Digital Forensics and Incident Response 2023 Year In Review

CyberCX

Contents

Foreword

Cyber incidents are, and will continue to be, an unfortunate fact of life for individuals, organisations, and communities in an increasingly connected world.

Over the 12 month period that this report covers, CyberCX's Digital Forensics & Incident Response (DFIR) team has been involved in most of the large, nationally significant and headline-grabbing breaches in both Australia and Aotearoa, as well as hundreds of smaller incidents that never make the news.

Ransomware, espionage, business email compromise, digital forensic investigations – at any given moment, we are usually responding to all of these types of incidents simultaneously, with the largest capability of its kind in the region.

The human impact of these breaches should not be understated; digital environments can ultimately be rebuilt as a function of time and resources, but the impact of data breaches on the people caught up in them cannot always be undone.

Providing high quality digital forensics and incident response (DFIR) services to help those people is the core mission of CyberCX's DFIR team.

Indeed, the common thread running through the myriad of incidents we respond to is the people we help – CISOs and security teams, business owners, IT staff, customers – real people, who suffered financial losses, had their data stolen, or lost their days, nights and weekends in an effort to respond and try to recover.

Our DFIR team prides itself on being first to the front lines, at any time of the day or night, guiding clients through incidents, evicting threat actors, and charting complex remediation – it is our job to find clarity in the chaos. We do this by earning trust from our customers, rolling up our sleeves, and providing world-class expertise when they need it most.

This report reflects casework from many thousands of people-hours, delivered by experts dedicated to their craft. I am immensely privileged to work with this team, whose hard work in responding to the incidents reflected in this report means they too put themselves and their skills on the line to defend organisations under attack, often sacrificing weekends or family time (or Christmas, twice) in doing so.

The threat actors we go up against are relentless in their efforts to exploit vulnerabilities and cause maximum harm to organisations large and small, across all industries. Our insights are therefore hard-won. They are also genuinely unparalleled in our region: our assessments and metrics are based on first-party sources and lived experience distilled from incident responders living in the communities they serve.

It is our sincere hope that organisations across Australia and New Zealand are able to leverage these valuable insights and implement our recommendations to increase their security posture. In doing so, together we can make life harder for the bad guys.

Hamish Krebs
Executive Director, Digital Forensics & Incident Response, CyberCX

Year In Review

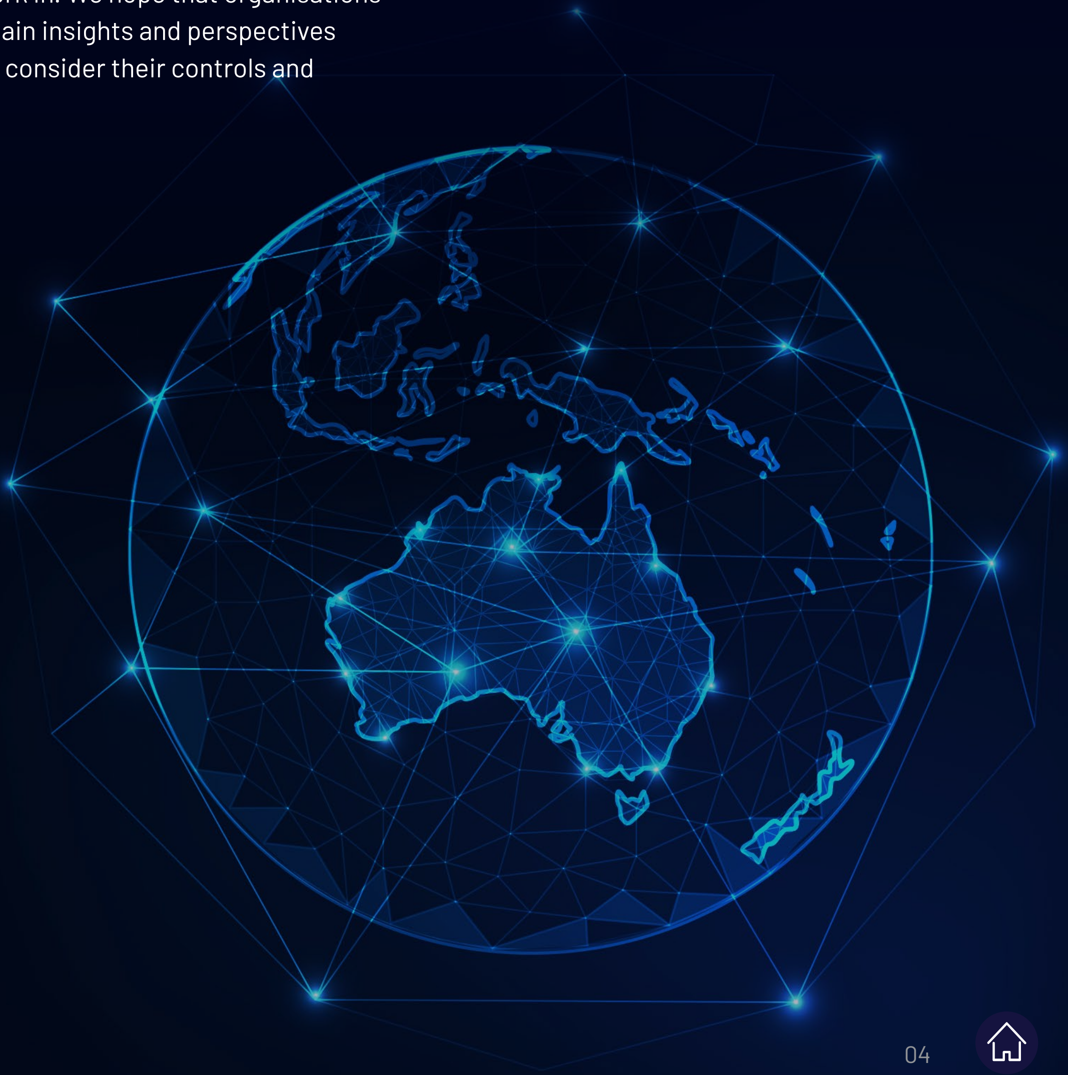
Introduction

CyberCX's Digital Forensics and Incident Response team is the largest in both Australia and New Zealand (AUNZ). Our cases represent an important sample of the threat trends and attacker tradecraft impacting organisations across our region.

Using data from a sample of over 100 serious incidents we responded to in 2023, this report highlights insights into incident trends in 2023 including an in-depth look into the most common incident categories – Cyber Extortion and Business Email Compromises.

Compared to other publicly reported statistics, such as those released by the Australian Cyber Security Centre (ACSC) and CERT NZ/National Cyber Security Centre (NCSC), our data is biased towards incidents which affect organisations rather than individuals.

