Triskele Labs

State of Cyber

Digital Forensics and Incident Response (DFIR) Report

Contents

Executive Summary

The 2023-24 financial year has been marked by numerous high-profile cyber-attacks that have garnered significant attention from Australia's media. However, for every large-scale attack reported in the media, there are numerous others that go unreported, highlighting the pervasive nature of cyber threats.

Our findings show that Threat Actors continue to employ familiar tactics and techniques, particularly when conducting ransomware attacks. Despite the increasing awareness and increased defensive measures, ransomware attacks remain a significant threat, disrupting business operations and causing financial and reputational damage to organisations.

There has also been a notable increase in Business Email Compromise (BEC) attacks, with a rise in session token theft being used to take control over accounts and attempt to perform payment redirection fraud.

Business Email Compromise attacks have evolved, becoming more sophisticated and frequent. Attackers are increasingly targeting session tokens, allowing them to bypass traditional security measures and gain access to sensitive information.

This method of compromise underscores the need for robust email security protocols and vigilant monitoring.

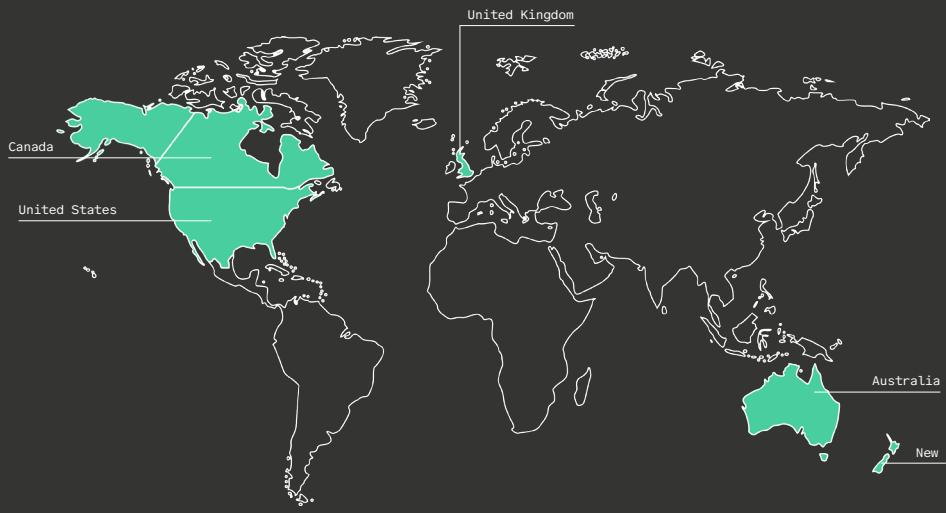
Unfortunately, all Australian organisations, regardless of size or industry, are potential targets for cyber security incidents. It is imperative for organisations to remain vigilant, continuously improve their security posture, and adopt comprehensive measures to protect against the ever-evolving cyber threat landscape. By doing so, they can better safeguard their assets, data, and reputation against cyber-attacks.

Background

This report covers statistics and information gathered from DFIR investigations conducted during the 2023-24 financial year. The data and insights from this are based on the work completed by the Triskele Labs DFIR Team, which has been operating for over three years.

Triskele Labs collaborates with numerous insurance carriers and law firms, providing specialised DFIR services that support legal and insurance claims related to cyber incidents. Our team works closely with these partners and clients to ensure that investigations are thorough, accurate and meet the necessary legal and regulatory standards.

The DFIR team have assisted hundreds of Australian organisations of all sizes, from small sole trader practices to large enterprise clients with thousands of servers and endpoints within their environment. This broad experience enables the DFIR Team to effectively respond to all types of cyber incidents experienced by businesses.



10 Years

5 Eyes Presence

80 Employees

Australian based

ISO27001

ISO20000

Contributors

The Triskele Labs DFIR Team comprises of experts located worldwide, enabling us to offer follow-the-sun forensic analysis capabilities. This round-the-clock coverage ensures organisations can quickly understand the nature and extent of cyber incidents and take necessary steps to safely restore operations.

Our global presence facilitates continuous monitoring, rapid response, and effective threat mitigation, minimising downtime and allowing organisations to resume normal activities swiftly and securely.

