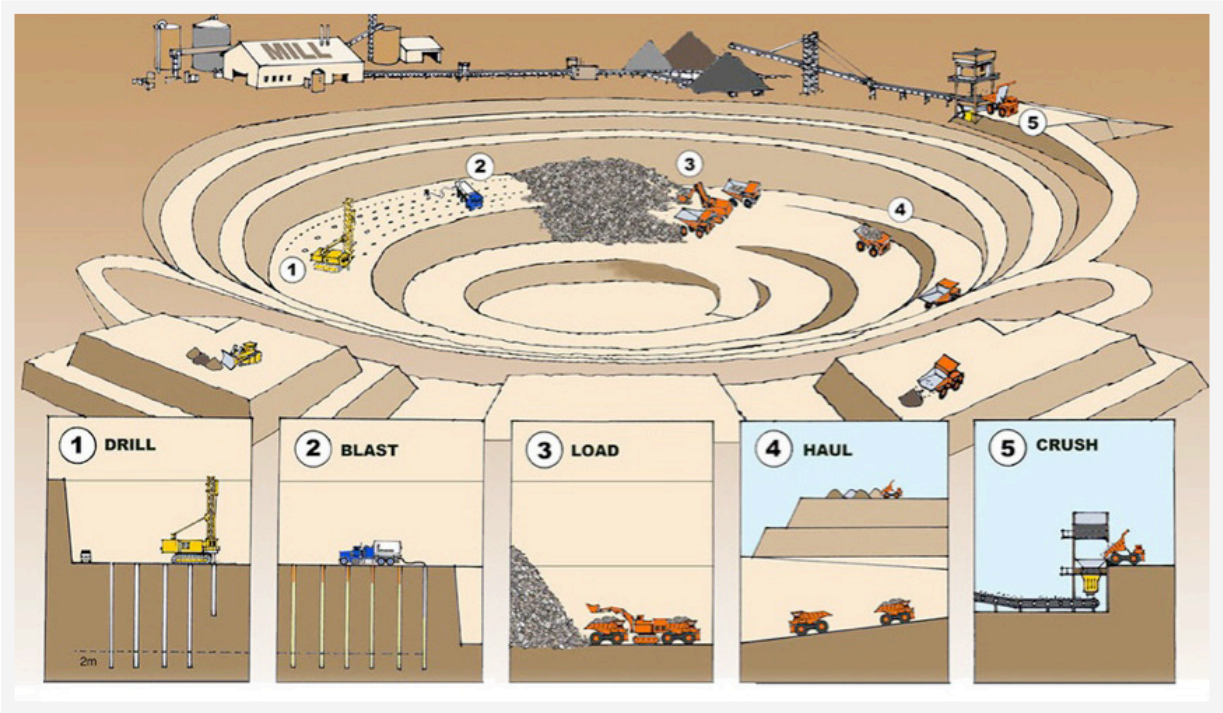


Figure 5: Open pit mine system overview[16]

Major equipment used in mines include heavy haulers, draglines, loaders, backhoes, scrapers, water trucks, drills, wheel dozers, graders, mining shovels, production conveyor belts, etc. Production operation mines use four major utilities to run: electricity, water, diesel, and compressed air.

Electricity is crucial to a mining operation. A typical mineral processing facility and mine uses 120MW of electricity for a 100,000 t/d (metric tons per day) operation.[17] Major considerations for electricity usage are: expected size of the mine, anticipated potential expansion, types of equipment to be used, haulage methods to be used, available power from the utility company, and the amount of capital investment for the electrical system. Mines will also have power generation facilities on-site to supplement the power needs and to act as backup in case the main power supply is disrupted.

The following diagram shows electricity distribution in an open pit mine:

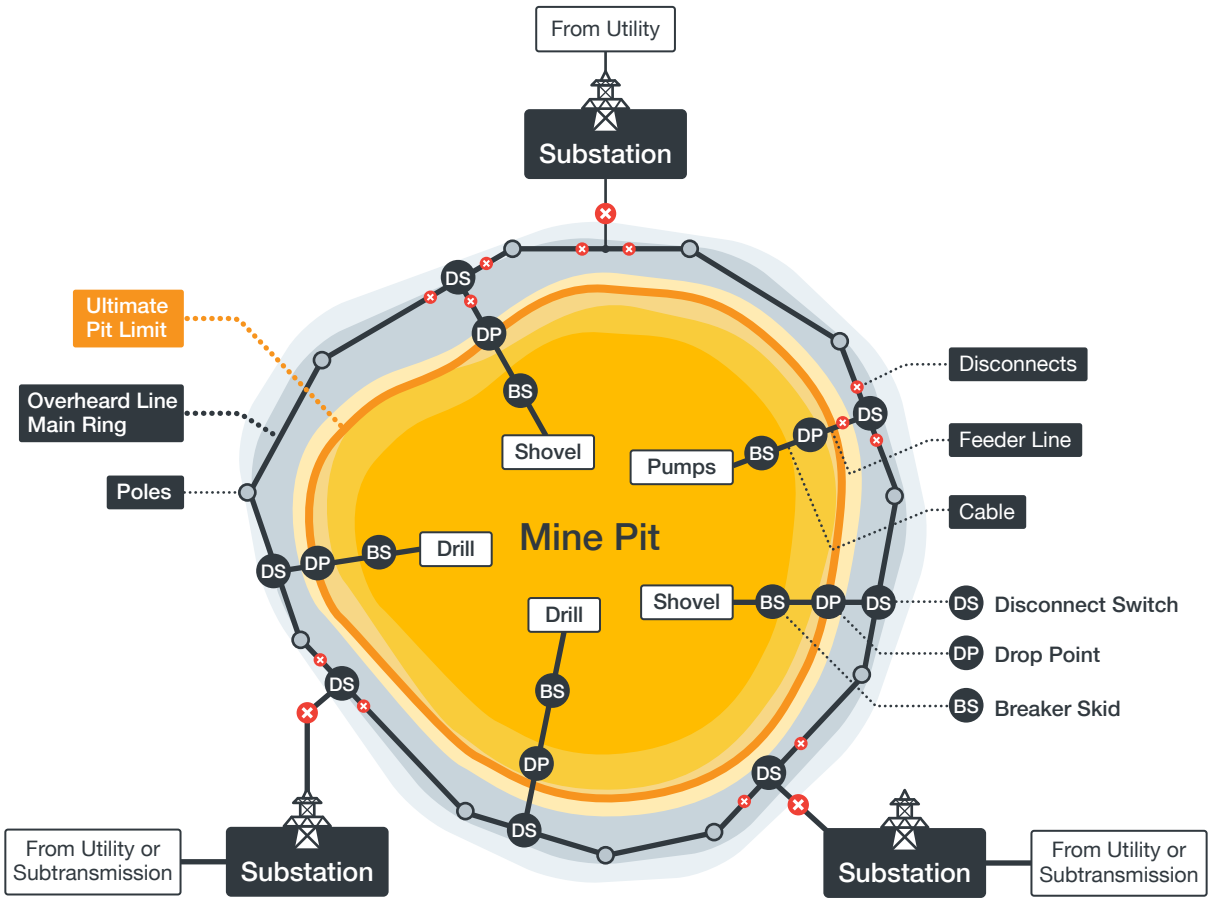


Figure 6: Open-pit ring mine radial power distribution system[18]

Major equipment in a mine that operates on electricity include: large autonomous and semi-autonomous grinding mills, ball mill drives, conveyor belts, high-pressure grinding rollers, cyclone feed pumps, mine hoists, dragline excavators, crushers, shovels, bucket wheel and bucket chain excavators. A steady electricity supply is the lifeblood of the modern mine. We have seen APT campaigns like BlackEnergy weaponized and targeting a mining company and power generation facilities in Ukraine.[19,20] Any serious disruption to the power supply resulting from a cyber attack or other reasons will effectively take the mining operation offline. The on-site power generation facilities are designed to provide backup power to essential equipment only for short periods of time.

Compressed air is used extensively in mining operations. Compressed air is stored energy and when controlled can be used for production purposes. It also has beneficial features such as being safer to use in certain situations, cleaner than other forms of energy, and easier to work with. Energy from compressed air is used to operate pneumatic equipment and pneumatic tools. Mining equipment that uses compressed air includes: pneumatic drills, air motors, instrumentation, etc.

Water is used in the mining industry for the extraction of minerals that may be in the form of solids, such as coal, iron, sand, and gravel; liquids, such as crude petroleum; and gases, such as natural gas.[21] Diesel is used throughout the mine to operate equipment such as haulers, trucks, dozers, drills, scrapers, shovels, backhoes, etc. Any disruptions to the supply chains of any of these major utilities resulting from a cyber attack or other reasons will effectively take the mining operation offline. The supply chain for the four major utilities forms part of the Achilles heel of any mining operation.

Mineral Processing

The ultimate goal of mining is to yield metals/minerals in their purest form. Mineral processing facilities don't need to be located at the mining sites and are typically built in central locations that can aggregate feeds from multiple mines. The mines crush the excavated ore rocks and transport them to the mineral processing facility. Processed metal/mineral concentrates are transported from the processing facility to the customers via rail, road, water, or air depending on the type, demand, and volume of the final product. The following diagram shows a high-level overview of the steps involved in metal extraction from ores at the King-king Copper-Gold Project:

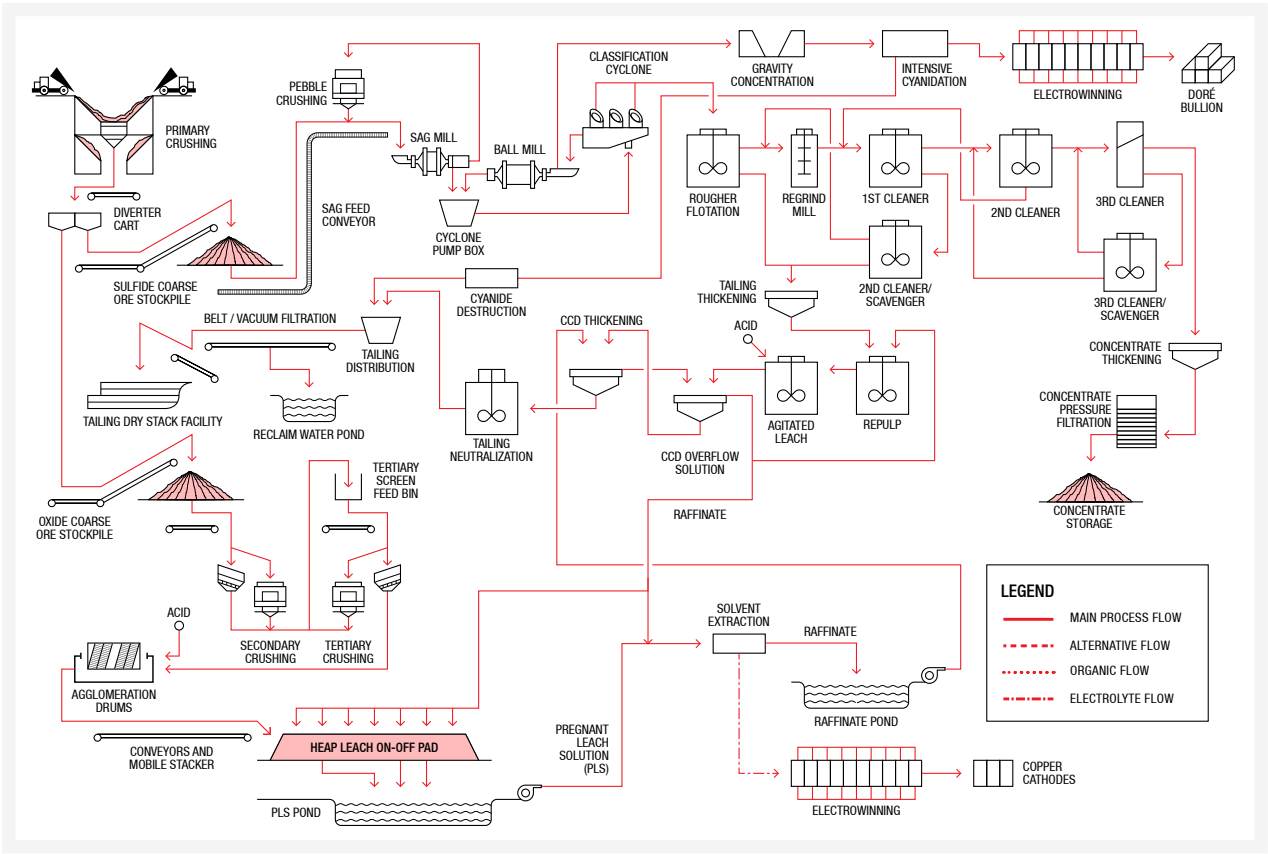


Figure 7: Flow chart of metal extraction at the King-king Copper-Gold Project[22]

Processing routes can be different and more than one route is possible for many metals (e.g., in the extraction of copper or gold from low-grade ores, heap or dump leaching is commonly used). The extraction process is optimized to achieve the highest possible recovery yield from the ores while maintaining acceptable purity (grade). Customers will further treat the concentrate to purify the metals/minerals. Unit operations in mineral processing include:[23]

- **Size reduction** – The process of crushing and grinding the ores to liberate valuable minerals from the ore, increase surface area for high reactivity, and to facilitate the transport of ore particles between unit operations.
- **Size separation** – Crushed and ground products are classified by particle size. Screens are used for coarse particulate sizing; cyclones are used for fine particles.
- **Concentration** – Physiochemical properties of minerals and other solids are used in the concentration operation and include: froth flotation, gravity concentration, and magnetic and electrostatic concentration.
- **Dewatering** – Most mineral processing operations are done in the presence of water. Solids must be separated from water for metal production. This is done with thickeners and filters.
- **Aqueous dissolution** – Many metals are recovered from ores by dissolving the desired metals in a process known as leaching with various lixiviates in the presence of oxygen. Following leaching the dissolved metals can be concentrated by carbon absorption, ion exchange, or solvent extraction. Purified and concentrated metals may be recovered from solution using reduction techniques like cementation and electrowinning.

