

Threat digest: Emerging cyber threats in the manufacturing and mining sectors

Forensic Technology Solutions

May 2021



Contents

Background	1
Introduction	1
Attacker tactics, techniques and procedures	2
Motivation and attack vectors	4
Ransomware	5
Potential impact	6
Conclusion	6
Annexure A	7



Background

We have compiled this document from research that was performed on organisations in the mining and manufacturing industries (the sectors) and trends noted by us. The document focuses on emerging cyber threats affecting these sectors, with a focus on South African and other Africa-based organisations. The output of our research is provided to you at no cost and is aimed at providing a value-added service as to how the potential losses of data can be limited by heightened awareness on the part of business.

This document is provided to you for your internal use and is not intended to, nor may it be relied upon by any other party (third party). The document may not, in whole or in part, be copied, quoted, referred to or disclosed to any other party without prior written consent. PwC does not accept any liability towards you nor towards any third party to whom the document is disclosed or disseminated whether in whole or in part.

Introduction

Everyday operations in a modern mining setup consists of drilling, controlled detonation, excavation, loading, haulage, crushing and mineral processing whilst manufacturing in South Africa is dominated by industries such as textiles, agro-processing, automotive, chemicals, information and communication technology, electronics, metals, clothing and footwear.

Today, the uptake of smart systems that use advanced technologies such as machine learning and the Internet of Things (IoT) have added an additional level of complexity. Termed ‘Smart Manufacturing/Smart Mining’, South African based industry leaders recognise that the terms encompass everything from Artificial Intelligence (AI) to robotics and cybersecurity¹. A multi-nation PwC survey on 4IR adoption found that:



87% of business leaders of industrial products companies agreed that 4IR technologies give companies a competitive advantage, and 79% agreed it creates new revenue streams².

Though there are obvious benefits in the convergence of these advanced systems and the Operational Technology (OT) that makes up the backbone of the sectors, it is also important to highlight that the reliance on such inter-connected and internet-dependent systems is not without its own risks. A 2019 survey by Fortinet found that 74% of OT-reliant businesses had experienced significant IT security breaches in the preceding 12 months³. These incidents had a host of adverse impacts on each organisation. These include, but are not limited to, loss in revenue, compromise of business-critical data, and damage to brand reputation.

The technologies most targeted by attackers within the sectors are Industrial Control Systems (ICS). ICS are embedded computer devices that are responsible for a myriad of automated process controls in industries (e.g., measuring instruments, packaging machinery and all other

¹ <https://www.itweb.co.za/content/Pero3MZxD9nvQb6m>

² <https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-industrial-products-insights-q3-2020.pdf>

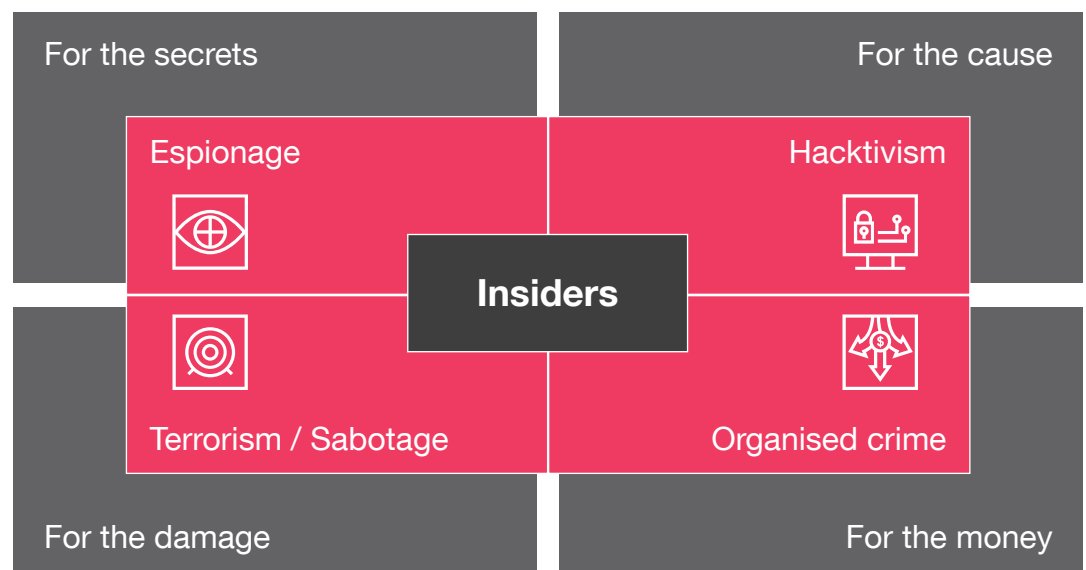
³ <https://www.csoonline.com/article/3392579/key-findings-on-the-state-of-operational-technology-and-cybersecurity.html>