We extend our gratitude to the Triskele Labs DFIR Team members for their invaluable contributions to this report:

Richard Grainger
Global DFIR Lead
Operations Australia

Craig Martin
Incident Response Manager
Operations Australia

Chris McAdam
Incident Response Associate
Operations Australia

Nick Thanos
Senior DFIR Analyst
Operations Australia

Jordan Lloyd
DFIR Analyst
Operations New Zealand

Michael Varley
DFIR Analyst
Operations United Kingdom

Jason Trapp
DFIR Analyst
Operations Canada

Olivia Lake
DFIR Intern
Operations United States

Jannis Herbst
DFIR Engineer
Engineering Australia

Cameron Paddy
DFIR Analyst
Operations New Zealand

Caleb Boyd
DFIR Analyst
Operations Australia

Incident Statistics

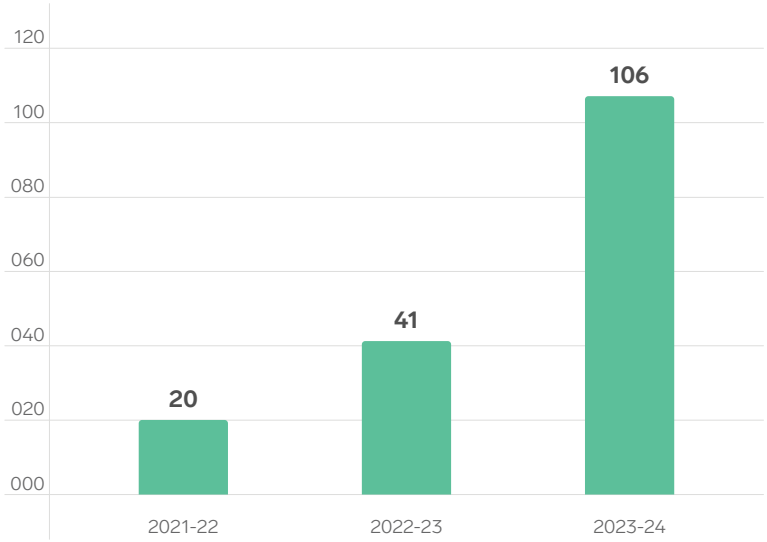
Incidents Year on Year

The Triskele Labs DFIR Team were engaged to perform 106 DFIR investigations over the course of the 2023-24 financial year, representing a 158% increase from the previous financial year. This significant rise in engagements highlights the growing prevalence and complexity of cyber incidents.

Over the past three financial years, the team has handled a total of 167 investigations, with 20 in 2021-22, 41 in 2022-23, and 106 in 2023-24, demonstrating a consistent and rapid increase in demand for DFIR services.

158% increase in demand for DFIR services.