Mineral processing is a complex industrial process involving numerous autonomous and semi-autonomous steps controlled by ICS, and is designed to achieve maximum yield from the ores. Mineral processing facilities thus face all the inherent cyber security risks associated with ICS.

Automation in Mining

Mining is a dangerous profession. In the 19th and 20th centuries thousands of fatalities occurred from mine explosions and other accidents.[24] Mine accidents stem from poisonous gas leaks, explosive natural gas leaks, dust explosions, structural collapse inside mines, earthquakes, flooding, malfunction of mining equipment, and the like. Today, mine safety, health legislations, advances in technology, and training has reduced mining deaths and injuries. The automation of hazardous, repetitive, and labor intensive tasks is a key contributor in improving mine safety. A cyber attack against the mining industry that targets automated mining equipment and processes jeopardizes the safety and lives of miners.

Autonomous operations started in the early 1990s.[25] By the mid '90s equipment suppliers were presenting buyers with options for automating equipment. Technology such as Global Positioning System (GPS), remote sensing, wireless communications, and high-speed telecommunications made automation viable. There are many driving factors behind mine automation:

- **Mining is a series of discrete operations such as drilling, blasting, loading, hauling, and materials processing.** The industry is moving towards low-grade, super-large, high-tonnage, and ultra-mechanized operations. This has created a need to increase yields through greater understanding and control of the production process. Automation increases the level of control in a highly variable and unpredictable environment by applying stringent rules to the decision-making process and removing randomness inherent in isolated decision-making.

- **Mines have to be built where the ore bodies are located, often times in remote locations.** In today's competitive economy mining companies are finding it increasingly difficult and expensive to attract and recruit skilled labor in unattractive locations. Automation allows staff to remotely operate equipment and oversee operations at the mining sites, and the mining company needs to maintain a smaller workforce at the actual mines. Automation also means a single operator can operate multiple machines and this reduces overall operational costs.

- **Ultimately, automation is a boon.** It improves the safety of miners, reduces operational costs, brings production consistency, increases production capacity, increases the level of control at each stage of production, limits operational variance, improves precision, manages equipment wear and tear through real-time monitoring, allows for accurate process modeling, etc.

Automation is suited to a number of key mining operations such as: production drilling and the real-time recognition of materials being drilled; automated materials handling using equipment like haul trucks, loaders, diggers, shovels, conveyors, and sizers; automated and accurate movement of equipment; monitoring of moving parts for maintenance and diagnostic intervention. One of the most visible elements of the modern mine are automated haul trucks.

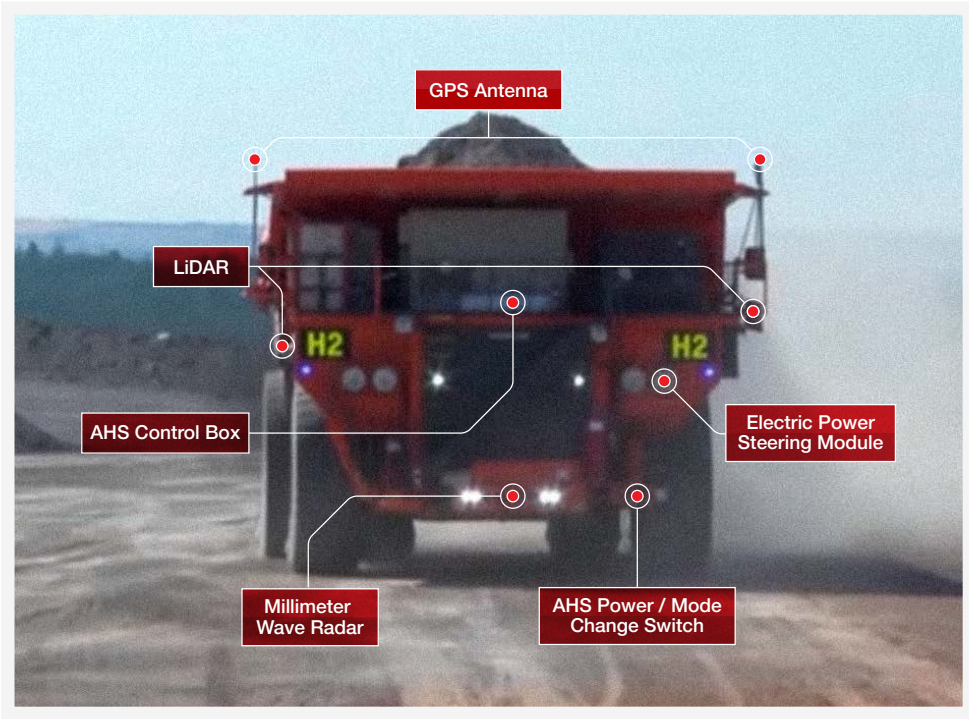


Figure 8: Hitachi Autonomous Haulage System (AHS) elements[26]

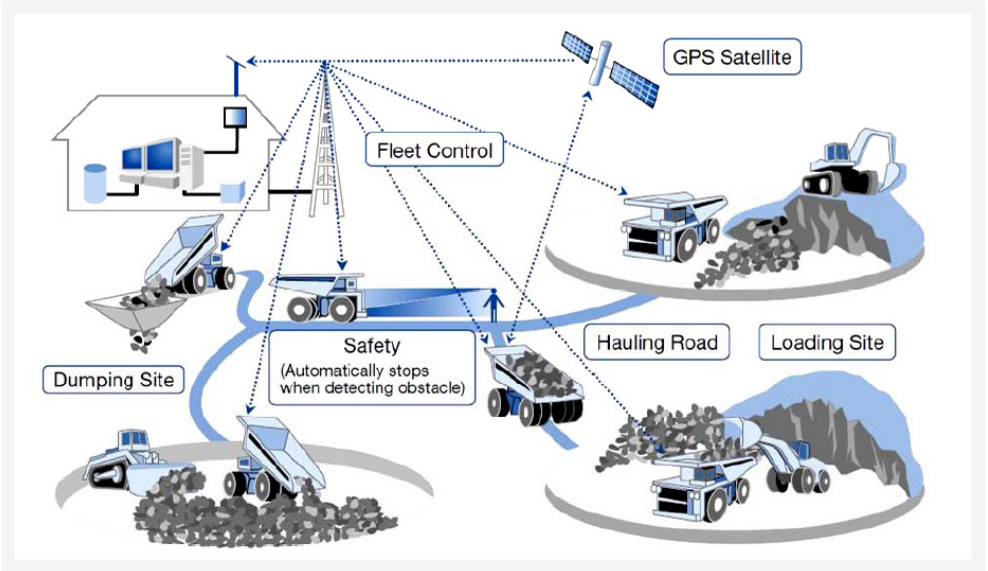


Figure 9: Autonomous Haulage System ecosystem[27]

Accurate positioning is important for the remote operations of automated haul trucks. On-board sensors generate real-time maps of the mine environment (geometry and geology) around these trucks so they can be remotely operated for positioning:

- Above ground they will use a combination of: Real Time Kinematic (RTK) Global Navigation Satellite System (GNSS) + machine sensors (e.g., odometers) + inertial guidance + perception-based positioning (e.g., radar, laser, vision, and sonar) + pseudolites (ground-based satellite or reference stations)
- Below ground they will use a combination of: radio frequency-based distance measurements + perception-based positioning (e.g., radar, laser, vision, and sonar) + machine sensors (e.g., odometers) + inertial guidance

These tools accurately locate and control the activities of the automated haul trucks. The position and status of all automated equipment in the mining site are fed to the central management system at the ROC. This allows for sophisticated process modeling and activity coordination that ultimately leads to improved mineral recoveries and lower costs. Any serious disruptions to the operations of automated mining equipment resulting from a cyber attack will take the mining operation offline causing financial loss and possible equipment damage.

With mines becoming automated, capacity increases are needed for the transfer and manipulation of huge amounts of data. Efficient data warehousing and data fusion solutions are needed for daily mining operations. This has led to the creation of the ROC.

Figure 10: BHP Billiton's Integrated ROC, Australia[28]

ROCs enable supervision, control, analysis, and data acquisitions from remote mining sites. Improvements in telecommunications infrastructure, in particular telephone networks and fiber-optic links are key enablers for the development of ROCs. Business drivers for the development of ROCs include:

- Improvements in occupational health and safety by removing operators from risk exposure
- Reduced labor cost by relocating high-cost, knowledge-intensive staff away from mines to cities
- Increased productivity through identification of inefficiencies in operations, collaborative planning between functions, process visibility across the production chain, and the creation of centralized knowledge and experience hubs
- Business integration with the regional offices and the head office to help them make fast and well-informed decisions

"As mining and resource companies move into the next generation of remote operations, cloud computing, big data and analytics, and mobility, they will need to dramatically increase their security posture in order to maintain on-going operations."[29] The ROC serves as the nerve center of the modern day mining operation. Cybercriminals planning disruptive or destructive cyber attacks against a mining company will attempt to compromise the ROC because the ROC serves as a single point of failure that can take the entire mining operation offline.

Mining Communication Infrastructure

A mining communications system (MCS) is a network of devices that collect, receive, or transmit information. The MCS has three components: the information source or transmitter, the communication pathway or network, and the information receiver.

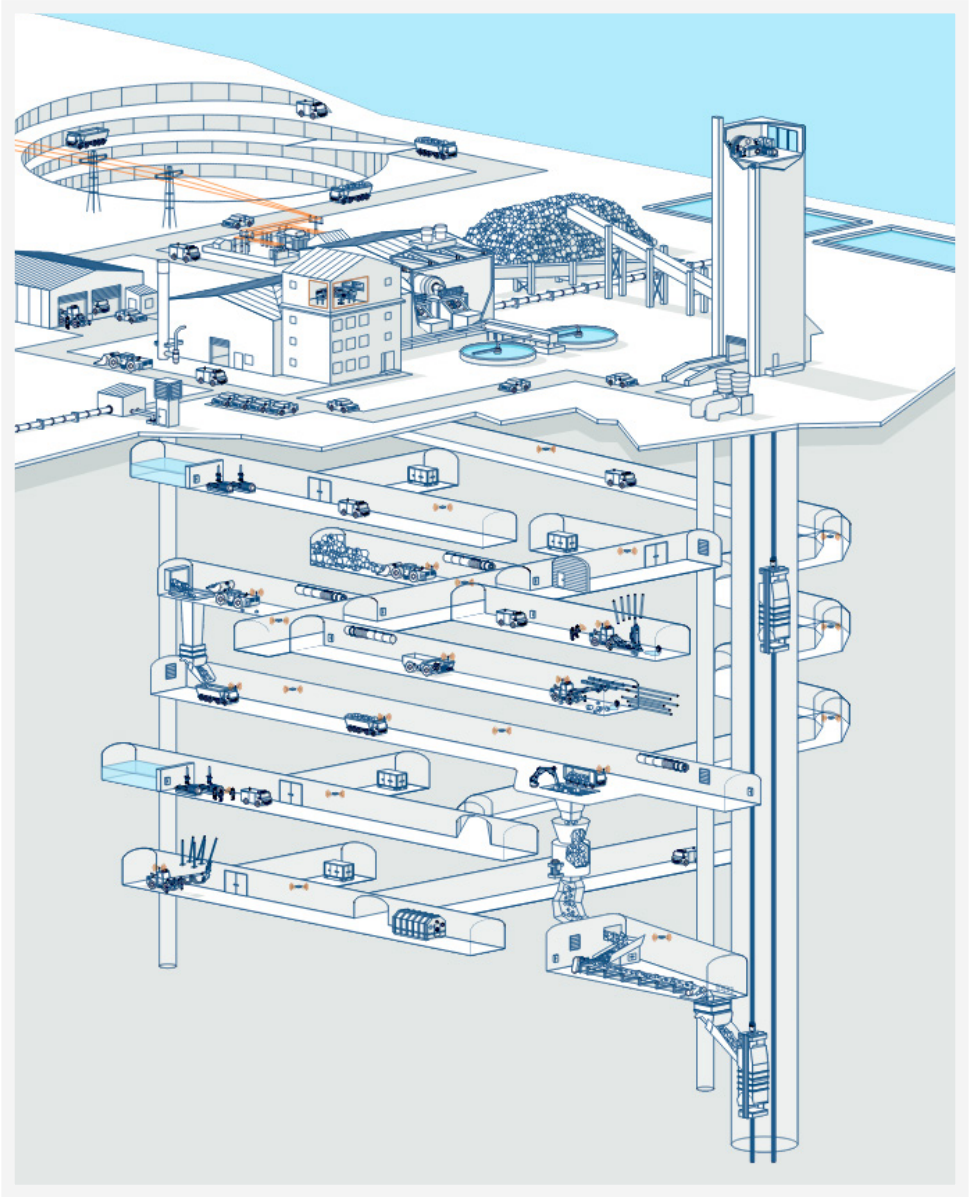


Figure 11: Example of wireless underground mine communications systems[30]

