Australian Mining Companies and Cybercriminals Digging for the Gold

ke-la.com/australian-mining-companies-and-cybercriminals-digging-for-the-gold/

March 7, 2021

While Australian mining companies are busy extracting natural minerals from their lands, cybercriminals are busy extracting sensitive information from mining companies' infrastructures and employees. For more than a century, Australia's economy has significantly benefited from the mining industry, with a particularly strong influence in the last decade. Employing over 260,000 people and being valued at more than 200 billion AUD, the mining industry is the primary contributor to the Australian economy, and in parallel under the spotlight for many cybercriminals. As growth of this industry continues to be evident, cybercriminals may be seen profiting more and more from the mining companies' sensitive information. This industry, once relying almost solely on human work, has now evolved with the digital age to make use of technological support for day-to-day operations – naturally creating more opportunities for cybercriminals to exploit.

Australia's mining industry comprises numerous companies, however for this research, we've decided to look into the top 5 companies to identify the interest of cybercriminals in this industry. The research consists of an overview of numerous cyber threats that we have identified, which if exploited correctly could cause significant risk to this industry. The highlights include:

- KELA identified more than **91,000 leaked employee-credentials pertaining to the top 5 Australian mining companies**, leaked through third party breaches over the last few years.
- KELA discovered **multiple compromised accounts** related to employees in the Australian mining industry, which might **provide access to sensitive corporate services.**
- KELA observed numerous **network vulnerabilities in the Internet-facing infrastructure** of the top 5 companies in the mining industry.
- KELA detected a compromised **network access listed for sale. Upon research, KELA identified that the victim is a company** that provides services and stores sensitive data belonging to companies in the mining and energy sector in Australia.

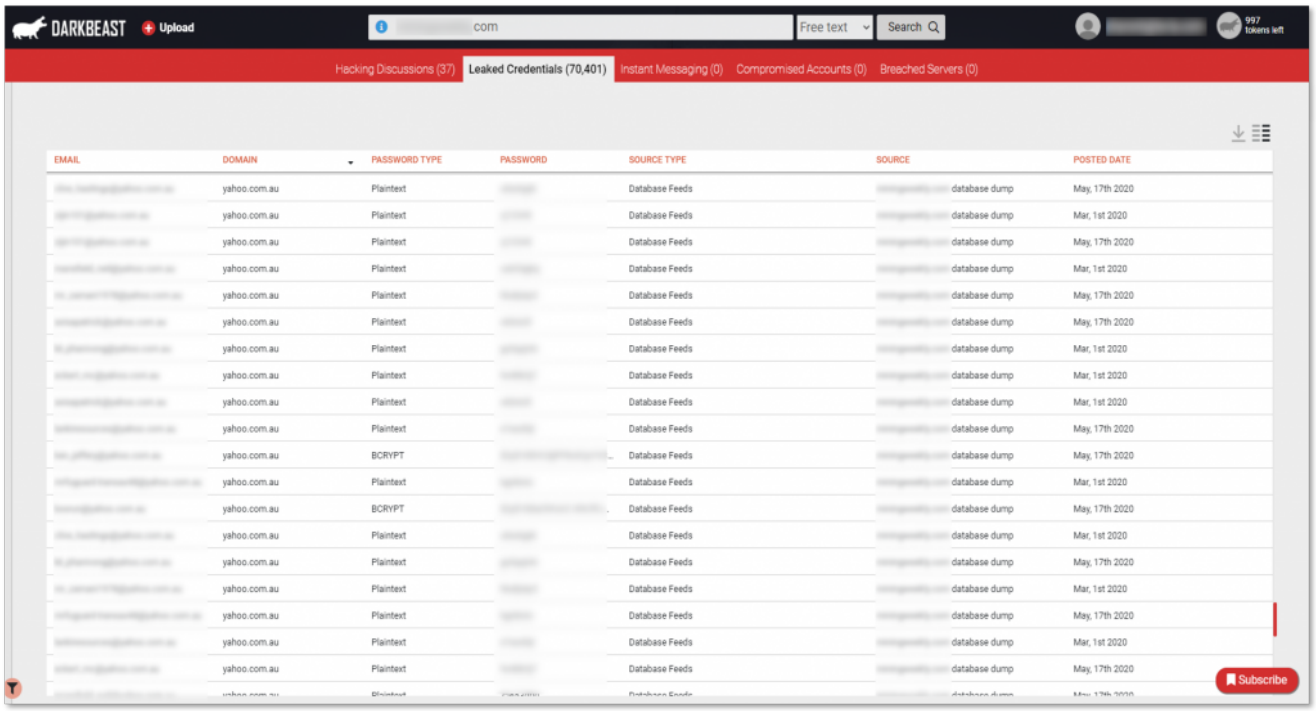
Practicing Safety Across the Board: Miners Must Maintain Both Physical and Cyber Safety