We are publishing this data as part of CyberCX's mission to secure the communities we live and work in. We hope that organisations across our region will use it to gain insights and perspectives on the threat landscape as they consider their controls and strategies for 2024.



2023 Key incident insights

Business email compromises (BEC) are continuing to grow year on year

There was a **37% increase** in business email compromises (BEC) investigated.

Multi-factor authentication (MFA) isn't stopping BEC

There were **five times more** cases that involved Adversary-in-the-middle (AITM) or session theft as Initial Access for BEC incidents than 2022.

"Data Extortion only" as a Cyber Extortion tactic was more common in 2023

The number of Cyber Extortion cases that involved the threat actor only stealing data (Data Extortion) and not deploying ransomware **more than tripled** (compared to 2022).

Remote access solutions with valid credentials became the number one initial access method for Cyber Extortion incidents

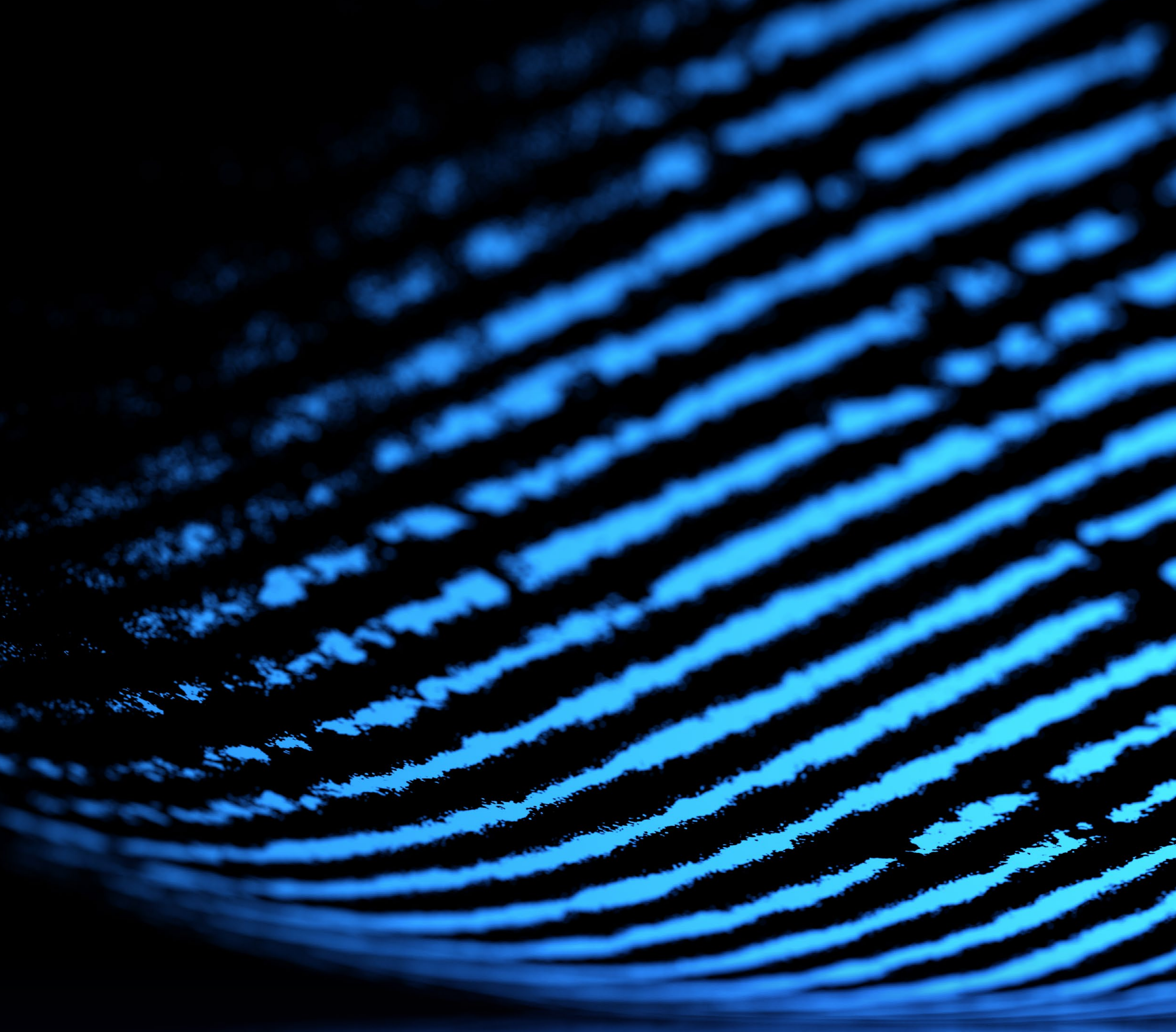
Valid credentials for remote access solutions became the most common initial access method over vulnerability exploitation.

Fewer victims are paying ransoms

We observed roughly **50% less** payments by victims of Cyber Extortion.

Not paying doesn't always mean your data will be leaked publicly

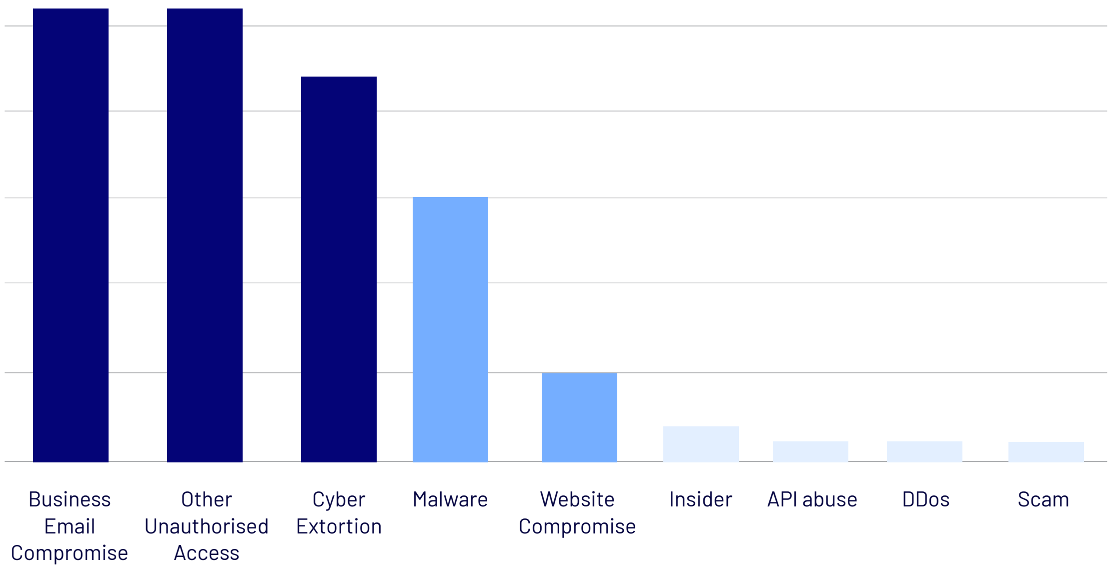
53% of Cyber Extortion Victims that had their data stolen and did not pay a ransom did not observe it leaked publicly or on a dedicated leak site (was 46% in 2022).