Mines traditionally have multiple communication networks for the different applications and for fault tolerance. Networked mining equipment uses wireless, wired, or hybrid (wired and wireless) connectivity. Underground mining networks mostly rely on cables, but wireless networks are also extensively used. The following table compares the different communication technologies:

Technology	Typical Application	Advantages	Disadvantages
VHF/UHF	Voice, data, tracking	High bandwidth, can allow many users, accomodate high traffic; multiple voice channels; small and wearable antennas; factors impacting safety are known	Best for line-of-sight applications (not good around bends)
MF	Voice, data	Can turn corners; metal infrastructure (pipes, track, wires, etc.) in the mine can help increase range (parasitic propagation)	Limited bandwidth; existing electrical and communications system may cause interference, though not as much as for ULF/ VLF/LF
ULF, VLF, and LF	Personal emergency devices	Can go through the earth	Natural phenomena, existing electrical and communications system can cause severe interference; very limited bandwidth; require surface or underground loop antennas
UWB	Tracking, data	Ideal for tracking; no interference from existing electrical and communication systems and multiple effects; very high bandwidth; simple architecture (potential to be inexpensive)	Very short range

Source: Nutler 2007; Chehri et al. 2008; Friedlos 2008; Swedberg 2008; NIOSH, n.d. (a).

Table 1: Comparison of the different communication technologies[31]

The MCS uses a variety of communications system infrastructure: wired mesh systems, wireless mesh systems, RFID leaky feeder infrastructure systems, fiber infrastructure systems, and serial infrastructure systems. A successful MCS has the following attributes:

- Can accommodate different types of information sources
- Can accommodate existing infrastructure
- Can accommodate information source mobility
- Supports safe, robust, and redundant operations
- Can be easily scaled up in size and allows for easy maintenance

One of the major applications of the MCS is mine monitoring systems. Mine monitoring systems are used for production monitoring, equipment status monitoring, and safety and environment monitoring. Monitoring system manufacturers typically have their own reporting applications. There are unified reporting applications that collate, process, and display information from all the different monitoring systems in the mine. To facilitate visibility across all the mine monitoring systems, received data from each system is fed into a central reporting database and further processed to get the unified picture. These reporting databases are valuable espionage targets for cybercriminals because they provide real-time status updates of the mining operation.

Intersection of Mining and Oil and Gas Industries

We mentioned previously that in countries like Canada and Venezuela, oil sands are surface-mined, processed, and converted into petroleum products. With oil sands production there is an intersection of mining with the larger and more complex oil and gas industry. In general the oil and gas industry has four main segments: upstream, midstream, downstream, and service.[32]

- **Upstream** – the exploration, recovery, and production of oil and natural gas
- **Midstream** – the collection and transportation of crude oil, natural gas, and refined products
- **Downstream** – the manufacturing, selling, and distribution of natural gas and products derived from crude oil
- **Service** – companies that provide services to the oil and gas industry but do not produce petroleum or petroleum products themselves

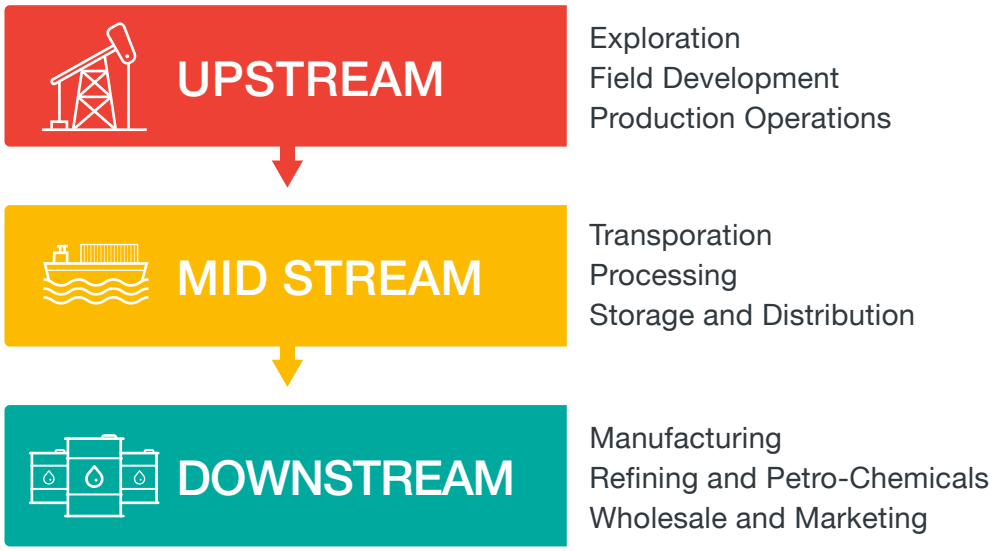


Figure 12: Oil and gas supply chain[33]

Majority of the companies in the oil and gas industry operate in one of these four main segments, but there are companies that operate in more than one segment. The super majors are the six largest non-state owned oil companies that do all functions: upstream, midstream, and downstream. The six super majors are Exxon Mobil, Total S.A., Royal Dutch Shell, BP, Chevron, and ConocoPhillips. It is important to our discussion to highlight the fact that third-party vendors and contractors play a major role in daily operations, and that means there are more available avenues for potential cyber attacks. Also, companies that belong to more than one segment of the oil and gas supply chain are at risk on multiple fronts. The retailer Target was victimized in one of the largest credit card data breaches back in November 2013. It later emerged that the cybercriminals broke into Target's network via a third-party Heating, Ventilation, and Air Conditioning (HVAC) vendor that had access to Target's corporate network.[34] Third-party vendors and contractors don't have uniform cyber security policies and practices. This creates exploitable weaknesses in the operations chain, as was demonstrated in the case of Target.

Everyday mining operations aren't discretely segmented like the oil and gas industry, but nonetheless they extensively employ both contractors and third-party vendors across the production chain. Contractors in turn hire subcontractors, all of which contribute to a challenging cyber ecosystem especially when the vendors, contractors, and sub-contractors all have operational needs to access the mining and corporate networks.

Economic Factors of Mining

Economic Cycles

The mining industry is a commodity-centric global player that is affected by the ups and downs of the market-driven global economy. One of the realities the mining industry has to cope with is: commodity prices are subject to significant short-term volatility as well as longer-term cycles. A contraction in manufacturing will result in reduced demands for raw materials and, in turn, slowdown for the mining industry. Conversely, supercycles that generally follow a major event, e.g., post-war rebuilding of infrastructure after World War II, increases demands for raw materials spurring major growth in the mining industry. The current supercycle, the industrialization of BRIC (Brazil, Russia, India, and China) economies is slowing down. This has led to a fall in demand for raw materials and consequently a drop in commodity prices. Falling demands and drop in commodity prices have caused slowdown in the economies of countries such as Australia and Canada, which heavily rely on the export of natural resources. On the flipside, in countries like the United States that are less dependent on the export of natural resources, the drop in commodity prices has had a comparatively smaller economic impact.

This economic dimension might at first glance not seem relevant to any discussion of cyber vulnerabilities. But it is important because it shows how vulnerable the economies of some countries are to any disruption affecting a key contributor of the economy, which can be also brought about by cyber attacks. The following figure shows the main export items that are important for the economies of specific countries. Any resource-rich country that builds its economy on mining commodities would be extremely vulnerable to any interference or disruption in this area.

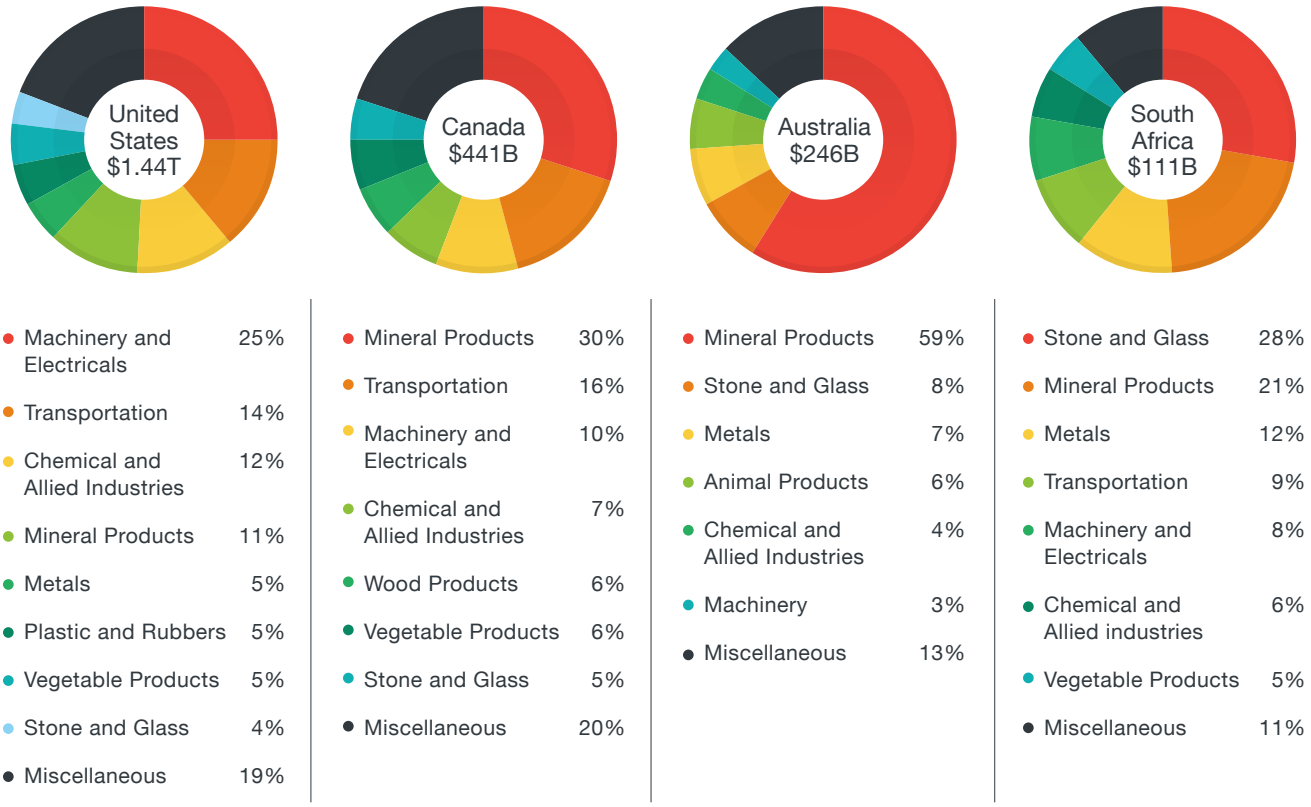


Figure 13: Main exports for United States, Canada, Australia, and South Africa in 2014[35]

Pricing of Metals and Minerals

The aim of exploration geology is to discover mineralized target areas that can be developed into profitable mines. For today's transnational mining company this may mean it is cheaper to produce copper from a few large mines in Chile than it is to produce copper locally from many small mines. As extraction costs fall, so do the prices of raw materials—the effects of globalization of trade. Currently there is a shift away from mining higher-grade, higher-quality ores in politically risky countries to mining lower-grade, lower-quality ores in politically stable countries. Advancements in technology and the production process have improved yields from lower-grade ores, which ultimately makes the mines profitable over their lifetimes. Prices for metals are set according to the weight of a standard unit of refined product. Reference prices for industrial metals or minerals may not be directly applicable to the final product of the mines. Mines will sell their products at different refined levels because of production constraints, transportation capacity, or to meet customer needs. There are two critical dimensions to pricing: transportability (ability to move the mined minerals) and homogeneity (degree of standardization), which ultimately determines the negotiated price between the buyer and seller.