Mining employees are busy in the underground, but what they may not know is that cybercriminals are just as busy in their underground cybercrime ecosystem. Diving into our sources, **we've identified more than 91,000 leaked employee-credentials pertaining to**

the top 5 Australian mining companies. These exposed credentials are email addresses or email:password pairs belonging to mining companies' employees, extracted from various breached databases constantly traded and circulating in the underground. These databases mostly include private and corporate email addresses and associated passwords, including plaintext ones. Looking further into this data, we found that these credentials were exposed in well-known breaches, such as NitroPDF, Canva, and several others.

The threats on mining companies' employees stemmed mostly from third-party breaches on victims unrelated to the mining industry, however we also identified a **targeted attack where cybercriminals succeeded in obtaining users' credentials of a website related to the mining industry**. KELA observed a breached database that was offered on the now unavailable Cit0day shop. Cit0Day.in – a private underground service advertised on hacking forums to other cybercriminals – operated as a database-as-a-service market by collecting hacked databases and then providing access to usernames, email addresses, and even cleartext passwords to other hackers for daily or monthly fees. Due to the automation of this type of market, Cit0day essentially offered actors to trade in much higher volumes but has been taken down by authorities in late 2020.

However, with KELA's caching capabilities, we were able to **identify more than 36,000 user credentials** (including email addresses with plaintext passwords) that have been **leaked in a breach of a South African website that provides daily news and updates about mining around the world**. While looking into the domains of the email addresses leaked, we were able to discover that nearly 250 corporate email addresses of Australian individuals were leaked, with the majority of those being corporate email addresses for individuals in the mining industry in Australia.



Exposed credentials (redacted) that were sold as part of a breached database belonging to a South African-based site offering daily news and updates about mining activities worldwide.

One of the recent breaches where we identified compromised credentials of mining companies' employees was in the Capital Economics breach discovered by KELA. The exposed data here contained data not only of Australian mining companies' employees but also data of users all over the world. Due to the fact that the victim – Capital Economics – is one of the leading independent economic research companies in the world, many of the records leaked included corporate email addresses, which could be of great value to cybercriminals looking to target corporate victims.

What Value is Seen in Leaked Credentials of Mining Companies' Employees?

Australia's mining industry has seen a vast shift towards automation over the last few years. The systems and processes, controlled by employees in the Australian mining industry, are vulnerable and valuable for cybercriminals looking for their next target. Leaked credentials lay out a plethora of opportunities for cybercriminals that get their hands on them.

Cybercriminals who obtain this data could use it to **perform actions such as phishing schemes in order to lure further victims into downloading malicious links to plant malware**. By doing so cybercriminals can eventually infect systems with ransomware that could disrupt daily mining processes. In a *worst-case-scenario*, **these cybercriminals may use this opportunity to lock systems and prevent mining companies from continuing operations until a ransom is paid**. As learned from analyzing past ransomware attacks and

the ransom amounts demanded, we've observed that ransomware groups generally price their ransom demands based on company revenue. That being said, the ransom that could be demanded from these companies will likely be in the millions, if not more. Other attacks that could be enabled through leaked credentials could be **business email compromises, social engineering attacks, and other internal network exploitations.**

What is certain is that with leaked credentials circulating in the Dark Net, **Australian mining companies are actively at risk.** The exposed sensitive data provides cybercriminals with opportunities to cause disruption of activities for long periods of time on Australia's most profitable critical infrastructure.