components of an assembly line that make parts of any production process). ICS devices are generally lesser known than enterprise information technology (IT) devices such as laptops, desktops and smartphones as they are typically unique to industries and utilised for specialised systems or operations.

The mining sector has been quick to adopt autonomous vehicles, remotely controlled excavators, Wi-Fi based site location tracking and smart adaptive ventilation systems whilst the manufacturing sector uses smart technologies for optimisation, quality checks and widespread systems controls. Cyber risks to these devices generally remain unknown and therefore unaddressed by organisations.

The COVID-19 pandemic served to exacerbate the problem; in the first six months of 2020 the manufacturing industry had seen a dramatic increase in intrusion activity with at least an 11% increase in network attacks compared to the same period in 2019⁴. In FY20 alone an estimated 70 cybersecurity incidents targeted the Australian mining and resources sector⁵. This escalation was not only in terms of sophistication but also in terms of the types of threat actors entering the space of attacking the sectors. In the rest of this document, we will examine and highlight the different threats to ICS technologies and the profiles of the actors perpetrating these attacks. We will also highlight notable incidents to help demonstrate the complexity and subsequent impact of ICS attacks.

Attacker tactics, techniques and procedures



PwC's global Threat Intelligence practice recognises four types of motivations driving attackers, namely espionage, hacktivism, terrorism/sabotage and organised crime.

Depending on the motivation there are a range of different tactics, techniques and procedures (TTPs) used by each attacker. This not only determines the impact of each attack but also the means by which organisations get targeted and subsequently compromised. Generally, we note that insiders can be part of any threat group.

Organisations who are mindful that a security breach in the sectors can take several different forms and originate from several different places are in a better position to imagine ways of implementing the correct defences. To begin with, we highlight notable breaches within the sector that PwC has responded to.

⁴ <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf>

⁵ <https://www.homeaffairs.gov.au/cybersecurity-subsite/files/cyber-security-strategy-2020.pdf>

PwC response to manufacturing and mining industry attacks

In February 2019, PwC South Africa responded to a ransomware attack where the operations of a major food manufacturing business were affected by a previously unknown strain of malware. This is commonly referred to as a 'zero day exploit' by security practitioners. The ransomware affected some of the foreign operations of the organisation and then promulgated across the network affecting at least three countries. This resulted in key corporate and financial systems being offline for over a week until the network had been rebuilt and cleaned of the malware. However, in the initial stages of the attack, PwC was able to separate the OT networks and corporate networks — which allowed manufacturing operations to continue. The attack could have had a far more devastating effect on the organisation had this not been done.

At the tail end of 2019, a joint response was launched by PwC's German, Belgian, UK, Canada and US incident response teams. A manufacturer in the aerospace sector had experienced an incident that disrupted operations across regions. In this instance, IT systems which were within the OT/ICS networks were freely allowed to access the internet and email. Further to this, in order to accommodate the needs of different partners, the organisation had provided data to them using **outdated communications protocols** that were retrofitted to use TCP/IP networks. Effectively, IT, OT, ICS and ERP systems were compromised and brought down by attackers.

PwC South Africa responded to attacks on two major mining companies in 2019. In both cases, the attacker had exploited weak security measures on both the organisations' networks following a migration of their email systems to cloud-based mailing platforms. Once on the network, the attacker was able to alter legitimate invoices and impersonate individuals involved in the settlement of payments in an attempt to get funds transferred from the business to an account they controlled. PwC was able to determine the list of compromised accounts and assist both businesses in implementing stronger security on their newly implemented cloud-hosted platforms.