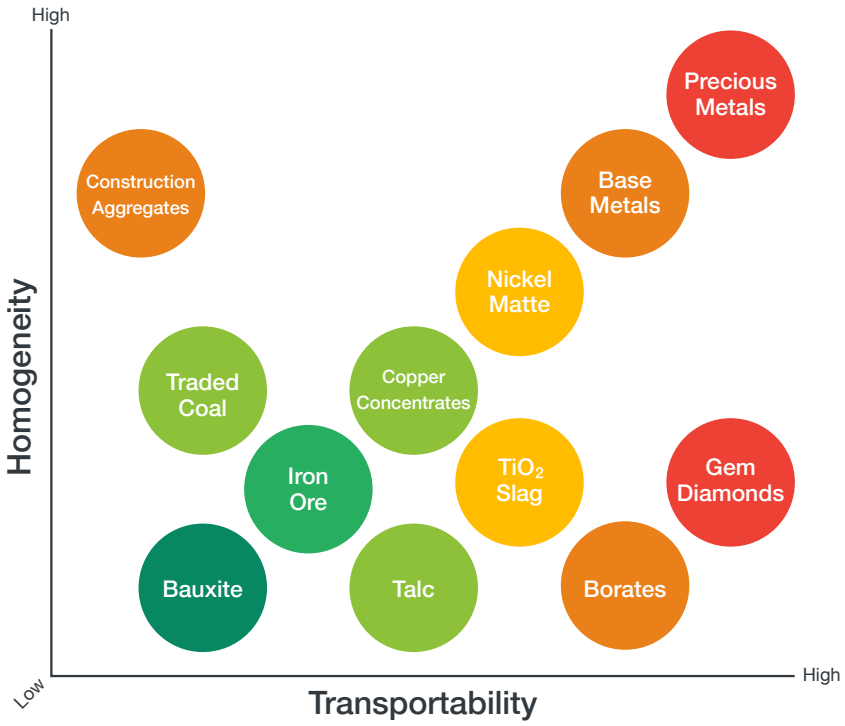


Figure 14: Two critical dimensions for pricing of metals/minerals[36]

The theft of pricing data is one of the goals of threat actors targeting the mining industry. The goals of a cyber attack against the mining industry are different from the goals of a cyber attack against the hospitality industry—espionage versus immediate financial gains. These are some of the specific threats that IT security in the mining industry have to understand when defending their ecosystem.

Cyber Attacks Targeting the Mining Industry

Why Is the Mining Industry Targeted?

When we analyze why the mining industry could be a viable and important target, there are three clear factors that explain its relevance.

1. Increasing and continued importance of commodities as traded entities on international markets
2. Reliance on natural resources for economic development
3. The need for countries to benefit from their own mineral deposits[37]

The mining industry is both a geopolitical and an economic target. Motivations for attacking the mining industry therefore go beyond any direct monetary value. The most important motivations are the following:

Latest Technical Knowledge and Intelligence for Competitive Advantage

Cyber espionage campaigns against the mining industry are largely geared towards ensuring interest groups have access to the latest technical knowledge and intelligence so they can maintain a competitive advantage and thrive in the global commodities market.

- The theft of pricing data for metals or minerals is one of the goals of threat actors targeting the mining industry. Having insider information about a mine's pricing data can help a competitor hijack a sales deal by outbidding the competition, or a buyer negotiate a better purchase price or change the terms of a takeover bid, etc. Customer information is another prime target for data theft. Competitors can use the stolen customer information to hijack future sales.
- Intellectual property (IP) such as production methods, mineral processing methods, chemical formulae, custom software, etc. is a lucrative target for cybercriminals. The theft of IP can drastically reduce the R&D costs associated with developing a new mine. IP theft is commonly done by foreign cyber espionage campaigns, which then transfer the knowledge to their local mining industry.

- Foreign cyber espionage campaigns are increasingly interested in learning about governance policies, decisions, and decision-making processes of corporate executives. This is because good decisions and good governance policies are critical to the success of any mining operation. The goal is to learn about these decisions and policies and apply them to the local mining industry.
- Mining companies invest billions of dollars every year exploring potential new mining sites in the hopes of "hitting pay dirt" i.e., discover an ore-rich area that can be successfully mined. The exploration phase generates big data sets that the geologists analyze to identify new ore deposit locations. The exploration data is expensive to generate and is key to the company's future growth and success, which makes this data a lucrative target for cyber espionage campaigns.
- The mining industry is moving towards low-grade, super-large, high-tonnage, and ultra-mechanized operations. This has turned smaller mining operations economically unfeasible leading to closures, mergers, and takeovers. The fundamental source of a mine's value is its potential ore reserve. Ore reserve and production data are key targets in cyber espionage campaigns especially when a merger or takeover bid is in the works—the goal is to deflate value if possible or to collect insider information and mount a successful bid.
- Mine-monitoring systems are used for production monitoring, equipment status monitoring, and safety and environment monitoring. There are unified reporting applications that collate, process, and display information from all the different mine-monitoring systems. Received data from each monitoring system is fed into a central reporting database and further processed to get the unified picture. These reporting databases are valuable espionage targets for cybercriminals because they provide real-time status updates of the mining operation.

Cyber Attacks with the Intent of Weakening a Nation's Economy

Cyber campaigns can also be used for conducting carefully planned strategic or retaliatory cyber attacks against a key contributor to the nation's economy.

- The high capital cost and long lifetime of a mining operation leads to lower rates of technological changes. This means mining operations are using equipment and communications protocols that are vulnerable to crippling cyber attacks because standards and equipment upgrades are deemed unnecessary for continued production.
- Any disruption to the supply chains of the major utilities used in mining (electricity, water, diesel, and compressed air) resulting from a cyber attack or other causes will effectively take the mining operation offline. The supply chain for the four major utilities forms part of the Achilles heel of any mining operation.

- Automation of hazardous, repetitive, and labor intensive tasks is a key contributor in improving mine safety. Cyber attacks that target automated mining equipment and processes jeopardizes the safety and lives of miners.
- Any serious disruptions to the operations of automated mining equipment resulting from a cyber attack will take the mining operation offline causing financial loss and possible equipment damage.
- Mineral processing is a complex industrial process involving numerous autonomous and semi-autonomous steps controlled by ICS and is designed to achieve maximum yield from the ores. Mineral processing facilities thus face all the inherent cyber security risks associated with ICS.
- The ROC serves as the nerve center of the modern-day mining operation. Cybercriminals planning disruptive/destructive cyber attacks against a mining company will attempt to compromise the ROC because the ROC serves as a single point of failure that can take the entire mining operation offline.
- Third-party vendors and contractors play a major role in daily mining operations, and that means there are more available avenues for potential cyber attacks. Third-party vendors and contractors don't have uniform cyber security policies and practices. This creates exploitable weaknesses in the operations chain.

Classic Theft of Data Such as PII, Credentials and Financial Data

Mining companies are also subject to data breaches that threaten all types of businesses (both big and small). The majority of data breaches aim to steal Personally Identifiable Information (PII), financial data, and credentials.[38]

- PII can be used for committing identity fraud, filing fraudulent tax returns, applying for loans or credit cards, registering fake accounts, selling to marketing firms, and launching spam and phishing attacks.
- Financial data can be used for creating counterfeit credit cards, paying bills, making fraudulent online transactions, and transferring money out of a victim's bank accounts.
- Credentials can be used for stealing IP, committing espionage, and launching spam and phishing attacks.
- There are cases where the stolen data is used in vengeance attacks and/or hacktivism. The victims are blackmailed or the stolen data is held for ransom payment.

The Perception of Mines as Environmental Polluters

Some environmentally conscious activists who are protesting the effect mining companies have in terms of environmental damage, wildlife habitat damage and other stated concerns, take it upon themselves to retaliate by inflicting damage to the mining companies.

What Types of Actors Are Interested?

Nation States

Nation states as perpetrators of cyber attacks or cyber-based interference might want to gather intelligence and are increasingly using cyber assets as the primary method for this. Governments in developed countries have created sophisticated and stealthy cyber assets that can lie undetected inside organizations for years collecting and transmitting data. Developing nations are utilizing cyber espionage as a quick and economical way of increasing their intelligence-gathering capabilities.

Organized Cybercriminal Syndicates

Intrusions orchestrated by criminal syndicates can be split into two categories. The first category is made up of criminal gangs who steal and sell sensitive information, encrypt sensitive documents and demand ransom, compromise computers and turn them into botnets, etc. The second category is criminal gangs, who have been contracted by national governments to conduct cyber espionage campaigns, or to carry out politically motivated disruptive or destructive cyber attacks—criminals for hire. By using criminal gangs national governments maintain plausible deniability in case of discovery. There may be some intersect between these two categories where easy profit can be made.

Competitors

Competitors spying on each other goes back to the origins of trade. Competitors are interested in information such as intellectual property, production methods, true production capacity, pricing information, customer information among others. In extreme cases competitors might launch disruptive or destructive cyber attacks against their competition in order to gain a stronger foothold in the market or overcome a disadvantage.

Hacktivists

Hacktivists are internet activists. They attack cyber assets in order to draw attention to their political causes and frequently choose high-visibility or high-profile targets. Often their targets and their stated causes do not match up. Mining, and oil and gas companies are frequent targets of hacktivists protesting the effect they have in terms of environmental damage, wildlife habitat damage, corporate greed and other stated concerns.

How do mining companies get compromised?

The most common attack route by which companies get infiltrated is via targeted attacks.

1. The first step for a targeted attack is entry into the organization's network.

2. From there the attacker will try to leverage the initial point of entry to laterally move within the network and successfully compromise other systems. The challenge here is to find a reliable method for infecting the organization's computers.

Some of the most commonly observed infection techniques (step 1) are:

- **Phishing and social engineering attacks:**
  Malware used in targeted attacks are never spammed out to millions of potential victims. Instead they are sent to a chosen few targets via phishing emails with effective social engineering lures. ICS security consultants, Digital Bond, conducted an experiment where they sent out spear phishing emails with an embedded link to key ICS personnel in different companies. They used Open Source Intelligence (OSINT) to identify their spear phishing targets. 25% of the highly targeted recipients fell victim to the spear phishing attack and clicked on the link. Job titles of the victims typically include: Control System Supervisor, Automation Technician, Equipment Diagnostic Lead, Instrument Technician, etc.[39]

- **Vulnerability exploitation**
  New software vulnerabilities are disclosed and patched every month by their respective vendors. Only a handful of these are successfully "weaponized." Once weaponized, the vulnerabilities will be used in cyber attacks for years e.g. CVE-2008-4841, CVE-2010-3333, CVE-2012-0158, CVE-2010-2568, etc. Exploits successfully compromise systems because patches for the vulnerabilities have not been routinely applied and many servers are still running OS which are no longer supported.

- **Watering hole attacks**
  The attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and leverage that to gain access to the network at the targeted user's place of employment.[40]

- **System misconfiguration exploitation**
  System misconfigurations can happen at any level of an application stack. The attacker discovers these flaws and exploits them to compromise the system. Example: an open directory in a webserver may expose important files and configuration information that an attacker can leverage.

- **Drive-by-download attacks**

  Malware is automatically downloaded to the computer and executed without the user's consent or knowledge. Pop-up download windows that appear during regular web browsing require the user's consent to continue. Drive-by-downloads can be initiated by simply visiting a website or viewing an HTML email message and requires no user interactions.[41]

- **Malvertising**

  Malvertising is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.[42] This is an effective infection strategy when paired with watering hole attacks2

- **3rd party vendors**

  Attackers are successfully compromising contractors and 3rd party vendors and leveraging them as backdoor pathways into the targeted corporate networks. The national retailer Target was victimized in one of the largest credit card data breaches ever back in November 2013. It later emerged that the cybercriminals broke into Target's network via a 3rd party HVAC vendor who had access to Target's corporate network.[43] 3rd party vendors and contractors don't have uniform cyber security policies and practices. This creates exploitable weaknesses in the operations chain, as was demonstrated in the case of Target.

- **Man-in-the-Middle (MitM)**

  MitM are attacks where the attacker intercepts, alters, and relays communications between two systems/endpoints/parties who believe they are directly communicating with each other. The attacker must be able to intercept all relevant messages passing between the two victims, and either alters the messages or inject new ones. This is easy in many situations e.g. an attacker within reception range of an unencrypted wireless access point can insert themselves as the man-in-the-middle. MitM attacks aim to circumvent mutual authentication, or the lack thereof. A MitM attack is successful only when the attacker can correctly impersonate the endpoint's behavior as expected from the legitimate other end.[44]

- **Infected equipment**

  Manufacturers ship brand new equipment preloaded with malware. While this may sound unlikely, there have been recent examples such as Lenovo shipping laptops pre-installed with malware.[45] In our conversations with IT security professionals working in different mining companies, stories of mining equipment coming preloaded with rather sophisticated malware such as Stuxnet were discussed many times.