Overview of incidents in 2023

Types of incidents

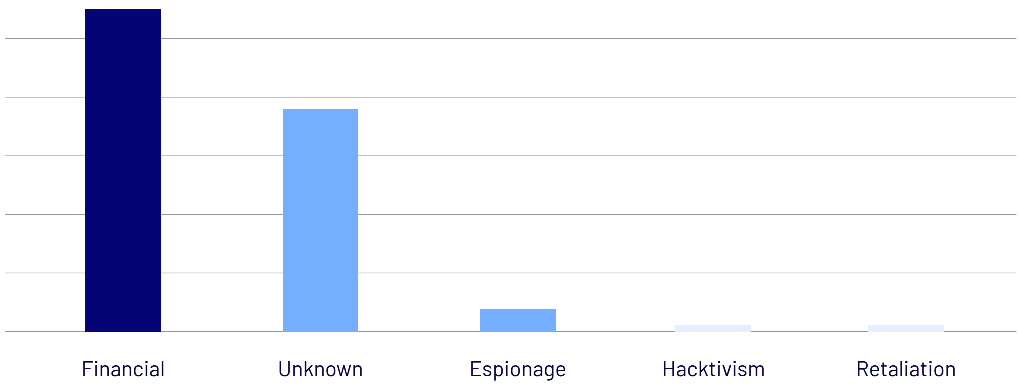
CyberCX responded to a wide range of scenarios, however, the most common were Business Email Compromise, Unauthorised Access, and Cyber Extortion. The data in this report include incidents from Australia and New Zealand that fell into the following exclusive categories.



Incident Types	Description
Business Email Compromise	An attack where criminals compromise victim's email accounts, typically through phishing emails. They then use access to send additional phishing emails or insert themselves into existing email threads about financial transactions.
Unauthorised Access	Malicious access to a network which did not result or display specific actions on the target. This may include such incidents as a compromised network device due to exploitation, but no further actions were taken.
Cyber Extortion	The confidentiality or availability of a victim's systems or data is held at ransom by a malicious actor. This can be facilitated by encrypting systems and files using **ransomware only**, or **data extortion only** by exfiltrating sensitive data and threatening to release it. In many cases incidents can include both, commonly referred to as "**double extortion**".
Malware Infection	User endpoints or servers were infected with malware.
Website compromise	A website and/or webserver was compromised, typically through vulnerabilities in Content Management Systems (CMS).
Insider	An actor with existing access or knowledge of an organisation, such as an employee or administrator, conducts malicious activities on a network.
API Abuse	Applications being used for unintentional results, such as abusing APIs in an automated fashion.

Threat actor motivation

CyberCX responds to a variety of cyber incidents that reflect the wider cyber landscape, the most common being financially motivated.



Motivation	Explaination
Financial	Actors motivated by financial gain
Unknown	Unknown is classified when the investigator has less than moderate confidence of the threat actor's motivation. This may be due to the incident being contained before there are actions on objectives or not enough attributable data is available.
Espionage	Incidents that involve a threat actor establishing access to systems or stealing information for intelligence purposes.
Hacktivism	Action based on social or political causes
Retaliation	Following certain actions such as employee termination or changes that result in the actor wanting to impact the organisation.

Espionage and time-to-detection (TTD)

The average TTD of espionage incidents was **390 days**, whereas financially motivated incidents was **60 days**, which highlights the stark difference in time going undetected.

The longest TTD we uncovered in 2023 was during a Compromise Assessment where the CyberCX DFIR team identified a state-sponsored threat actor had access to, and was monitoring, an environment for more than two years. Some organisations choose to actively hunt for latent compromise in their environment through a process called a Compromise Assessment.

2.2 years longest time-to-detect (TTD) of a threat actor conducting espionage activities uncovered by CyberCX in 2023

Vulnerabilities

Below are the vulnerabilities the team observed being exploited in 2023 mapped to the relevant incident category. During our investigations it is common to uncover previous incidents that may not have been discovered until a later incident, which explains why the team commonly identifies exploitation of much older vulnerabilities.

Vendor/Product	Vulnerability Exploited	IR Case Categories
Primetek Primefaces	CVE-2017-1000486	Website Compromise
Telerik	CVE-2019-18935	Other Unauthorised Access
Citrix Netscaler	CVE-2019-19781	Malware
OpenPBX	CVE-2019-3705	Other Unauthorised Access
Citrix Netscaler	CVE-2021-26855	Cyber Extortion Other Unauthorised Access
Pentaho (Log4j)	CVE-2021-44228	Website Compromise
Zoho ManageEngine	CVE-2022-47966	Other Unauthorised Access
IBM Aspera Faspex	CVE-2022-47986	Other Unauthorised Access
GoAnywhere	CVE-2023-0669	Cyber Extortion
Cisco IOS XE	CVE-2023-20198	Other Unauthorised Access
Confluence	CVE-2023-22515 CVE-2023-22518	Cyber Extortion
Adobe ColdFusion	CVE-2023-26360 CVE-2023-29298	Other Unauthorised Access
Barracuda Email Gateway	CVE-2023-2868	Other Unauthorised Access
Citrix Netscaler	CVE-2023-3519	Other Unauthorised Access
Citrix Netscaler	CVE-2023-4966	Cyber Extortion Malware Other Unauthorised Access

Principal Investigator Phill Moore recently ***published an in-depth look*** at some of the compromised Citrix NetScaler devices we investigated and the trend of commonly finding much older compromises than initially thought.