Other notable attacks in the sector

In July 2018 Level One Robotics and Controls Inc, a vendor specialising in automation solutions for several companies, suffered an attack where sensitive data of over 100 companies in the manufacturing industry was stolen from its servers. Notable from this incident is how a single **supply chain breach** resulted in the loss of critical business data and intellectual property of over 100 companies, the consequences of which cannot be easily quantified⁶.

In 2019, the MIT Technology Review published an alert on a new piece of malware called **Triton**⁷. This malware was designed to disable safety systems which are built to prevent catastrophic industrial accidents. Initially discovered in an attack launched on a Saudi Arabian based power station, the malware has since been adopted and altered by other hackers to launch attacks all over the world.


The Industry Destroyer Attack

Industroyer⁸ is a modularised piece of malware that is designed to disrupt various types of critical ICS infrastructure and processes. In 2016 it was used to launch an attack against the Ukrainian power grid that cut energy supplies to much of the city of Kiev. This was an important reminder that while the target may be businesses in the sector, the consequences can potentially affect entire populations

⁶ <https://www.upguard.com/breaches/short-circuit-how-a-robotics-vendor-exposed-confidential-data-for-major-manufacturing-companies>

⁷ <https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/>

⁸ <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>



The attacks mentioned above are not isolated; 2020 has also seen its fair share of attacks. Some matters include the following:

- Tower Semiconductor, a semiconductor chip manufacturer from Israel, suffered a cyberattack that halted some of its manufacturing operations.
- In December 2020, Rio Tinto was named as one of the organisations affected by the widespread SolarWinds supply chain attack. As a result, the hackers had access to privileged accounts and widespread monitoring of all affected organisations⁹.
- In June 2020, the Australian beverage maker, Lion, also suffered a cyberattack which affected its internal systems and disrupted its manufacturing process.
- In North America, the Tesla factory in Nevada was targeted in a serious cybersecurity attack, where a Russian hacker attempted to recruit an employee to introduce malware onto their systems. The employee disclosed this to the company and, with help of law enforcement, was able to thwart the attack.

It is important to note that local regulator stipulations and disclosure laws play a major role in the number of incidents that are reported and, as a by-product, known to the public. Laws tailored to cater for these areas are maturing.

Motivation and attack vectors

Espionage has been growing as one of the driving forces behind cyberattacks in the manufacturing industry¹¹. Cybercriminals gain access to the networks of businesses in the sectors with the aim of stealing trade secrets and intellectual property. However, our research revealed that although in 2020 there was a notable uptick of espionage-motivated incidents as compared to the same period last year, the majority of the attacks have predominantly been financially motivated (63-95%)¹². The sophistication of attacks varies widely depending mostly on existing security controls. Attackers elect to exploit common and publicly accessible technologies then propagate across the network once an initial foothold has been gained. We have also drawn on our experience conducting cybersecurity assessments and penetration tests from across our global network to identify the ten most common security vulnerabilities in OT/ICS networks. These have been listed in Annexure A. Generally, the most common attacks noted by PwC's incident response teams over 2019 and 2020 were:

- Infiltration of insecure email platforms following cloud adoption.
- Phishing.
- Insecure remote access platforms (VPN, remote login etc).

⁹ <https://www.abc.net.au/news/science/2020-12-23/hack-russia-nsw-health-rio-tinto-serco-solarwinds-cybersecurity/13009348>

¹⁰ <https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=ZA#:~:text=27%20Jan%202020-,In%20terms%20of%20section%2022%20of%20POPIA%2C%20where%20there%20are,such%20data%20subject%20cannot%20be>