- **Insider job**

  Insider jobs are the most difficult infection vector to protect against as it involves people that the organization trusts, or who can abuse their privileges to commit crimes. These could be disgruntled or disillusioned employees out to take revenge, or could be unscrupulous individuals out to make some quick cash by victimizing their employers.

Lateral movement (step 2) involves activities related to reconnaissance, credential theft, and infiltrating other computers.[46] Attackers compromise a machine inside an organization's network; using the compromised machine as a beachhead they will attempt to gain access to other networked computers and spread malware onto them. Lateral movement uses the victim's own resources against themselves – the attacker will use legitimate Windows OS features and tools used by IT Administrators to move around the network. Lateral movement happens at human speed and takes time to succeed. Stealth is an important factor in lateral movement in order to remain undetected, penetrate deep inside the victim's network and stay there for as long as possible.

Notable Cyber Attacks That Have Occurred

News stories about cyber attacks against the mining industry don't gain a lot of attention compared to news stories on cyber attacks targeting other industries such as retail, hospitality, technology, or more "high-profile" attacks targeted at banks or hospitals. We compiled a list of mining industry cyber attack stories between 2010 and now that demonstrates the actual impact of some of the cyber threats discussed in this research paper. This list shows that these attacks do occur and bring significant fallout.

Date	Victim(s)	Description
April 2010	Rio Tinto Group, BHP Billiton Ltd. and Fortescue Metal Groups	Mining giants Rio Tinto Group, BHP Billiton Ltd. and Fortescue Metal Groups were all attacked by hackers originating from Asia. Experts believe that the main goal behind these attacks was commercial espionage.[47, 48]
February 2011	BHP Billiton	BHP Billiton's boss, Marius Kloppers, confirmed that the main reason behind his push for market pricing of key commodities was espionage campaigns, run by nation states and competitors, have penetrated deep inside BHP Billiton's business. Market pricing for key commodities minimizes any impact of differential information that one party or the other may hold.[49]
April 2011	Australian Federal Parliament	Hackers broke into Australian Federal Parliamentary email accounts to gain access to email conversations between ministers and executives of Australian mining companies operating in China.[50]

Date	Victim(s)	Description
October and November 2011	Potash Corporation, law firms, and the Government of Canada's Finance Department and Treasury Board	Hackers attacked the secure networks of several law firms and eventually broke into computers of the Government of Canada's Finance Department and Treasury Board. They phished employees at these two departments with an email pretending to come from an aboriginal group. The hackers were searching for insider information about a corporate takeover bid for the Potash Corporation of Saskatchewan.[51, 52, 53]
February 2012	Lynas	Lynas Corporation, a rare earth mining company, had its website hacked by hacktivists. Activists were protesting against the environmental impact of Lynas's operations in Malaysia.[54]
July 2012	TVI Resource Development	Canadian mining company TVI Resource Development (TVIRD) was discovered to be the victim of a "sophisticated, vicious, and concerted" cyber attack. Emails purportedly coming from TVIRD claimed murder and other criminal conspiracies against small-scale miners in Balabag, Philippines. The goal was to discredit TVIRD and force them to give up their Mineral Production Sharing Agreement in Balabag so that the small-scale miners will have exclusive possession over the area for their illegal mining operations.[55]
January 2013	Bumi	Samin Tan, chairman of Bumi, one of the world's largest mining companies, got phished by a person who claimed to be working for Wikipedia. Documents related to Bumi's finances and private email conversations were stolen.[56]
May 2013	AngloAmerican	Anonymous, as part of their Operations Green Rights campaign against companies accused of being responsible for "destroying nature and ancient cultures," attacked AngloAmerican, the world's largest producer of platinum. Anonymous breached the company's websites and leaked sensitive data online. Information leaked includes PII, credentials, and investor information.[57]
October 2013	Brazil's Mines and Energy Ministry	Documents leaked by former NSA contractor Edward Snowden purported Western spy agencies targeted phone calls and email conversations to and from Brazil's Mines and Energy Ministry.[58]
May 2014	Alcoa Inc. and Allegheny Technologies Inc.	Aluminum maker Alcoa Inc. and metal supplier Allegheny Technologies Inc. were identified as victims of hacker attacks originating from Asia. Alcoa and Allegheny did not disclose the hacking incidents to the Securities and Exchange Commission (SEC) because the thefts weren't "material" to their business and hence disclosure was not mandatory as per SEC rules. Commercial espionage was the most likely goal behind these cyber attacks.[59]

Date	Victim(s)	Description
February 2015	Nautilus Minerals and Marine Assets Corporation	Canada's Nautilus Minerals and Dubai-based marine solutions company Marine Assets Corporation (MAC) were victims of a cyber scam that resulted in Nautilus paying a $10-million deposit intended for MAC into an unknown bank account.[60]
April & May 2015	Detour Gold Corp.	Canadian gold mining company, Detour Gold Corp. was hacked by a group that calls themselves the Angels_Of_Truth. 100GBs+ worth of data was stolen from the Detour Gold networks. 18GBs of compromised documents were shared on a torrent site.[61, 62]
June 2015	Codan	Australian communications, metal detection, and mining technology firm Codan reported sales and prices of the firm's metal detectors have collapsed after hackers stole its designs and began manufacturing counterfeit metal detectors.[63]
November 2015	International Mineral Resources	International Mineral Resources (IMR) filed a lawsuit claiming rivals EuroChem Volga-Kaily hired New York City law firm Salisbury & Ryan to dig up information on IMR after a mining business deal went bad. Salisbury & Ryan allegedly hired a former Soviet military counter intelligence officer to conduct a hacking campaign against IMR.[64]
February 2016	The New South Wales Department of Industry, Resources and Energy	Hackers targeted the New South Wales Department of Industry, Resources and Energy. They unsuccessfully attempted to access confidential information related to mining approvals.[65,66]
February 2016	Ukrainian mining company	BlackEnergy and another APT campaign, Sandworm, were discovered as the likely perpetrators behind outages at two power generation facilities in Ukraine in December 2015. BlackEnergy and KillDisk were discovered in attempted similar cyber attacks against a mining company and a large railway operator also in Ukraine.[67]
April 2016	Goldcorp	The Canadian gold-mining firm Goldcorp suffered a major data breach. The hackers leaked 14.8GBs of data online by publishing a document on Pastebin with a URL address to a full torrent download. The archive includes employee PII and financial data.[68]

Corporate espionage Hacktivism Manipulation Physical damage

Table 2: Notable cyber attacks on mining companies

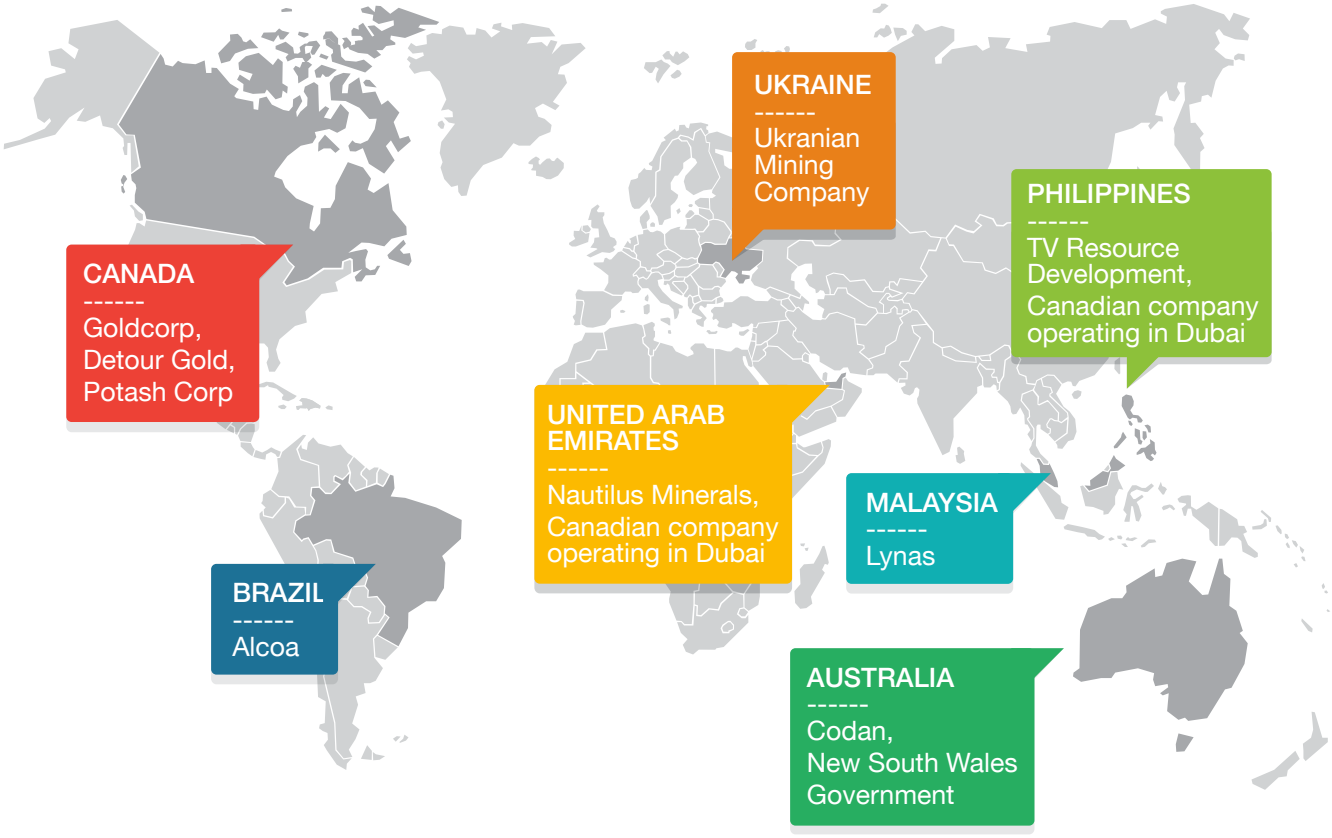
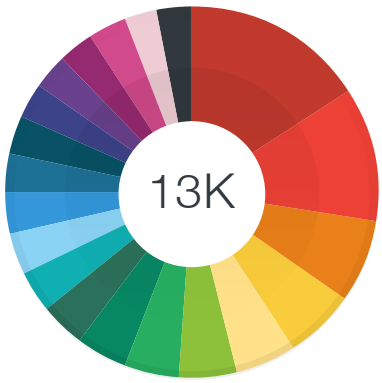


Figure 15: Geographic locations of cyber attacks on mining companies

Top Malware Threats Against Industries

Using Trend Micro's Smart Protection Network, we collected customer infection data for three industries that are subject to daily cyber attacks: Energy, Manufacturing, and Oil and Gas, for Y2015. Smart Protection Network does not have a separate industry categorization for Mining. The data collected is representative of Trend Micro's customer base and may not accurately represent the threat landscape, but still provides a good approximation of the general trends:

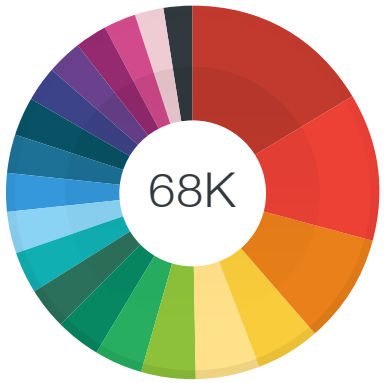


ADW_OPENCANDY	15.9%	ADW_TOMOS.SMN	3.6%
MAL_OTORUN1	11.7%	WORM_MESSEN.SMF	3.5%
MAL_HIFRM	7.3%	HKTL_KEYGEN	3.4%
CRCK_KEYGEN	6.1%	ADW_DEALPLY	3.2%
MAL_OTORUN2	5.3%	PE_SALITY.RL	3.2%
ADW_DOWNWARE	4.9%	ADW_DEALPLY.SM	3.1%
MAL_BUNDPIL-4	4.7%	WORM_GAMARUE.SMF	3.1%
ADW_ELEX	4.5%	ADW_BROWSEFOX	3.1%
MAL_BUNDPIL-2	3.9%	ADW_CROSSID	3.0%
MAL_BUNDPIL-6	3.7%	ADW_CROSSRIDER	2.8%

Figure 16: Top 20 malware detected in the Energy sector in 2015

ADW_OPENCANDY	16.2%	ADW_BROWSEF	3.7%
PUA_MONTIERA	9.3%	ADW_MYPCBACKUP	3.4%
ADW_MULTIPLUG	7.6%	TROJ_GEN.R021C0EFA15	3.2%
MAL_HIFRM	7.2%	ADW_DOWNWARE	3.0%
PUA_BROWSEFOX	6.0%	TROJ_GEN.R03EC0ODB15	3.0%
CRCK_KEYGEN	5.3%	PE_SALITY.RL	2.9%
MAL_OTORUN1	5.3%	ADW_DEALPLY.SM	2.8%
ADW_ELEX	4.6%	ADW_CROSSID	2.8%
ADW_FAKEGOOG	4.2%	JS_REDIR.VIBP	2.7%
ADW_CROSSRIDER	4.2%	HKTL_KEYGEN	2.6%