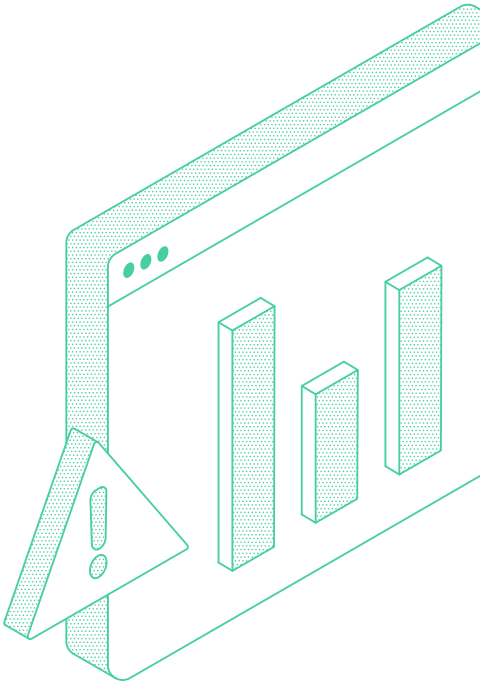
Incident Numbers



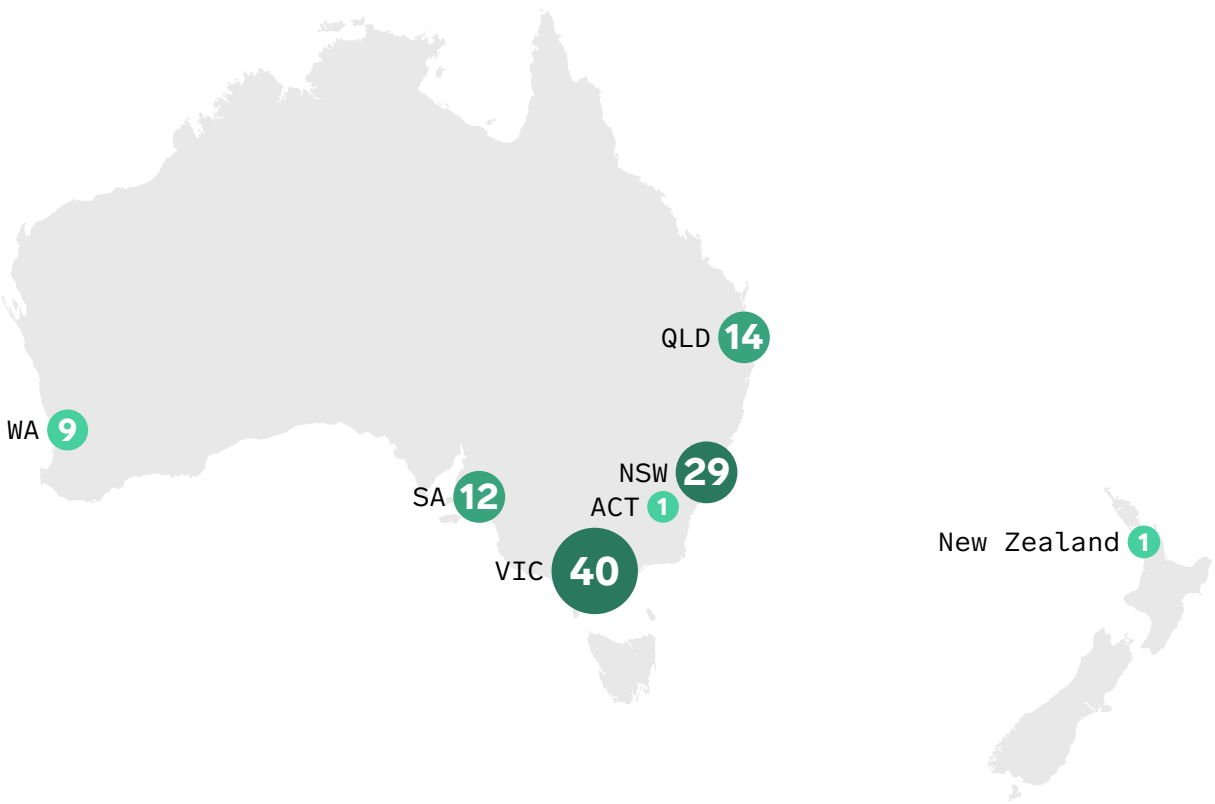
Incident Heatmap

In the past financial year, the Triskele Labs DFIR Team has responded to 106 cyber security incidents, with affected organisations headquartered across various regions. Notably, Victoria (VIC) had the highest number of incidents at 40, followed by New South Wales (NSW) with 29. Queensland (QLD) and South Australia (SA) also experienced significant numbers, with 14 and 12 incidents respectively.

This data highlights that cyber security threats impact businesses across all Australian states, as well as New Zealand, demonstrating the widespread nature of these incidents and the importance of robust cyber security measures for organisations regardless of their location.



Incidents in Australia and New Zealand



Incident Types

Throughout the past financial year, the Triskele Labs DFIR Team has dealt with a variety of cyber incidents, reflecting the diverse and evolving threat landscape.

Business Email Compromise (BEC) incidents were the most frequent, with a total of 49 cases.

BEC attacks typically involve attackers gaining unauthorised access to business email accounts, often through phishing schemes, and then using these accounts to attempt payment redirection fraud.

These incidents can lead to significant financial losses and damage to an organisation's reputation. The prevalence of BEC cases highlights the ongoing need for robust email security measures and user awareness training to prevent phishing attacks.

Ransomware incidents were also significant, with 29 incidents responded to. These attacks involve the encryption of data and demands for ransom payments to restore access. The impact of ransomware can be severe, disrupting business operations and leading to potential data loss and financial costs.