Access to Corporate Services Through Compromised Accounts

While leaked credentials pose a significant threat to organizations when utilized correctly by the obtainers, compromised accounts are both easy to purchase and instantly ready to use by its buyers. KELA discovered multiple compromised accounts related to employees in the Australian mining industry, essentially providing buyers with access to portals behind sensitive corporate domains and subdomains.

Compromised accounts refer to any credentials, cookie sessions and additional technical fingerprints that are available for sale in various automated shops, such as Genesis, which is automatically monitored by KELA's technologies. These accounts are stolen from victims' computers generally via infections by banking trojans or other stealers. Such accounts can grant access to tools and software used in a targeted environment, such as RDP, VPN solutions, and more. They could be leveraged by a sophisticated actor to gain initial network access to the relevant corporate's network. These markets grant threat actors with access to desired services with the click of a button and at a price of a couple of dollars per bot.

In our research, we identified that accounts for security token services were compromised for three of the top 5 companies.[1] These services instantly **provide cybercriminals with access to the companies' corporate environments, enabling them to manipulate security mechanisms within them**. Within these compromised accounts, we also identified that accounts to Active Directory Services were compromised – accounts that can be used to access systems and applications located across organizational boundaries.[2] Upon further research, we also detected a compromised account that likely leads to the intranet of one of the companies.[3] By purchasing this account, the attacker is instantly **granted access to the internal computer network of the organization and gains visibility into internally shared information by the organization**.

Last, we identified an instance of an infected computer that contains details to access a mining company's contractor website. For the same company, the portal used to securely transfer files to clients could be compromised through the bots available for purchase.

The examples of compromised accounts listed above can easily and quickly provide attackers with the initial access they need in order to enter the corporate network of these mining companies.

Until now, the examples laid out in this research highlighted threats that are targeting the employees of the industry through leaked credentials or compromised accounts, however, we have also identified threats targeting the companies' networks and supply chains that pose a significant risk to their attack surface.

Mapping Out Mining Companies' Network Vulnerabilities

KELA **identified multiple network vulnerabilities – weaknesses in the Internet-facing infrastructures – pertaining to the top 5 companies of the Australian mining industry**. Among these, KELA identified multiple accessible developer-related environments, that were easily detectable by the presence of indicative keywords in the hostnames. When analyzing these hostnames, we found that they require corporate credentials to sign in. By leveraging the tens of thousands of credentials that are publicly circulating, an attacker may be able to access these internal resources by testing out the different corporate email addresses and passwords that are exposed.

Last, KELA identified that some of the companies researched are actively operating with technologies that have known flaws exposed to the public internet. For example, one company was found to be using version 2.0 of ASP.NET (an open-source web framework for .NET) for its contractor system which can be exploited through multiple publicly disclosed CVEs.

While each threat on its own may seem minimal, the combination of available sensitive resources proves to pose a real-time risk to the organizations. In this instance, we were able to find both an internal resource that's publicly exposed to the internet (i.e. the sensitive hostname) and the opportunity to gain access to said resources (i.e. the 91,000+ leaked credentials related to these organizations or multiple compromised accounts available for sale on automated botnet markets).