Figure 17: Top 20 malware detected in the manufacturing sector in 2015



ADW_OPENCANDY	16.7%	ADW_VPAYD	3.7%
MAL_HIFRM	12.8%	ADW_TOMOS.SMN	3.4%
MAL_OTORUN1	9.3%	ADW_CROSSRIDER	3.3%
CRCK_KEYGEN	5.8%	HKTL_KEYGEN	3.2%
WORM_DOWNAD.AD	5.5%	PE_SALITY.RL	3.1%
MAL_OTORUN2	4.6%	PUA_MONTIERA	2.9%
TROJ_GENERIC.APC	4.2%	ADW_MYPCBACKUP	2.7%
ADW_DEALPLY.SM	3.8%	ADW_DOWNWARE	2.7%
ADW_ELEX	3.7%	ADW_DEALPLY	2.6%
ADW_MULTIPLUG	3.7%	ADW_FAKEGOOG	2.3%

Figure 18: Top 20 malware detected in the oil and gas sector in 2015

From the Smart Protection Network data we can make the following observations:

- ADW_OPENCANDY is the top threat detected in all three industries. This is an adware module that is normally bundled with free software and is installed by default if the user simply clicks Next during the installation process. OpenCandy can change: the default homepage, desktop background, and default search engine. It also installs unwanted toolbars or plugins/extensions in the browser. OpenCandy transmits information about the user and their browsing habits to third parties without consent.[69]
- MAL_OTORUN, MAL_HIFRM, and CRCK_KEYGEN infections are predominant across all three industries. MAL_OTORUN detects worms that propagate using removable USB storage devices by relying on the autorun or autoplay feature in Windows. This feature enables removable media such as CDs and removable drives to start automatically upon insertion or connection to the system. MAL_HIFRM detects the presence of malicious Iframes in webpages. CRCK_KEYGEN detects cracking applications that may be unknowingly installed from a malicious/compromised website or manually installed by the user. These applications generate fake serial numbers to crack into programs that need valid serial numbers to function fully.
- Adware infections dominate all three industries. This could be because the adware modules are bundled together with free software, or was installed without user consent by a malicious/compromised website. In addition to displaying annoying advertisements, adware may change the browser homepage, change the default search engine, install browser plugins or toolbars, and transmit information about the user and their browsing habits to third parties without consent.
- Malware used in targeted cyber attacks would never show up in a pie chart of Top 20 malware for Y2015. This is because the success of targeted attacks depends on stealth, and the attackers go to great lengths to ensure their malware remains undetected by security scanners.

It is very interesting to observe the absence of ransomware in the top 20 malware list across all three industries. Ransomware may be using adware as their initial infection vector, and blocking the adware prevents further malware infections. Or, we may need to expand the malware list beyond top 20 to find ransomware infections cases.

Industrial Control Systems: A Weak Point for the Mining Industry

ICS in Mining Operations

Autonomous mining operations started in the early 1990s.[70] By the mid '90s equipment suppliers were offering buyers effective options for automating equipment. Technology such as GPS, remote sensing, wireless communications, and high-speed telecommunications made automation viable. Automation is suited to a number of key mining operations such as: production drilling and the real-time recognition of materials being drilled; automated materials handling using equipment like haul trucks, loaders, diggers, shovels, conveyors, and sizers; automated and accurate movement of equipment; monitoring of moving parts for maintenance and diagnostic intervention.

SCADA, distributed control system (DCS), programmable logic controller (PLC), remote terminal unit (RTU), improvised explosive devices (IED), actuators, and sensors are extensively used to automate processes at mine sites and mineral processing facilities. Examples of automation in mining are:[71]

- Autonomous haulage systems installed in haul trucks carry excavated ore rocks to the ore-crushing facilities. Accurate positioning is important for the remote operations of automated haul trucks. On board sensors such as RTK GNSS, odometers, inertial guidance, radar, laser, vision, sonar, etc. generate real-time maps of the mine environment (geometry and geology) around these trucks so they can be remotely operated.
- Command and Control (C2) systems control autonomous vehicles at the mine sites. C2 systems handle real-time telemetry data collection and processing for vehicle monitoring and control purposes. The C2 systems also monitor and report vehicle performance and maintenance data.
- Collision avoidance and geo-fencing systems are used in the mine sites to prevent collisions and accidents by autonomous vehicles.
- Remotely controlled (via line-of-sight or tele-operated) dozers and excavators are used to safely perform mining tasks in hazardous environments.
- Process Knowledge Systems (PKS) control different mining operations to help maximize production, reduce operating costs, and increase profits while improving safety, reducing risks, and minimizing resource requirements.
- Mining companies can automate the environmental, geotechnical, and vibration monitoring of slope movements, excavations, tunnels, and adjacent structures via sensors that record seismic activity and the result of groundwater investigations, and check the presence of poisonous gas. Unified monitoring systems aggregate real-time site condition data from the different on-site sensor networks.

- Real-time analysis of mineral material composition using laser-induced-breakdown spectroscopy (LIBS) technology installed above conveyor belts.
- Level, positioning, volume, pressure, and flow measurements using (wired or wireless) sonar, electromagnetic, radar, and vibration sensors.
- Automated systems are also used in underground longwall mining, for instance, in the remote assessment of rock-burst hazards in the longwall areas of mines, in electro-hydraulic control systems that support hydraulic cylinders and props in underground mining, and in pilot-controlled or fully automatic electrohydraulic servo valves.
- Motion sensors or accelerometers for automated drilling equipment using a variety of technologies such as vibration, inertial, seismic, and tilt sensing are also in use.
- Conveyor belt monitoring, control, and communications systems monitor and control conveyor belts several kilometers in length. Conveyor applications include coal/ore loaders, longwalls, crushers, and materials handling.

ICS environments face constant threats of cyber attacks. Potential ICS vulnerabilities affect various areas of operations. Any organization relying on Industrial Control Systems need to employ a comprehensive plan to mitigate any risks at the different level of operations. We will be exploring industrial controls security in a separate publication in greater detail.

Exposed ICS Devices on the Internet

Shodan is a search engine for internet-connected devices. The basic unit of data that Shodan gathers is the banner. The banner is textual information that describes a service on a device. For web servers this would be the headers that are returned, or for Telnet it would be the login screen.[72] As part of premium subscription, Shodan has an image search database at https://images.shodan.io/ to browse screenshots it has collected. Screenshots are collected from three different sources: Virtual Network Computing (VNC), Real Time Streaming Protocol (RTSP), and webcams.

We conducted searches through the Shodan image search database looking for examples of Human-Machine Interface (HMI) controlling ICS devices, where the HMIs were exposed on the internet. In this section we present some of the more interesting HMI screenshots that we collected. An important consideration to keep in mind: exposed HMI does not mean the system was compromised, but was poorly configured. Also, by virtue of being exposed on the internet, the system is vulnerable to compromise.[73]

Note: Internet-exposed HMIs were NOT accessed; all screenshots of internet-exposed HMIs were collected through Shodan.

Figure 19: Exposed HMI on the internet, collected through Shodan[74]

The screenshots show exposed HMIs for: carbon dioxide (CO2) sensors, water pumps, a milling machine, compost tank, water treatment plant, and a conveyor belt. Shodan is a publicly available search engine and anyone can access information about exposed ICS devices. Someone with nefarious intentions could easily abuse this information to attack exposed ICS devices. Shodan explicitly searches for exposed ICS devices by looking for ports and other metadata unique to ICS communications protocols.[75]

We also downloaded GeoIP data for all devices tagged as category:ics by Shodan and plotted them together with known mining locations in Google Earth. The goal was to visualize the volume of ICS devices exposed in the immediate vicinity of mines. In the following screenshots the yellow squares represent mines, the red pins represent exposed ICS devices, and the green squares represent major population centers like cities or large towns.

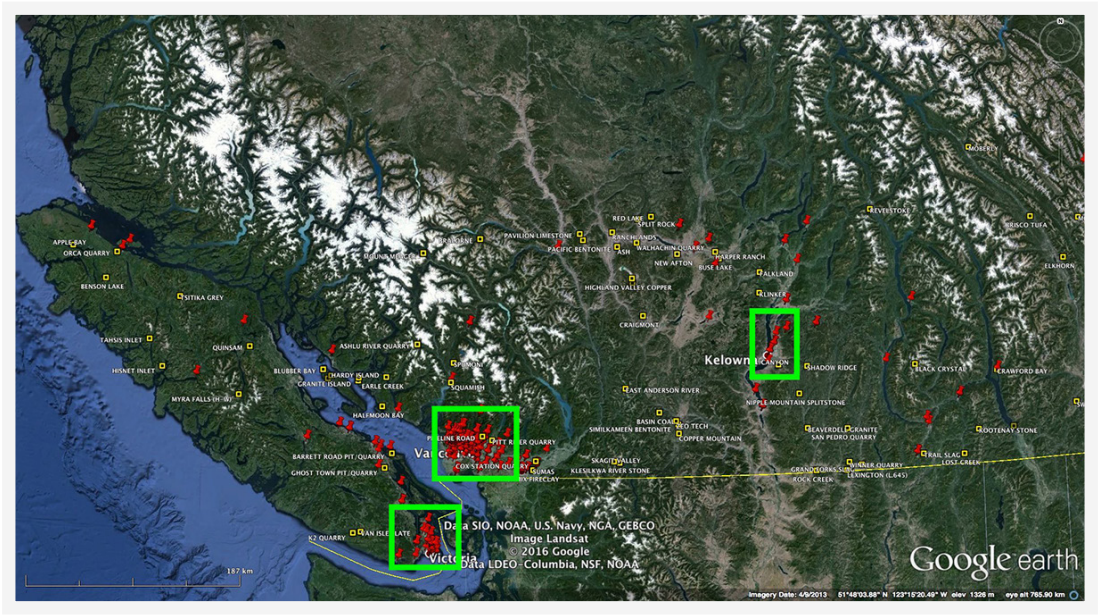


Figure 20: Exposed ICS devices and mining locations in Southern British Columbia, Canada[76]

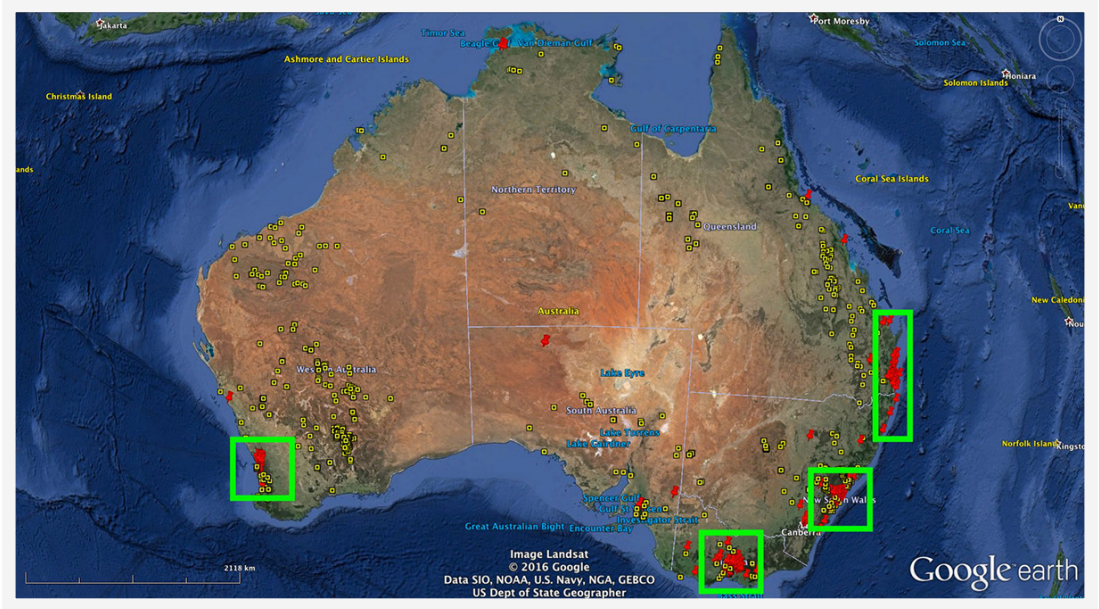


Figure 21: Exposed ICS devices and mining locations in Australia[77]