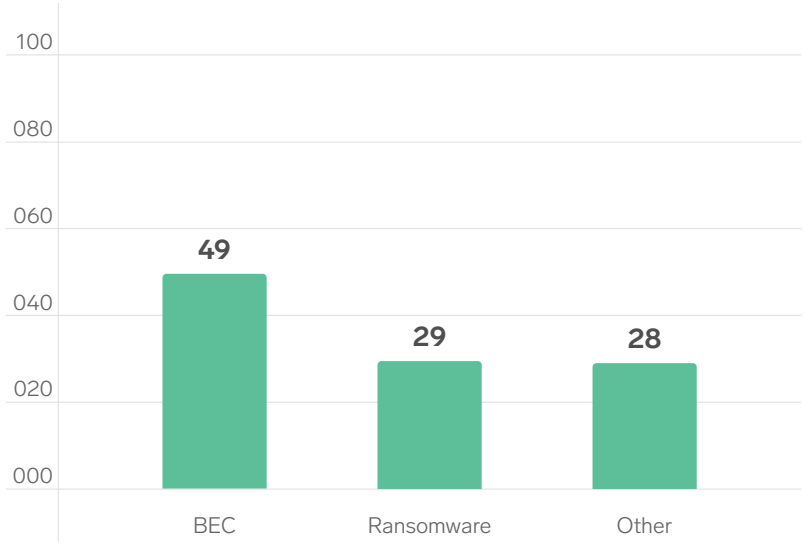
In addition to ransomware and BEC incidents, the DFIR team also investigated 28 other types of cyber incidents. These included a mix

Business Email Compromise (BEC) incidents were the most frequent, with a total of 49 cases.

of malware infections, unauthorised access attempts, insider threats, and data breaches that did not fall into the specific categories of ransomware or BEC.

This variety underscores the complexity of the cyber threat landscape and the necessity for a comprehensive security strategy that addresses multiple attack vectors.

The data collected over the past financial year reveals key insights into the most common threats and the effectiveness of current security measures. By analysing these incidents, Triskele Labs can better understand the tactics, techniques, and procedures (TTPs) used by Threat Actors, enabling targeted advice to incident response strategies and provide more effective protection for clients. As cyber threats continue to evolve, the importance of staying vigilant and prepared cannot be overstated.



Incidents have caused substantial impact to victim organisations, often resulting in complete operational shutdowns.

Industry Verticals

The data reveals that every industry sector can be impacted by a cyber incident, with finance (21 incidents) and healthcare (13 incidents) being the most affected. This broad distribution of incidents across various sectors underscores the opportunistic nature of Threat Actors, who do not necessarily target specific organisations but exploit vulnerabilities wherever they find them.

The significant representation of finance and healthcare may be indicative of poorer security controls within these industries, making them more susceptible to attacks.