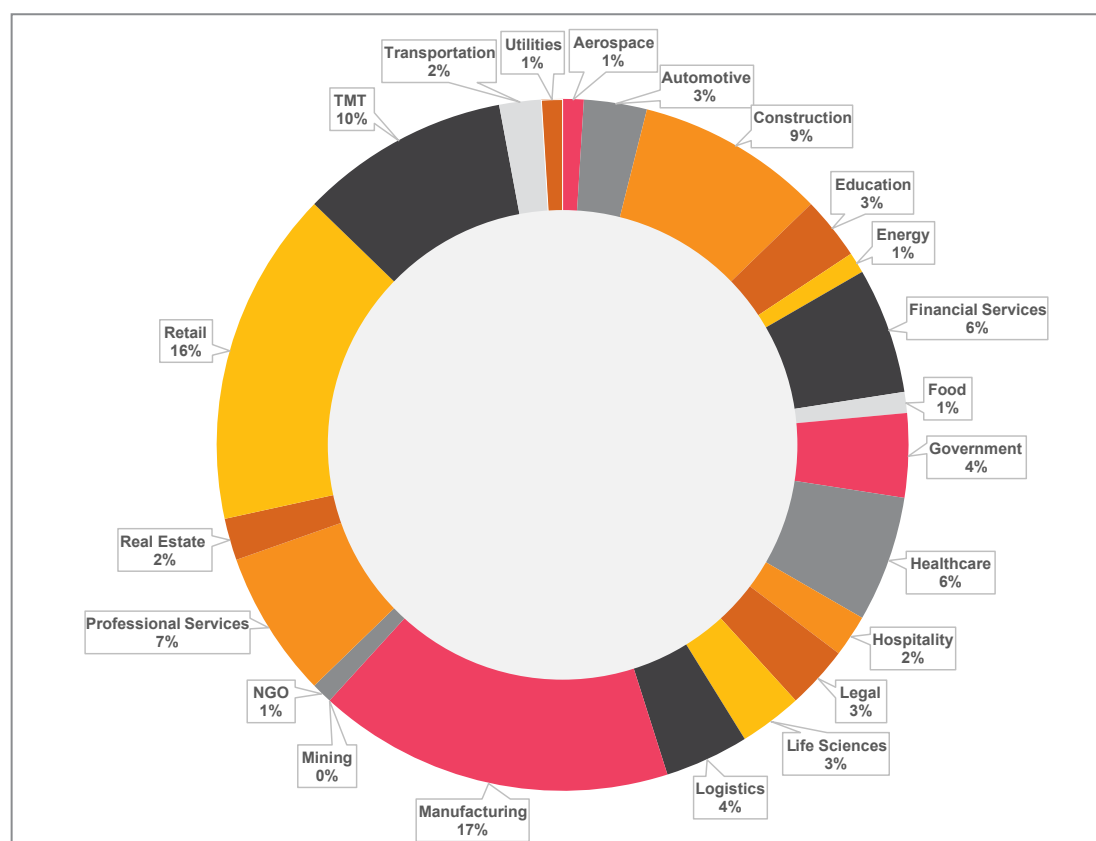
¹¹ <https://www.hornecyber.com/newsroom/news-releases/why-are-cybercriminals-targeting-the-manufacturing-industry/>

¹² <https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/>

Ransomware

Once attackers have a foothold in an organisation, the tools and tactics used by them are usually designed to monetise their attacks by the simplest means possible. Currently, the most common tool in the hacker's arsenal is ransomware. Ransomware is a type of malicious software (malware) that holds your systems or data to ransom. The current trend is for attackers to encrypt data and to displays messages demanding a ransom be paid to the attacker before they can allow access to the data.

Figure 1: Ransomware attacks per industry, 2020




At a global level, PwC tracked ransomware attacks across various industries for 2020. The graph above represents the proportion of data advertised on 'leak' sites due to ransomware attacks. Of these, 17% affected the manufacturing sector but no data appears to have been advertised from the mining sector. Based on our experience, the nature of attacks in the mining sector have largely been focused on electronic payment fraud, industrial espionage and sabotage. Given the nature of ransomware attacks, organisations in the mining sector should not ignore the threat posed by these attacks.

Data available for the African continent is limited, however we believe this to be a representation of how susceptible African organisations in the sectors are to these types of attacks. The Verizon 2020 Data Breach Investigations Report¹³ notes that attacks on the sectors made up 11% of the cases they investigated globally in 2019, whilst Kivu noted that 18% of the cases they investigated globally were in the manufacturing sector. Kivu further notes that despite this rather modest percentage, businesses in the manufacturing industry represented 62% of the ransoms that were paid in 2019 with over \$6.9M paid to attackers¹⁴.