Cyber extortion insights

Cyber extortion insights

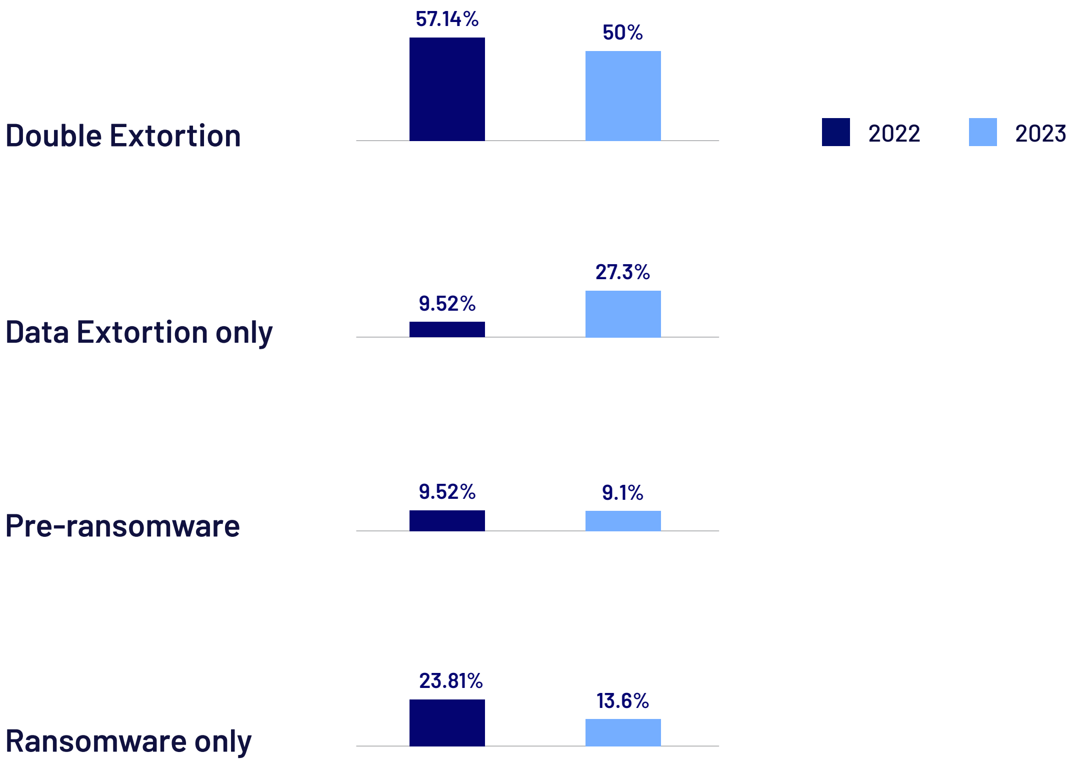
The CyberCX DFIR team tracks Cyber Extortion cases in four different categories. **Ransomware, Data Extortion**, both (**Double Extortion**), and incidents where the threat actor was removed from the environment before their objectives were completed (Pre-Ransomware). **Pre-ransomware** cases are classified based on an intelligence-led assessment of the threat actor's activities, techniques, and demonstrated intent prior to eviction.

32%

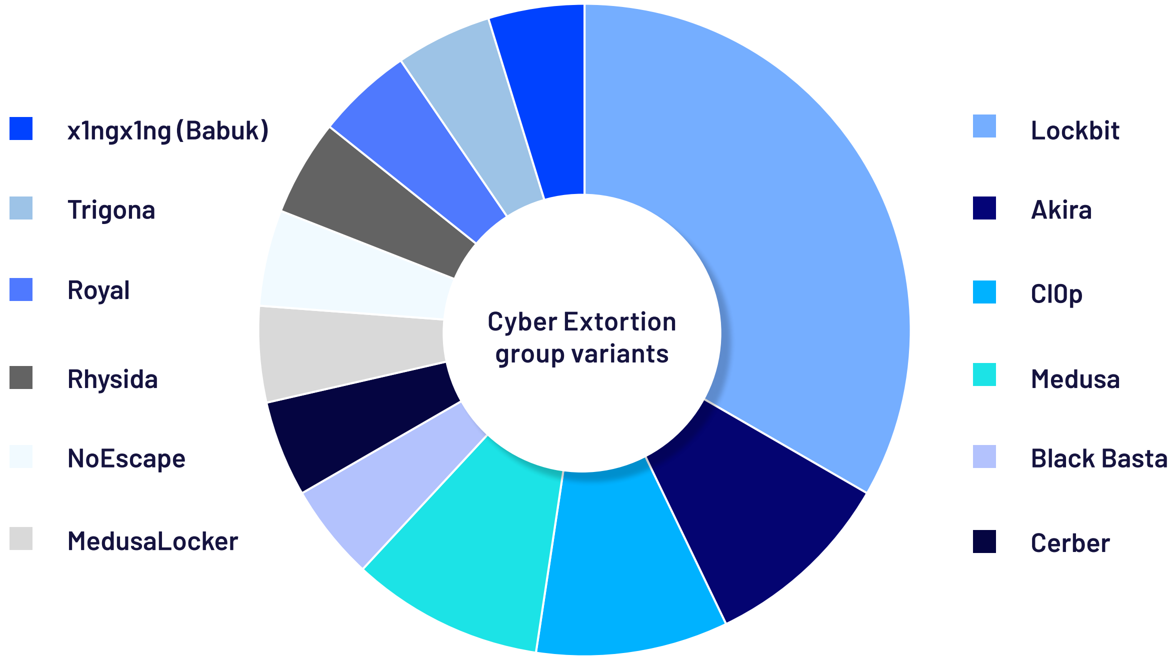
of Cyber Extortion victims had an EDR solution deployed in some capacity.

Overall, the team responded to similar volumes of Cyber Extortion incidents as 2022. However, 2023 saw a three-fold increase in the number of 'Data Extortion only' cases while 'Ransomware only' cases decreased.

While extortion groups such as Cl0p relying on exploitation of Managed File Transfer (MFT) devices influenced this trend, groups that typically rely on Double Extortion, such as Akira and LockBit were also observed in 2023 resorting to Data Extortion only.



In 2023, CyberCX responded to incidents involving at least 12 different Cyber Extortion families. The most prominent ransomware variant CyberCX responded to affecting Australian and New Zealand organisations was LockBit, which accounted for approximately a third of cyber extortion cases.



Does not paying mean your data will be leaked?

Of the Cyber Extortion victims that had data exfiltrated from their networks, and did not pay, 53% of victims have not observed their data published publicly or on a dark web leak site. While the data was never publicly released, it is feasible that the data could have been reused or monetised, for example by selling it to other threat actors. However, this is not possible to verify with confidence.

Once removing data points from the extortion families that don't have a Dedicated Leak Site (DLS), the figure becomes 42%. This discrepancy is due to a subset of extortion groups that chose not to publicise the data they have stolen.

As many rely on dedicated leak sites to track ransomware victims, our case insights reinforced that public ransomware statistics for AUNZ are often incomplete.

The following sections include a closer look at key phases of an attack that have been broken down into the trending techniques of 2023. In certain sections we attribute tool usage and techniques to a certain extortion group that function as Ransomware-as-a-Service (RaaS). We acknowledge and understand that many of these actors are affiliates to multiple extortion groups and their techniques and tooling do not represent the RaaS group in its entirety.

Initial access vectors

Move over Exploitation, Valid Credentials takes the top!