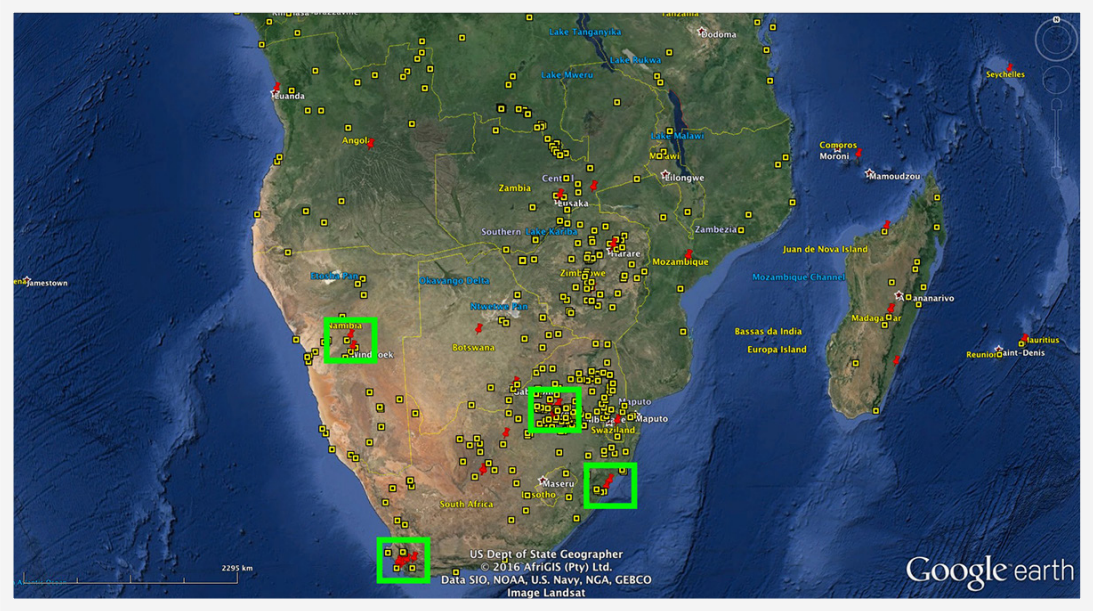


Figure 22: Exposed ICS devices and mining locations in outh Africa[78]

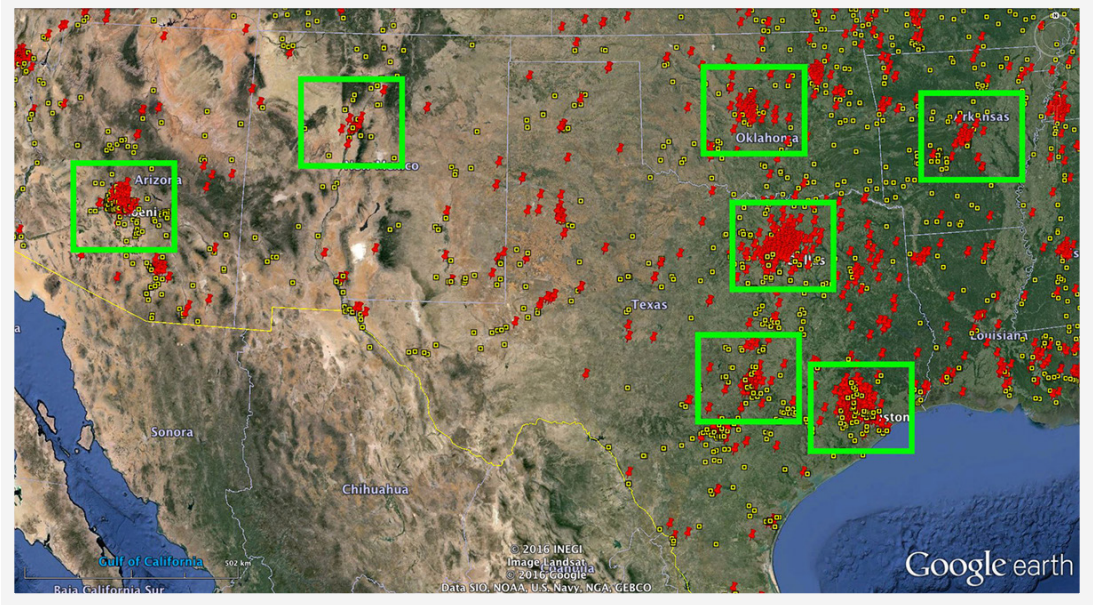


Figure 23: Exposed ICS devices and mining locations in AZ, NM, TX, OK, AR, and LA[79]

From the Google Earth map plots we make the following observations:

- The vast majority of the mines are situated in remote locations and have very few exposed ICS devices in their immediate vicinity.
- The majority of the exposed ICS devices are located in population centers such as large towns and cities.
- Modern mines are heavily automated and their ICS control centers are typically located in population centers hundreds or thousands of kilometers away from the mining sites. An HMI system physically located in the control center, which remotely controls ICS devices at the mine site, could be exposed on the internet, thus jeopardizing operations at the mine.
- The United States (US) plot is a bit difficult to discern because of the many population centers scattered all over the states. On closer inspection we discovered that the US data also follows the expected trend: majority of the mines are situated in remote locations and there are very few ICS devices exposed in the immediate vicinity of the mines.
- There is a high probability that there are non-ICS devices exposed at the mine sites. Those devices could be servers, desktops, mobile devices, etc. They can be targets for sensitive data theft, or can be used as an initial entry point and lateral pathway into the corporate network.

Defense and Protection in Mining Facilities

Protection of Facilities Dealing with Natural Resources

In today's competitive global market for commodities and manufactured goods, the reliance on natural resources for economic development and fluctuating geopolitical climates have all contributed to making industries targets for cyber espionage campaigns, and in extreme cases disruptive and destructive cyber attacks. These cyber espionage campaigns are geared towards ensuring interest groups have access to the latest technical knowledge and intelligence so they can maintain competitive advantage and thrive in a market-driven global economy. Cyber campaigns are also used for conducting carefully planned strategic or retaliatory cyber attacks against a nation's critical infrastructure.

Cyber attack and data breach prevention strategies should be considered an integral part of daily business operations. Ultimately, no defense is impregnable against determined adversaries. Cyber attacks and data breaches are inevitable. Having effective alert, containment, and mitigation processes are critical. The key principle of defense is to assume compromise and take countermeasures:

- Quickly identify and respond to ongoing security breaches
- Contain the security breach and stop the loss of sensitive data
- Preemptively prevent attacks by securing all exploitable avenues
- Apply lessons learned to further strengthen defenses and prevent repeat incidents

Top 5 Defensive Strategy Recommendations

Based on our research findings on the different types of cyber threats faced by the mining industry, we make recommendations for the implementation of five defensive strategies that we consider a mandatory minimum for mining companies:

1. **Network segmentation** – Segment the network into distinct security zones and implement layers of protection to isolate critical parts of the network. The Purdue Model[80] is an excellent guide for network segmentation where the corporate network requires access to the control/ICS network.

2. **Patch Management** – Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate and/or apply software patches, and minimize the window of opportunity for attackers.

3. **Access control** – This is a broad topic that covers all aspects of controlling access to networks, critical assets (e.g., data, resources, systems), devices or services (including physical and electronic access) according to the formal determination of who/what have needs and rights to access assets based on an approved classification.

4. **Intrusion detection** – the first order of business for targeted attacks is entry inside the organization's network; the second order of business for targeted attacks is leveraging the initial entry point to laterally move within the network and compromise other systems. All systems require some method of monitoring system activity and identifying potentially malicious events in the network. Without this ability to monitor a system, minor security issues will remain undetected until they become critical security incidents.

5. **Incident Planning and Response** – A comprehensive cyber incident response plan should include both proactive measures and reactive measures. Proactive measures are those that can help prevent incidents or better allow the organization to respond when one occurs, whereas reactive measures can help detect and manage an incident once it occurs.

Conclusion

In this paper we have explored aspects of the mining industry that are relevant to cyber espionage and attack campaigns in order to understand why the mining industry has become a target and what threat actors are trying to gain by attacking mining companies.

The modern mining company is a transnational corporation running highly coordinated production operations across multiple sites, in multiple countries with varied geopolitical climates, all the while responding to the demand and supply needs of a market-driven global economy. There are three main factors that explain why the mining industry is a viable and important target:

1. the increasing and continued importance of commodities as traded entities on international markets,

2. reliance on natural resources for economic development, and

3. the need for countries to benefit from their own mineral deposits

This makes the mining industry both a geopolitical and an economic target. Conversely, threat actors have learned to 1) leverage the significant role that mining commodities play in regional and global supply chains and for national economies, and 2) to exploit the weaknesses that mining companies are exposed to due to heavy reliance on integrated and automated systems.

Comparing attacks targeted at the mining industry with attacks on other industries - be they financial, retail or hospitality - the main difference we see is that attacks on the former are far more focused on espionage as opposed to immediate financial gains. The stolen intellectual property and other proprietary information, such as pricing data, of course, can result in long-term monetary gain. Foremost, however, they are used to influence and manipulate competitive dynamics in favor of interest groups, gain an advantage over the competition or even weaken an entire nation's economy. The motivation to get a hold of such information points towards what actors might have an interest in undertaking such actions.

In the course of the paper we have outlined specific threats and the geopolitical impact that IT security in the mining industry have to thoroughly understand when defending their ecosystem.

References

1. Michael J. Assante. (January 9, 2016). *SANS Industrial Control Systems Security Blog.* "Confirmation of a Coordinated Attack on the Ukrainian Power Grid." Last accessed on April 4, 2016, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

2. Kyle Wilhoit. (February 11, 2016). *TrendLabs Security Intelligence Blog.* "KillDisk and BlackEnergy Are Not Just Energy Sector Threats." Last accessed on April 4, 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.

3. Kyle Wilhoit. (February 11, 2016). *TrendLabs Security Intelligence Blog.* "KillDisk and BlackEnergy Are Not Just Energy Sector Threats." Last accessed on April 4, 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.

4. James Hampshire. (September 25, 2015). *Mining Journal.* "Cyber security in mining: not an underground risk." Last accessed on April 5, 2016, https://www.controlrisks.com/~/media/Public%20Site/Files/PDF/Cyber%20security%20in%20mining.pdf.

5. Trend Micro. (2016). *Trend Micro.* "Cybercrime and the Deep Web." Last accessed on May 9, 2016, http://www.trendmicro.com/vinfo/us/security/special-report/cybercrime-and-the-deep-web/global-cybercrime-map/.

6. James Hampshire. (September 25, 2015). *Mining Journal.* "Cyber security in mining: not an underground risk." Last accessed on April 5, 2016, https://www.controlrisks.com/~/media/Public%20Site/Files/PDF/Cyber%20security%20in%20mining.pdf.

7. Gartner. (2016). *Gartner.* "Operational Technology (OT)." Last accessed on May 9, 2016, http://www.gartner.com/it-glossary/operational-technology-ot/.

8. Alan Hindes. (2015). *Telstra.* "IT Security in the Mining, Oil & Gas Sector—Making IT part of your company's DNA." Last accessed on May 9, 2016, https://ovumindustrycongress.com/making-it-part-of-your-company-dna/.

9. NCCIC/ICS-CERT (April 19, 2016). *US Department of Homeland Security.* "NCCIC/ICS-CERT Year in Review FY2015." Last accessed on April 21, 2016, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2015_Final.pdf.

10. Jonathan Fildes. (February 15, 2011). *BBC News.* "Stuxnet virus targets and spread revealed." Last accessed on April 21, 2016, http://www.bbc.com/news/technology-12465688.

11. Liam O' Murchu. (2010). *Virus Bulletin Conference.* "An indepth look into Stuxtnet." Last accessed on April 21, 2016, https://www.virusbulletin.com/conference/vb2010/abstracts/indepth-look-stuxnet.

12. Kim Biddulph. (November 24, 2013). *Schools Prehistory and Archaeology.* "Why prehistory? Why not Stone Age, Bronze Age, Iron Age?" Last accessed on June 17, 2016, https://schoolsprehistory.files.wordpress.com/2013/11/timeline-page001.jpeg.

13. Wikimedia Foundation, Inc. (March 4, 2016). *Wikipedia.* "Three-age system." Last accessed on April 6, 2016, https://en.wikipedia.org/wiki/Three-age_system.

14. Homeland Security. (October 27, 2015). *Department of Homeland Security.* "Critical Infrastructure Sectors." Last accessed on April 6, 2016, https://www.dhs.gov/critical-infrastructure-sectors.

15. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition).* "Section 2.3. Figure 2.3-3." Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

16. http://strategicimages.com.au/images/system_open_pit_mine.jpg

17. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition)*. Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

18. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition)*. "Section 9.1. Figure 9.1-21." Englewood,

CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

19. Michael J. Assante. (January 9, 2016). *SANS Industrial Control Systems Security Blog.* "Confirmation of a Coordinated Attack on the Ukrainian Power Grid." Last accessed on April 4, 2016, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

20. Kyle Wilhoit. (February 11, 2016). *TrendLabs Security Intelligence Blog.* "KillDisk and BlackEnergy Are Not Just Energy Sector Threats." Last accessed on April 4, 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.