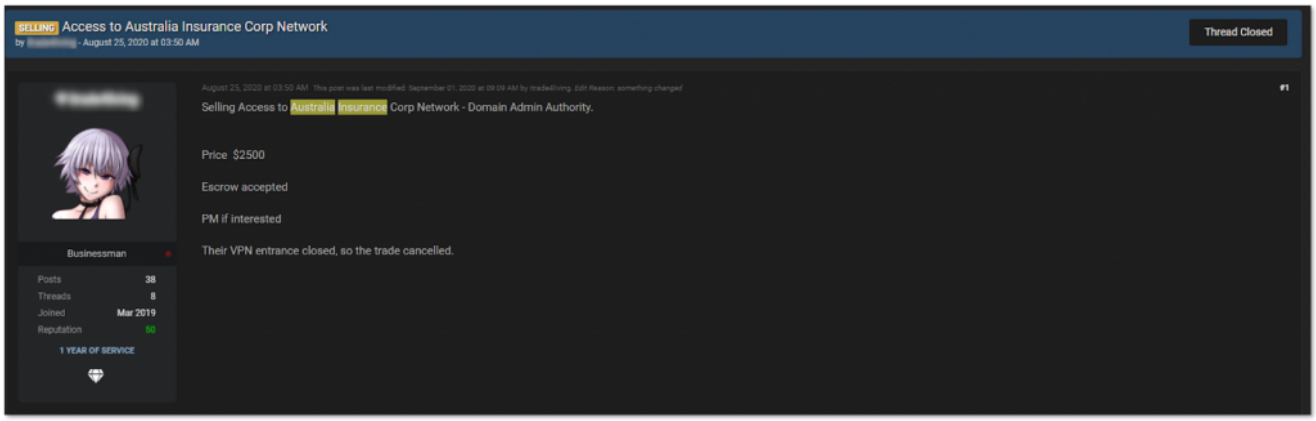
During our research, we have also identified possible supply chain threats that could affect these and other companies in the Australian mining industry.

Attack Surface Threats Through the Mining Industry Supply Chain

As ransomware attacks grow, we've been seeing an increasing trend of ransomware-as-a-service, with ransomware operators working together with affiliates and initial access brokers to help simplify the infection process. While looking into initial network access for sale related

to mining companies, we were able to identify compromised access to an Australian insurance company, which offers services tailored to the Australian mining and energy sector.

The victim whose services consist of protecting businesses in the mining industry from cyber risks was targeted by network exploitation. The threat actor posted this access specifying that he had Citrix access with domain admin privileges for sale and priced it at $2,500. This showcases a typical example of how a buyer can purchase this access to perform lateral movement in order to compromise other areas of the network and potentially gain sensitive information related to clients – in this case mining companies using the victim's insurance services.



Listing of compromised network access for sale belonging to an Australian insurance company that offers services tailored to the mining and energy sector.

Summing Up the Exposure of Australian Mining Companies in the Dark Net

As presented above Australian mining companies play a critical role in supporting their country's economy. What mining companies and their employees must understand is that this critical infrastructure is just as important and appealing in cybercriminals' eyes. With the numerous threat types that we observed in the Dark Net, mining companies and their employees are facing a serious risk that continues to grow as the industry undergoes a digitization process.

Throughout this research we've presented numerous threats posed to the employees, networks, and supply chains of companies in the Australian mining industry. Each threat is obviously critical on its own, however when combining several of them, the overall threat instantly becomes more severe.

During this research we've taken a look at the top 5 companies, however the industry as mentioned earlier is the greatest influencer on the Australian economy. The mining industry must be actively mitigating the ongoing threats that are targeting their environment. Based on the threats listed throughout this research this could mean:

1. Investing in prioritization of vulnerability patching.

2. Implementing the necessary monitoring tools and systems, in order to be made aware of any threats that emerge in real time.

3. Educating employees not only about physical safety – which is something enforced and heavily practiced by mining companies – however also about cyber safety, including how their data should be safely used online, and how to properly identify suspicious activity

By combining ongoing monitoring with the necessary education and mitigation activities, the companies within this highly valuable industry can be sure to be one step ahead of attackers in order to mitigate threats and thwarts attempts of cyber-attacks against them.

Interested in learning more about how mining companies can proactively monitor their environment and better protect themselves? Contact KELA here.

---

[1] KELA was able to identify that these are sensitive token services due to the links that were provided in the format of ‘sts.domain’. See here for more details: https://en.wikipedia.org/wiki/Security_token_service

[2] Links identified were in the format of ‘adfs.domain’

[3] Links identified were in the format of ‘access.domain’