In Cyber Extortion incidents, the top three techniques of initial access (mapped to MITRE ATT&CK) observed in 2023 were:

Rank 1 ↑ **Valid Accounts - T1078 & External Remote Services - T1133** (previously #3)

Rank 2 ↓ **Exploit Public-Facing Application - T1190** (previously #1)

Rank 3 ↓ **Brute Force - T1110** (previously #2)

In 2022, 38% of Cyber Extortion cases involved exploitation of a vulnerability, which decreased to 23% of cases in 2023. Valid credentials used on an external remote service such as a VPN went from 19% (2022) to 36% making it the most common initial access method of 2023. There was only one observed incident that involved distributed malware in 2023. Various distributed malware networks such as *QBot were disrupted by Law Enforcement* last year which may have affected our observations of this trend.

Below is a mapping of initial access methods to extortion groups observed utilising each technique:

Initial Access Technique	Extortion Groups
Valid Accounts - T1078 & External Remote Services - T1133	Akira Lockbit Medusa Rhysida Trigona x1ngx1ng
Exploit Public-Facing Application - T1190	Cerber Cl0p
Brute Force (RDP) - T1110	LockBit MedusaLocker
Phishing - T1566 to deliver Qbot (QakBot) - S0650	Black Basta

Valid accounts - T1078 & external remote services - T1133

Threat actors were commonly using valid credentials against remote services in 2023 to gain initial entry into an organisation. This category is very different to brute forcing access as there was no indication of spraying or guessing passwords in these cases, inferring the threat actor knew the password at the time of the intrusion.

For several incidents, this was traced back to a user that had infected their non-corporate machine with infostealer malware resulting in their saved browser credentials being stolen. Infostealer typically is delivered in trojanised software which aims to steal saved credentials and cookies from the device it is run on. It should be noted that the majority of these incidents did not have MFA or other preventative controls applied thoroughly across all external access points in their network.

For those that did have an MFA mechanism employed, we observed the following circumstances that led to the threat actor gaining access:

- A legacy remote access solution that didn't have MFA enforced that was planned to be decommissioned.
- A service account that didn't have an MFA requirement used to gain a VPN connection.
- The threat actor identified accounts that were yet to be enrolled in MFA and enrolled themselves.

Of note there were no extortion cases that commenced with MFA fatigue or SIM swapping.

Exploit public-facing application - T1190

There were four critical vulnerabilities that CyberCX observed associated with the Cyber Extortion cases we investigated.

Vulnerability ID	Vendor	Cyber Extortion Family
CVE-2021-26855 (ProxyLogon)*	Microsoft Exchange	Royal
CVE-2023-4966 (CitrixBleed)	Citrix	Pre-ransomware
CVE-2023-0669	GoAnywhere	Cl0p
CVE-2023-22515	Confluence	Cerber

** In this case, the threat actor had successfully compromised the Exchange server to deploy a web shell in 2021. The victim organisation patched the server but the web shell remained. It was not used until 2023 to deploy Royal ransomware.*

Brute force (RDP) - T1110

RDP being exposed to the internet is arguably one of the quickest ways to get ransomed. However, we still observe it as one of the main access methods via brute force and password spraying. It is rare that organisations we assist intentionally leave these hosts open to the internet. The most common reason that leads to this vector is when cloud workloads have had their network rules accidently left open to the world during set up or via a misconfiguration.

In one instance, a misconfiguration left a specific server open to the internet for months, during which it was encrypted by the same ransomware variant three times before further actions by the threat actor caused an outage and, based on the naming and TTPs observed, this was done by 2-3 affiliates within the group. During our analysis, a review of the internal ticketing system confirmed that the change was intentional, however the follow up activity to close the vulnerability was not scheduled.

Tooling

Once in the victim network, the threat actor attempts to understand the environment. This includes identifying key systems and applications running, such as Domain Controllers, Backup Servers and File Shares. Below is a list of tools in order of occurrence that we see the threat actor bring into the network.

Scanning/Enumeration Tool	Extortion Groups
ADFind	LockBit
ADRecon	Rhysida Pre-ransomware
Advanced IP Scanner	Akira LockBit MedusaLocker Royal x1ngx1ng
Advanced Port Scanner	Rhysida
Netscan (SoftPerfect)	LockBit Trigona Pre-ransomware
KPortScan3	LockBit

Threat actors continue to rely on Living-off-the-Land Binaries (LOLBINs) to run commands and execute code. PowerShell (T1059.001) is a tool that threat actors continue to rely on to facilitate enumeration and execution phases of an attack. We have also observed the use of WinRM via PowerShell for lateral movement.

Command and control

Cyber extortion actors were observed using less Command and control (C2) frameworks in 2023, choosing to rely on Remote Monitoring and Management (RMM) tools and proxying traffic instead.

Rank 1 Remote access software - T1219

Rank 2 Proxy - T1090

Rank 3 Cobalt strike - S0154

Remote access software - T1219

Remote Monitoring and Management (RMM) tools are not a new technique that Cyber Extortion threat actors employ and are being abused regularly to maintain access to networks. Anydesk was a fan favourite in 2023, with over six different extortion groups deploying it to victims.

RMM Tool	Extortion Groups Family
Action1	Pre-ransomware
Anydesk	Akira Lockbit Medusa MedusaLocker Rhysida Trigona Pre-ransomware
Atera	MedusaLocker Pre-ransomware
FixIT.Me	Akira Pre-ransomware
ScreenConnect	Royal Pre-ransomware
Splashtop	Pre-ransomware
Zoho Assist	Pre-ransomware

Proxy - T1090

Threat actors will commonly establish a SOCKS proxy with their infrastructure to allow direct access to internal services. In 2023, we observed a Black Basta affiliate deploy SystemBC which provided a way for the threat actor to RDP directly into the network. A Rhysida associate established a PowerShell based SOCKS proxy through a user's Run key.

Cobalt strike - S0154

CyberCX has observed a decline in the use of the infamous tool, however was still utilised in cases associated with the following extortion groups:

- Black Basta
- Lockbit
- Royal
- Trigona

In previous years, Cobalt Strike was not only observed in the majority of Cyber Extortion incidents, but was also used to facilitate further major events in the attack chain. With the decline in the usage of the tool, threat actors have moved to deploy other dedicated tools such as proxying software and scanners instead.

Exfiltration

Walking out of the building with your data using SFTP

By a significant margin, the main two methods of exfiltration in Cyber Extortion incidents were SFTP and cloud storage usage.

Rank 1 ↑ **Exfiltration over alternative protocol (FTP & SFTP) - T1048** (previously #2)

Rank 2 ↓ **Exfiltration over web service: exfiltration to cloud storage - T1567.002** (previously #1)

Exfiltration over alternative protocol (FTP & SFTP) - T1048

Threat actors will use applications commonly found in enterprise environments to facilitate exfiltration of data to threat actor-controlled infrastructure. Those most commonly observed in 2023 included:

- WinSCP
- FileZilla
- TotalCommander

In many cases the organisation did not block outbound SFTP or port 22 traffic to the internet which allowed this activity. Threat actors will commonly change their listening port for their SFTP server to port 443 to mimic HTTPS, however application aware firewalls will still be able to identify it is SFTP traffic; this greatly assists during forensic investigations.