¹³ <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>

¹⁴ https://kivuconsulting.com/wp-content/uploads/2020/06/Kivu-Threat-Intel_2019-Paid-Ransomware-Report_May2020.pdf



There are several different types of ransomware, each controlled by different hacker groups and built to propagate across networks and exploit targets in various ways. Some of the variants commonly known to have affected businesses in the sectors in 2020 include, but are not limited to:

- **Conti**, a ransomware variant that targeted the Volkswagen Group¹⁵.
- **Maze**, a threat group that claims to have extracted data from and encrypted the systems of the semiconductor manufacturer SK Hynix¹⁶, electronics giant LG and steel sheet manufacturer Hoa Sen Group¹⁷.
- **RansomEXX**, the variant that affected the technology manufacturer Konica Minolta¹⁸.
- **DopplePaymer**, the ransomware group that targeted Amphastar Pharmaceuticals, a manufacturer of specialist inhalation products.

Potential impact

A common misconception is that cyberattacks are exclusively an IT problem. However, the reality is that the problem is becoming more pronounced as technology is being embedded in operational processes. Apart from the loss of data and intellectual property, the risk to the core business operations becomes heightened and could lead to severe disruption through cyberattacks. In addition, safety, health, environment and quality (SHEQ) systems could also be impacted as there is a growing dependence on smart devices to support these processes and functions.

In all, the combination of emerging technologies, immature understanding of the risks these present to organisations, high dependence for operations and, in many organisations among the sectors, insufficient spending on cybersecurity, present a fertile ground for threat actors to launch attacks.

Another key area which is often overlooked by clients we have dealt with is incident response processes and the ability to deal with a large-scale cyberattack. PwC has dealt with at least three large clients who had to completely disconnect from the Internet for extended periods while crisis and remediation efforts were underway. In one instance, a significant portion of the client's server estate was damaged during a cyberattack. The recovery efforts had to be carried out over two months with systems being gradually phased into operation over this time.

Conclusion

Organisations in the manufacturing and mining sectors face a myriad of different cyber threats. Recent experiences with clients in these sectors lead us to believe that organisations in this space have not been paying enough attention to these threats. They are also not prioritising the implementation of the appropriate mitigation strategies, whilst threat actors are starting to take an interest in organisations operating in this space.

Due to the increasing level of technology adoption, the consequences of attacks on organisations in the sectors can be widespread and potentially devastating. It is therefore important for businesses to understand key risk areas, attack vectors and vulnerabilities to ensure that they employ the correct controls to improve security and protect their assets.

¹⁵ <https://www.securitynewspaper.com/2020/08/27/volkswagen-group-infected-by-conti-ransomware/>

¹⁶ <https://www.donga.com/en/article/all/20200910/2176572/1/SK-Hynix-LG-Electronics-fall-victim-to-ransomware-attacks>

¹⁷ <https://securityaffairs.co/wordpress/107379/cyber-crime/hoa-sen-group-maze-ransomware.html>

¹⁸ <https://www.bleepingcomputer.com/news/security/business-technology-giant-konica-minolta-hit-by-new-ransomware/>

Annexure A

Top 10 vulnerabilities to manufacturing OT networks

PwC has carried out extensive research in the field of OT networks. Much of the research we carry out in this area is done to understand the different types of threats and vulnerabilities facing OT and ICS in use within the sectors. We have also drawn on our experience conducting cybersecurity assessments and penetration tests from across our global network to identify the ten most common security vulnerabilities in OT/ICS networks¹⁹. By identifying cybersecurity flaws and the risks these vulnerabilities present, decision-makers in the sectors will be better placed to implement appropriate security controls, design more secure architectures, monitor targeted attacks and maintain effective cyber resilience for their OT/ICS networks:

Internet accessible OT systems



OT systems are often directly connected to the Internet in most cases so that third-party vendors can remotely connect to the system to perform diagnostics and maintenance. This makes it possible for potential attackers to directly perform password 'brute forcing' or probe these interfaces, which can cause OT systems to become unstable or fail completely, resulting in business disruption.