21. The USGS Water Science School. (August 7, 2015). *U.S. Geological Survey.* "Mining water use." Last accessed on April 13, 2016. http://water.usgs.gov/edu/wumi.html.

22. St. Augustine Gold and Copper, Ltd. (December 2013). *Developing the King-King Copper-Gold Project.* "Process & Plant." Last accessed on June 22, 2016, http://www.slideshare.net/CHFIR/st-augustine-gold-copper-ltd-november-2011.

23. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition).* Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

24. Mine Safety and Health Administration – MSHA. (Unknown). *United States Department of Labor.* "Injury Trends in Mining." Last accessed on April 15, 2016, http://arlweb.msha.gov/MSHAINFO/FactSheets/MSHAFCT2.htm.

25. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition).* Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

26. Hitachi Construction Machinery Channel. (February 18, 2015). *Youtube.* "Hitachi dump trucks Autonomous Haulage Solution." Last accessed April 15, 2016, https://www.youtube.com/watch?v=c9_Os6Ha-Gk.

27. Julian Parreira. (November 10, 2010). *UBC Engineering Physics Project Lab.* "Automation in the Mining Industry." Last accessed April 15, 2016, http://projectlab.engphys.ubc.ca/wp-content/uploads/MINE432-2010Nov10_Parreira.pdf.

28. BHP Billiton. (March 13, 2015). *Youtube.* "Integrated Remote Operations Center (IROC), Australia." Last accessed on April 15, 2016, https://www.youtube.com/watch?v=wXJjM9ppHtA.

29. Mark LaCour. (January 27, 2013). *Modalpoint.* "1-Oil & Gas Overview – modalpoint." Last accessed on April 18, 2016, https://www.youtube.com/watch?v=oADTmdTyrFU.

30. ABB. *ABB Mining Illustration.* "ABB Mining Illustration." Last accessed on April 15, 2015, https://library.e.abb.com/public/6029d76aadb0f2bac1257e030050cc43/abb-mining-illustration.pdf.

31. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition).* "Section 9.3. Table 9.3-1." Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

32. Mark LaCour. (January 27, 2013). *Modalpoint.* "1-Oil & Gas Overview – modalpoint." Last accessed on April 18, 2016, https://www.youtube.com/watch?v=oADTmdTyrFU.

33. Avata Supply Chain Management Experts & Oracle Partner. Last accessed on April 15, 2016, http://avata.com/wp-content/uploads/2015/05/Oil-and-Gas-AVATA-1024x536.jpg.

34. Brian Krebs. (February 14, 2014). *KrebsonSecurity.* "Target Hackers Broke in Via HVAC Company." Last accessed on April 18, 2016, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

35. Center for International Development. *The Atlas of Economic Complexity.* "What did X export in 2014?" Last accessed on April 15, 2016, http://atlas.cid.harvard.edu/explore/tree_map/export/ita/all/show/2014/.

36. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition).* "Section 2.2. Figure 2.2-7." Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

37. Numaan Huq. (September 22, 2015). *Trend Micro.* "Follow the Data: Dissecting Data Breaches and Debunking the Myths." Last accessed on May 6, 2016, https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf.

38. Dale Peterson. (January 21, 2013). *Digital Bond.* "S4X13: ICS Spear Phishing." Last accessed: May 11, 2016. http://www.digitalbond.com/blog/2013/01/21/s4x13-ics-spear-phishing/.

39. Margaret Rouse. (August 2015). *TechTarget.* "Watering hole attack." Last accessed: May 5, 2016. http://searchsecurity.techtarget.com/definition/watering-hole-attack.

40. Margaret Rouse. (May 2009). *TechTarget.* "Drive-by download." Last accessed: May 5, 2016. http://searchenterprisedesktop.techtarget.com/definition/drive-by-download.

41. Wikimedia Foundation, Inc. (April 27, 2016). *Wikipedia.* "Malvertising." Last accessed: May 5, 2016. https://en.wikipedia.org/wiki/Malvertising.

42. Brian Krebs. (February 14, 2014). *KrebsonSecurity.* "Target Hackers Broke in Via HVAC Company." Last accessed: April 18, 2016. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

43. Wikimedia Foundation, Inc. (April 15, 2016). *Wikipedia.* "Man-in-the-middle attack." Last accessed: May 18, 2016. https://en.wikipedia.org/wiki/Man-in-the-middle_attack.

44. Jose Pagliery. (February 19, 2015). *CNN Money.* "Lenovo slipped 'Superfish' malware into laptops." Last accessed: May 5, 2016. http://money.cnn.com/2015/02/19/technology/security/lenovo-superfish/.

45. Trend Micro. (July 11, 2013). *Trend Micro Research Paper.* "Lateral Movement: How Do Threat Actors Move Deeper Into Your Network?" Last accessed: May 5, 2016. http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf.

46. James Hampshire. (September 25, 2015). *Mining Journal.* "Cyber security in mining: not an underground risk." Last accessed on April 5, 2016, https://www.controlrisks.com/~/media/Public%20Site/Files/PDF/Cyber%20security%20in%20mining.pdf.

47. Jesse Riseborough. (April 19, 2010). *Bloomberg.* "Rio, BHP, Fortescue Hit by China Computer Hackers, ABC Reports." Last accessed on May 6, 2016, http://www.bloomberg.com/news/articles/2010-04-19/rio-tinto-bhp-billiton-fortescue-hit-by-china-computer-hackers-abc-says.

48. Staff Reporter. (May 12, 2010). *ABC News*. "Rio hacked at time of Hu arrest." Last accessed on May 6, 2016, http://www.abc.net.au/news/2010-04-19/rio-hacked-at-time-of-hu-arrest/403346.

49. Mark Bendeich, Ben Blanchard, and Daniel Magnowski. (February 16, 2011). *Mineweb.* "BHP's Kloppers' concerned over Chinese industrial espionage." Last accessed on May 6, 2016, http://www.mineweb.com/archive/bhps-kloppers-concerned-over-chinese-industrial-espionage/.

50. Cole Latimer. (April 15, 2011). *Australian Mining.* "Chinese hack Australian miners' email." Last accessed on May 6, 2016, https://australianmining.com.au/news/chinese-hack-australian-miners-emails/.

51. Michael Allan McCrae. (October 31, 2011). *Mining.com.* "Hackers target Canadian government's potash documents." Last accessed on May 6, 2016, http://www.mining.com/hackers-target-canadian-governments-potash-documents/.

52. Greg Weston. (November 29, 2011). *CBC News.* "Foreign hackers targeted Canadian firms." Last accessed on May 6, 2016, http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810.

53. Michael A. Riley and Sophia Pearson. (January 31, 2012). *Bloomberg Technology.* "China-Based Hackers Target Law Firms to Get Secret Deal Data." Last accessed on May 20, 2016, http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms.

54. Andrew Duffy. (February 28, 2012). *Australian Mining.* "Lynas website hacked as thousands protest." Last accessed on May 6, 2016, https://australianmining.com.au/news/lynas-website-hacked-as-thousands-protest/.

55. Patrick Villavicencio. (July 30, 2012). *InterAksyon.* "Sophisticated cyber attack uncovered vs mining firm in the Philippines. Last accessed on May 6, 2016, www.interaksyon.com/infotech/sophisticated-cyber-attack-uncovered-vs-mining-firm-in-the-philippines.

56. Stephanie Buckley. (January 11, 2013). *Quartz.* "Mega mining company Bumi gets hacked by someone posing as a Wikipedia researcher." Last accessed on May 6, 2016, http://qz.com/42795/mega-mining-company-bumi-gets-hacked-by-someone-posing-as-a-wikipedia-researcher/.

57. Eduard Kovacs. (May 7, 2013). *Softpedia.* "Website of AngloAmerican Mining Company Hacked by Anonymous for OpGreenRights." Last accessed on May 6, 2016, http://news.softpedia.com/news/Website-of-AngloAmerican-Mining-Company-Hacked-By-Anonymous-for-OpGreenRights-335092.shtml.

58. The Associated Press. (October 7, 2013). *CBC News.* "Canadian spies targeted Brazil's mines ministry: report." Last accessed on May 6, 2016, http://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975.

59. Chris Strohm, Dave Michaels, and Sonja Elmquist. (May 20, 2014). *Bloomberg.* "U.S. Companies Hacked by Chinese Didn't Tell Investors." Last accessed on May 6, 2016, http://www.bloomberg.com/news/articles/2014-05-21/u-s-companies-hacked-by-chinese-didn-t-tell-investors.

60. Henry Lazenby. (February 2, 2015). *Creamer Media's Mining Weekly.* "Nautilus Minerals falls victim to cyber scam, prepays $10m into wrong account." Last accessed on May 6, 2016, http://www.miningweekly.com/article/nautilus-minerals-the-victim-of-a-cyber-scam-prepays-10m-to-wrong-account-2015-02-02.

61. Rachelle Younglai. (June 23, 2015). *The Globe and Mail.* "Small Canadian gold firm suffers computer hack." Last accessed on May 6, 2016, http://www.theglobeandmail.com/report-on-business/industry-news/energy-and-resources/small-canadian-gold-firm-suffers-computer-hack/article25083416/.

62. Dissent. (June 22, 2015). *Databreaches.net.* "Russian hackers claim they still own Detour Gold, dump more data." Last accessed on May 6, 2016, http://www.databreaches.net/exclusive-russian-hackers-claim-they-still-own-detour-gold-dump-more-data/.

63. Staff Writer. (June 25, 2015). *ITNews.* "Aussie mining tech firm counts cost of Chinese hacking." Last accessed on May 6, 2016, http://www.itnews.com.au/news/aussie-mining-tech-firm-counts-cost-of-chinese-hacking-405753.

64. Nick Rummell. (November 16, 2015). *Courthouse News Service.* "Mining Company Says Law Firm Hacked It." Last accessed on May 6, 2016, http://www.courthousenews.com/2015/11/16/mining-company-says-law-firm-hacked-it.htm.

65. Cole Latimer. (February 3, 2016). *Australian Mining.* "NSW mining department hacked." Last accessed on May 6, 2016, https://australianmining.com.au/News/NSW-mining-department-hacked/.

66. Nick Tabakoff. (February 2, 2016). *The Daily Telegraph.* "Computer hackers targeted NSW Department of Industry, Resources and Energy mining secrets." Last accessed on May 6, 2016, http://www.dailytelegraph.com.au/news/nsw/computer-hackers-target-nsw-department-of-industry-resources-and-energy-mining-secrets/news-story/8a567dfccab45543abc70596427097a4.

67. Kyle Wilhoit. (February 11, 2016). *TrendLabs Security Intelligence Blog.* "KillDisk and BlackEnergy Are Not Just Energy Sector Threats." Last accessed on April 4, 2016, http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.

68. Dissent Doe. (April 27, 2016). *The Daily Dot.* "Hackers have breached Goldcorp, a Canadian gold-mining firm." Last accessed on May 6, 2016, http://www.dailydot.com/politics/goldcorp-hack-data-dump/.

69. Wikimedia Foundation, Inc. (April 15, 2016). *Wikipedia.* "OpenCandy." Last accessed on May 9, 2016, https://en.wikipedia.org/wiki/OpenCandy.

70. Peter Darling. (February 25, 2011). *SME Mining Engineering Handbook (3rd Edition).* Englewood, CO: Society for Mining, Metallurgy, and Exploration, 2011. Print.

71. Mining-technology.com. (2016). *Mining-technology.com.* "Control and Automation Systems Image Gallery." Last accessed on April 28, 2016.

72. John Matherly. (February 2016). *Leanpub.* "Complete Guide to Shodan." Last accessed on June 17, 2016, https://leanpub.com/shodan.

73. Note: Internet-exposed HMIs were NOT accessed; all screenshots of internet-exposed HMIs were collected through Shodan.

74. Note: Internet exposed HMIs were NOT accessed; all screenshots of internet exposed HMIs were collected through Shodan.

75. John Matherly. (2016). *Shodan.* "Industrial Control Systems." Last accessed on April 26, 2016, https://www.shodan.io/explore/category/industrial-control-systems.

76. Geo data source: http://www.empr.gov.bc.ca/Mining/Geoscience/MapPlace/thematicmaps/Pages/GoogleEarth.aspx

77. Geo data source: http://www.australianminesatlas.gov.au/mapping/downloads.html

78. Geo data source: http://mrdata.usgs.gov/catalog/cite-view.php?cite=853

79. Geo data source: http://mrdata.usgs.gov/catalog/cite-view.php?cite=17

80. Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A. Johnston, Sabina Piyevsky, Mark Schillace, Gregory Wilcox, Dan Zaniewski, and Steve Zuponcic. (September 9, 2011). Cisco and Rockwell Automation. "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. Last accessed on May 3, 2016, http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com