Exfiltration over web service: exfiltration to cloud storage - T1567.002

In previous years, we saw threat actors exclusively use applications to sync data to cloud storage such as Rclone and MegaSync; in 2023 we mostly observed direct upload through Web Browsers on the exfiltration hosts.

The top cloud storage sites observed in 2023 were:

- mega[.]io
- 4shared[.]com (4Sync)
- temp[.]sh
- uploadnow[.]io

Time-to-detect (TTD)

The average TTD for Cyber Extortion incidents was **18 days,** with the maximum being 75 days, between initial access and detection. Compared to the overall average TTD of financially motivated incidents (60 days), Cyber Extortion is significantly faster to being detected.

It is worth noting that with many of the Cyber Extortion cases we respond to, detection is typically when ransomware is detonated.

Less than 1 day

the minimum time observed between initial access and detonation of ransomware

75 days

the maximum TTD for a cyber extortion incident

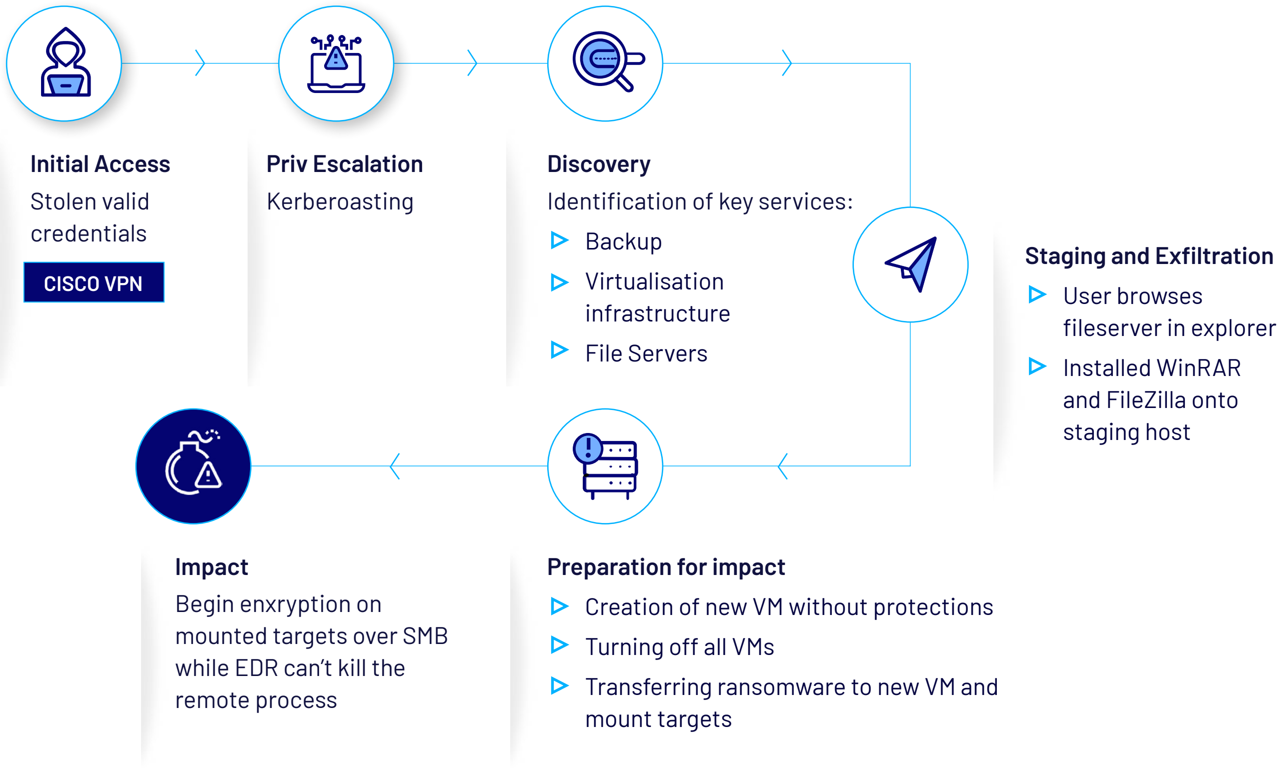
Cyber Extortion Category	Average TTD 2022	Average TTD 2023
Ransomware (only)	Less than one day	12.15 days
Data Extortion (only)	15 days	16.5 days
Double Extortion (Both)	12 days	18.2 days

There was a significant increase in the average TTD for Ransomware Only cases in 2023 due to decrease of cases where the threat actor deployed ransomware as soon as they gained access.

Cyber extortion case insights: Akira ransomware & evading EDR

CyberCX DFIR Principal Investigators Phill Moore and Zach Stanford posted the blog "*Weaponising VMs to bypass EDR*" which highlighted a technique being observed more frequently by Cyber Extortion threat actors. By creating a blank virtual machine or "safe haven" within the organisation, the threat actor can continue their attack unimpeded by EDR.

Below is the full attack chain of an Akira incident the DFIR team responded to in 2023.



Initial Access
Stolen valid credentials

CISCO VPN

Priv Escalation
Kerberoasting

Discovery
Identification of key services:

- Backup
- Virtualisation infrastructure
- File Servers

Staging and Exfiltration

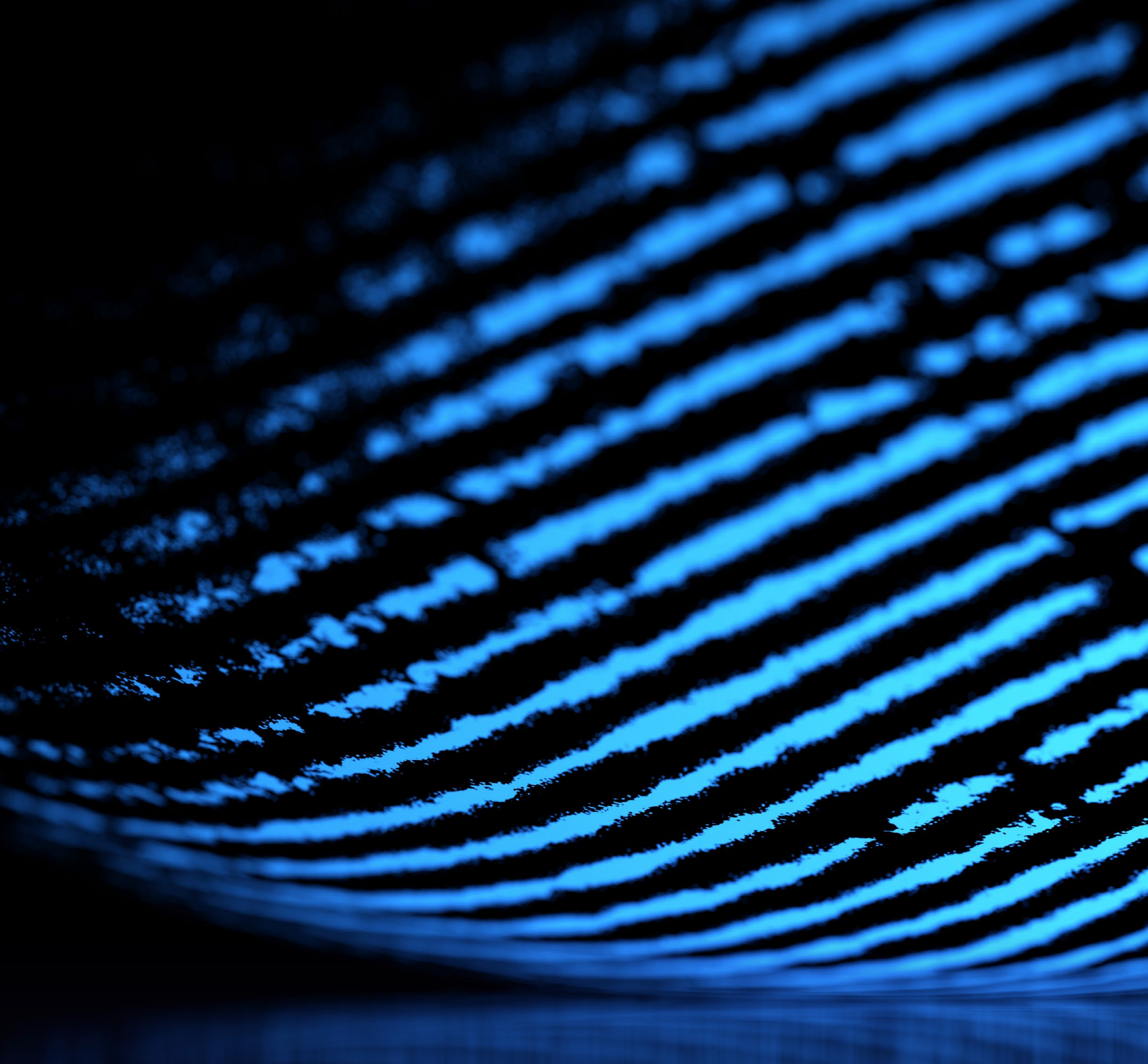
- User browses fileserver in explorer
- Installed WinRAR and FileZilla onto staging host

Preparation for impact

- Creation of new VM without protections
- Turning off all VMs
- Transferring ransomware to new VM and mount targets

Impact
Begin enxryption on mounted targets over SMB while EDR can't kill the remote process

CyberCX's 2023 Ransomware and Cyber Extortion Best Practice Guide, reflects significant changes to the global cyber security landscape as businesses, organisations, and governments continue to grapple with established and emerging cyber threats.



Business Email Compromise (BEC) insights

Business Email Compromise (BEC) insights

BECs are extremely common and effective, yet they do not get the same level of attention that threats like ransomware and data extortion do. BECs are the silent scourge of the industry, affecting everyone from small to large organisations. Even organisations with mature security posture and controls can still being affected financially if their third parties are compromised.

$500,000AUD
was the largest amount lost due to a single BEC in 2023

BEC & Multi-factor authentication (MFA)

MFA is not always enough

As security becomes a priority at all levels of business, security controls such as Multi-factor Authentication (**MFA**) and conditional access policies are becoming widely adopted. In response, threat actors have adapted and developed new techniques.

While many incidents responded to could have been prevented by conditional access policies, MFA, and blocking legacy authentication, there were several scenarios CyberCX investigated where this was not enough to protect the organisation.

The team responded to five times as many cases that involved Adversary-in-the-middle (AITM) or session theft as Initial Access for BEC incidents in 2023 than 2022.

AITM phishing sites allow a threat actor to sit between the victim and the email service during authentication to intercept the request and enable the capture of credentials and, more importantly, a valid session cookie. The threat actor will not be prompted for MFA once they have this cookie.

MFA “bypass” methods observed:

- Accepting MFA request accidently - The victim approves a malicious MFA request through push notification after the threat actor obtains credentials through phishing.
- MFA fatigue - The victim approves a malicious MFA request through push notification spam or coercion.
- Session hijacking - A valid session is stolen through session hijacking or AITM phishing sites.
- Logic error in Entra ID conditional access policies that unintentionally allowed single factor for certain conditions.

Post-compromise actions

Once the threat actor has gained control of a mailbox, they conduct a number of activities, which include:

- Enrolling additional MFA devices to compromised users.
- Modifying policies to allow-list actor-controlled domains in Exchange Online.
- Create Entra ID applications that have persistent access to a mailbox.
- Adding permissions to mailboxes (typically in Finance or Accounts teams).
- Identifying active conversations regarding payments, invoicing, or transactions.
- Modifying real invoices or documents that have been used in the past.
- Hijacking email conversations and providing an “updated” invoice or purchase order with the actor’s payment details.
- Creating lookalike domains to insert them into conversations.
- Creating inbox rules to hide responses to emails sent via the victim.
- Furthering their phishing campaigns.

Time-to-detect (TTD)

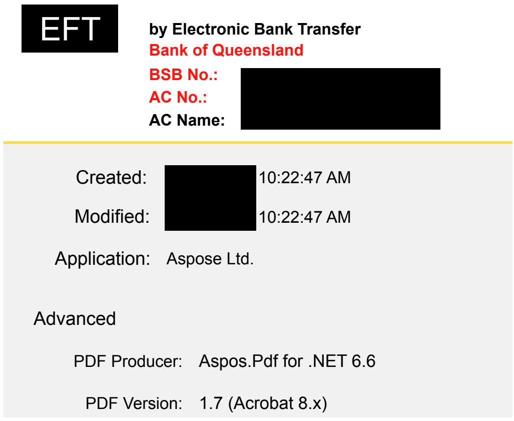
11.5 days

Average time-to-detect for BEC

The TTD observed in BEC is longer than what is observed in other case types. The threat actor's objective in many of these cases is invoice fraud. Due to the nature of their goals, the threat actor typically does not conduct any "malicious" activities in the environment until they identify the right opportunity to strike.

BEC case insights: Fraudulent invoices and application access to mailboxes

Often the fraudulent invoices are identified due to non-technical processes such as communicating with the invoicing party via an out-of-band channel such as phone call. Incidents resulting in successful payments to the threat actors have taken place when a breakdown in communication has occurred, or existing invoicing procedures were not followed or did not exist.