OT/ICS systems located within corporate networks



Corporate systems usually require some level of interconnectivity with the OT network in order to access operational data or export data to third-party management systems. The increasing frequency of cyberattacks on corporate IT networks means that this type of overlap between the networks poses a serious risk as attackers may be able to use a compromised corporate IT system to access OT networks.

Insecure remote connectivity to OT/ICS networks



The use of strong multifactor authentication mechanisms, enforced password policies and appropriate security patching practices can minimise the risk of compromise through remote access devices. In addition, monitored jump-boxes, dedicated to brokering all remote access connectivity to the ICS/OT network, can provide an extra level of security.

Missing security patches



OT/ICS systems are known to run outdated software versions with known security vulnerabilities, leading to increased risk of compromise by an attacker. Processes and procedures should be established to thoroughly test patches and apply updates to OT systems. If a patch is found to cause production issues, other compensating controls such as segregation, authenticated access, logging and monitoring, firewall and device hardening may be employed to reduce the probability of compromise.

¹⁹ <https://www.pwc.com/ca/en/services/consulting/technology/operational-technology.html>



Poor password practices

Businesses may have strong corporate password standards but often fail to apply these to their OT environment. Common issues include:

- Operators and administrators using the same usernames and passwords for corporate and OT systems.
- Generic user accounts usually having easily guessable passwords or passwords that are identical to the username.
- Failure to change default vendor credentials on embedded devices and management interfaces from the initial installation or setup.

Organisations need to establish and maintain a strict separation between authentication mechanisms and should require separate username conventions for the corporate IT and OT/ICS networks.



Insecure firewall and peripheral device policy management issuing security patches

Firewalls that segregate OT networks from corporate networks are an essential control in protecting both networks. However, insecure configuration and management of these firewalls significantly increases the potential attack surface of the OT network. Without properly secured firewalls, security threats to the corporate IT network can easily propagate to the OT network, leaving it susceptible to attack.



Lack of segmentation within OT/ICS networks

Many OT networks are designed and configured in a flat and unsegmented configuration to simplify the management of the network. It is imperative for organisations to define a clear separation between critical and non-critical systems in the OT/ICS networks. This will not only limit the impact of a breach but also help apply appropriate security controls to the most critical systems and data on the network.



Unrestricted outbound internet access from OT networks

In some instances, direct outbound Internet access is enabled from the OT network, for example, to allow for patching or for operator maintenance research. Direct Internet access from the OT network also increases the risk of external command-and-control attacks. Outbound access to the Internet from OT systems should be restricted, with any exemptions requiring a formal risk assessment. In the case of such exemptions, OT/ICS systems requiring external access must be securely patched, closely monitored and appropriately segregated from the rest of the OT network.



Weak peripheral protection from the corporate IT network to the OT/ICS systems

Connectivity to the corporate IT network, from the OT network, may provide a pivot to enter the corporate environment through insecure OT devices, increasing the risk of unauthorised access. It is important to restrict access between these two networks, based strictly on business need. Any connection between the OT network and the corporate IT network should be through systems hosted in a DMZ, or secure gateway between the two networks.



Insecure encryption and authentication for wireless networks

OT networks often use wireless and microwave solutions to connect devices and systems, sometimes over considerable distances. It is not uncommon for the deployed wireless equipment in OT networks to use deprecated security protocols or technologies, leaving them vulnerable to modern eavesdropping and authentication bypass attacks. Using strong wireless encryption protocols, industry-standard cryptographic algorithms and mutual authentication between communicating OT systems is the best way to minimise the risk of wireless attack.



How can PwC help?

To have a deeper discussion about how to protect against or investigate digital compromises, please contact the PwC Forensic Technology Solutions team:

Junaid Amra

+27 (0) 82 953 9325
junaid.amra@pwc.com

Solomon Bhala

+27 (0) 65 970 6189
solomon.bhala.za@pwc.com





At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

©2021 PwC Inc. [Registration number 1998/012055/21] ("PwC"). All rights reserved.

PwC refers to the South African member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/za for further details. (21-26898)