EFT

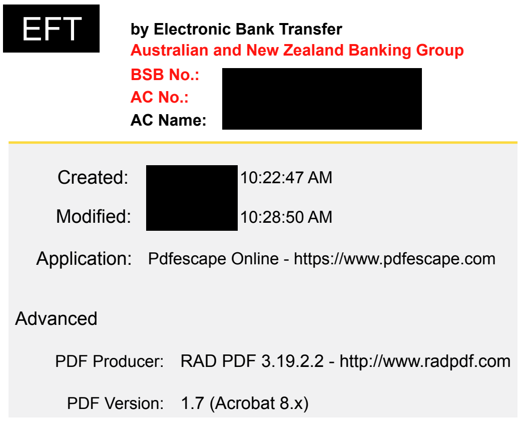
by Electronic Bank Transfer
Bank of Queensland
BSB No.:
AC No.:
AC Name: [redacted]

Created: [redacted] 10:22:47 AM
Modified: 10:22:47 AM
Application: Aspose Ltd.

Advanced

PDF Producer: Aspos.Pdf for .NET 6.6
PDF Version: 1.7 (Acrobat 8.x)

Original invoice



EFT

by Electronic Bank Transfer
Australian and New Zealand Banking Group
BSB No.:
AC No.:
AC Name: [redacted]

Created: [redacted] 10:22:47 AM
Modified: 10:28:50 AM
Application: Pdfescape Online - https://www.pdfescape.com

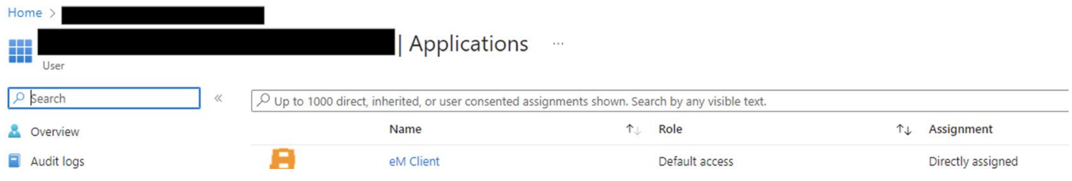
Advanced

PDF Producer: RAD PDF 3.19.2.2 - http://www.radpdf.com
PDF Version: 1.7 (Acrobat 8.x)

Modified invoice

During multiple incidents in 2023, one of the post-compromise activities involved enrolling the compromised user with an application that allows persistent access to the victims, mailbox and, in certain cases, full synchronisation.

The threat actor successfully added the eM Client application as a service principal to the victim's account in Entra ID, allowing the application to access resources in Microsoft 365.



Home > [redacted]

[redacted] | Applications ...

User

Up to 1000 direct, inherited, or user consented assignments shown. Search by any visible text.

Name	Role	Assignment
eM Client	Default access	Directly assigned

The eM Client application has mailbox and contact synchronisation capabilities. The team observed the following permissions scopes being added to the account:

- IMAP.AccessAsUser.All
- EWS.AccessAsUser.All
- offline_access

Takeaways

Use phishing-resistant MFA to stop Business Email Compromise

Don't just rely on MFA by default, use FIDO2 keys or Windows Hello for Business to ensure session hijacking cannot bypass your controls.

Fortify all remote access points

CyberCX is still responding to large scale incidents where MFA on VPN or remote access points would have impeded the attack. Ensure all users are enrolled, and any legacy remote access methods are decommissioned before they can be abused. If feasible, don't allow users to login to your systems from unmanaged devices.

Conduct regular scanning for leaked credentials

Infostealers are one of the most common ways threat actors gain valid credentials to VPN accounts. Credential stealing malware is even more successful on home computing systems where security is not a priority. Ensure threat actors can't use these credentials on your systems by enforcing MFA on all internet facing systems. Conduct regular scanning for leaked credentials.

Clean up your organisation's data

Don't make it easy for attackers to steal your data. Audit what you've got, before it comes back to bite you. Corporate share drives are still one of the main targets for data theft due to their lack of controls and content.

For more actions to prepare and prevent Cyber Extortion, read our
2023 Ransomware and Cyber Extortion Best Practice Guide

How can we help?

Be prepared with a DFIR retainer

Escalating early can be the difference between being ransomed and containing your incident. Make sure you have a ***retainer*** in place with the CyberCX DFIR team to ensure you are prepared.

Proactively hunt in your network with a Compromise Assessment

A ***Compromise Assessment*** provides a point-in-time snapshot of whether a network contains evidence of current or historical malicious activity, with a particular focus on highlighting artefacts that are most often overlooked or can remain hidden to other detection capabilities.

Know your enemy

Stay informed and up-to-date with the latest developments from our ***Cyber Intelligence*** team. Our unique capability can empower your team, from strategic threat assessments to operational intelligence reports on the latest threat actor tradecraft and insights.

Test your organisation for the latest threats

Our Security Testing and Assurance and Cyber Intelligence practices use our insights responding to incidents to formulate up-to-date and relevant emulation scenarios to run ***Red and Purple teaming exercises***.

Is your organisation's network resilient from a ransomware attack?

Ensuring your organisation is resilient against threat actors requires end-to-end expertise. Understanding how your network and systems are set up and how to align them with security best practice is fundamental. ***Find out how the Network and Infrastructure Solutions practice can assist here***.

Ensure your cloud email is secure

The data stored in your users' mailboxes can be some of the most sensitive data in the organisation. Make sure your cloud is resilient to MFA resistant phishing by talking to our ***Cloud Security and Solutions team***.

About CyberCX

CyberCX is the leading provider of professional cyber security and cloud services across Australia and New Zealand. With a workforce of over 1,400 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents and build resilience in an increasingly complex and challenging threat environment.

Through our end-to-end range of cyber and cloud capabilities, CyberCX empowers our customers to securely accelerate opportunities in the digital economy.

Our expertise is represented across 12 cyber security and cloud practices:

- Strategy & Consulting
- Governance, Risk & Compliance
- Security Testing & Assurance
- Privacy Advisory
- Identity & Access Management
- Network & Infrastructure Solutions
- Cloud Security & Solutions
- Managed Security Services
- Cyber Capability, Training & Education
- Cyber Intelligence
- Digital Forensics & Incident Response
- Cyber Strategic Communications

Contact us to find out how CyberCX can boost the cyber security skills of your entire organisation.

National Headquarters

Level 4, 330 Collins Street,
Melbourne, VIC 3000

cybercx.com.au

1300 031 274

New Zealand Head Office

Level 10, 10 Brandon Street,
Wellington 6011

cybercx.co.nz

0800 436 273

CyberCX