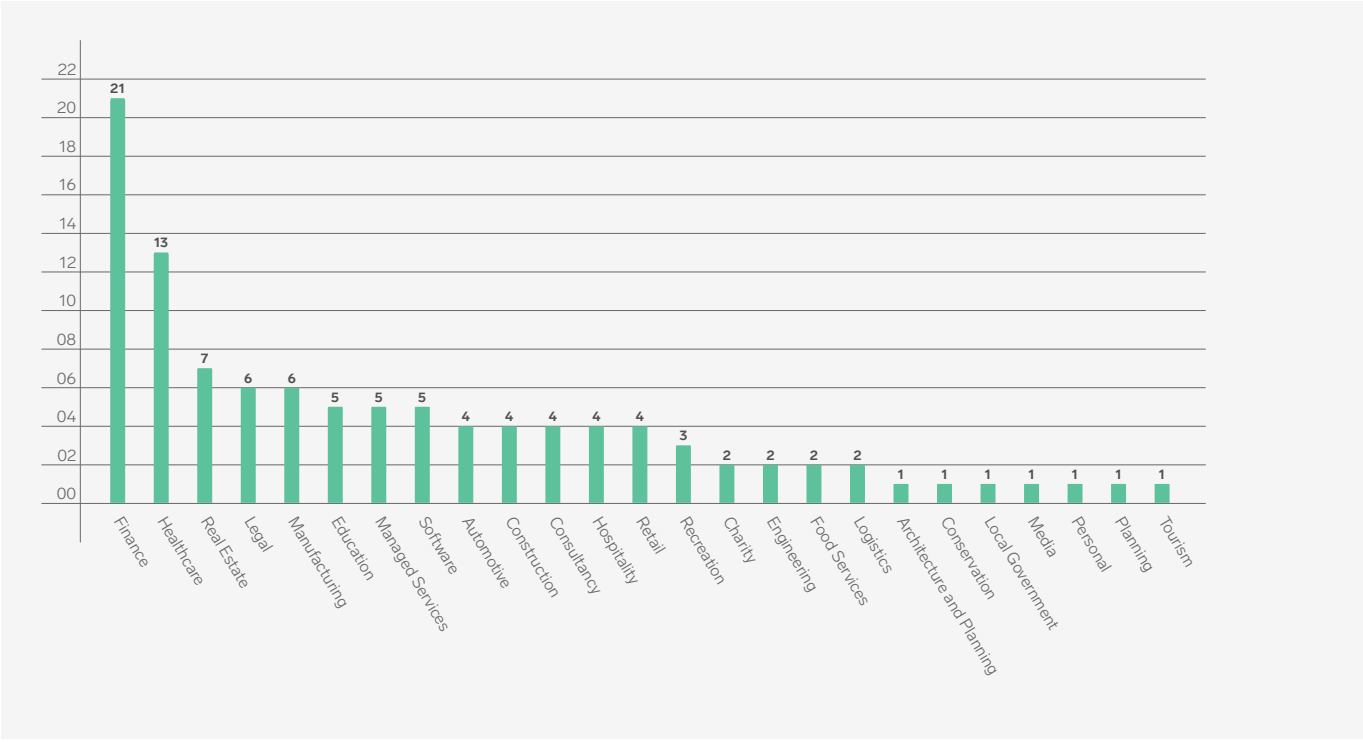
Incidents have caused substantial impact to victim organisations, often resulting in complete operational shutdowns until successful recovery measures are implemented.

Other sectors such as real estate, legal, manufacturing, education,

and managed services have also experienced multiple incidents, highlighting that no industry is immune to cyber threats.

This emphasises the critical need for robust security measures and preparedness across all sectors to mitigate the risks and ensure swift recovery from cyber incidents.

# of Engagement by Industry Vertical



Ransomware

Overview

During the 2023-24 financial year, 27% of engagements by the Triskele Labs Digital Forensics and Incident Response (DFIR) team were related to ransomware attacks.

Ransomware is a type of cyber incident where a Threat Actor gains unauthorised access to an organisation's network, encrypts critical data, and demands a ransom for the decryption key.

This attack vector has become increasingly sophisticated, with double and triple extortion tactics becoming more prevalent.

The average dwell time across all Triskele Labs' ransomware engagements is 33 days.

Double and Triple Extortion Tactics

Traditionally, ransomware attacks involved encrypting data and demanding payment for the decryption key. However, Threat Actors have evolved their tactics to include double extortion.

In these scenarios, attackers not only encrypt the data but also exfiltrate it beforehand. They then threaten to publish the stolen data if the ransom is not paid, increasing pressure on the victim organisation.

Some Threat Actors have escalated this approach further, employing triple extortion techniques. This involves contacting individuals within the victim organisation or its customers, either through email or phone, to inform them of the attack and apply additional pressure. This strategy aims to increase the likelihood of ransom payment by involving more stakeholders and raising the reputational stakes for the victim.

Stages of a Typical Ransomware Attack

A typical ransomware attack generally follows several key stages:

Initial Access
The Threat Actor exploits a vulnerability or misconfiguration to gain entry into the network. Common methods include phishing attacks, brute force attacks on exposed Remote Desktop Protocol (RDP), and exploiting unpatched software vulnerabilities.

Privilege Escalation
Once inside the network, the attacker seeks to gain higher-level access. This is often achieved by exploiting additional vulnerabilities or using weak passwords to obtain domain administrator privileges.

Discovery
The attacker scans the network to identify critical systems, backup locations, and sensitive data. This reconnaissance helps in planning the most impactful attack strategy.

Persistence

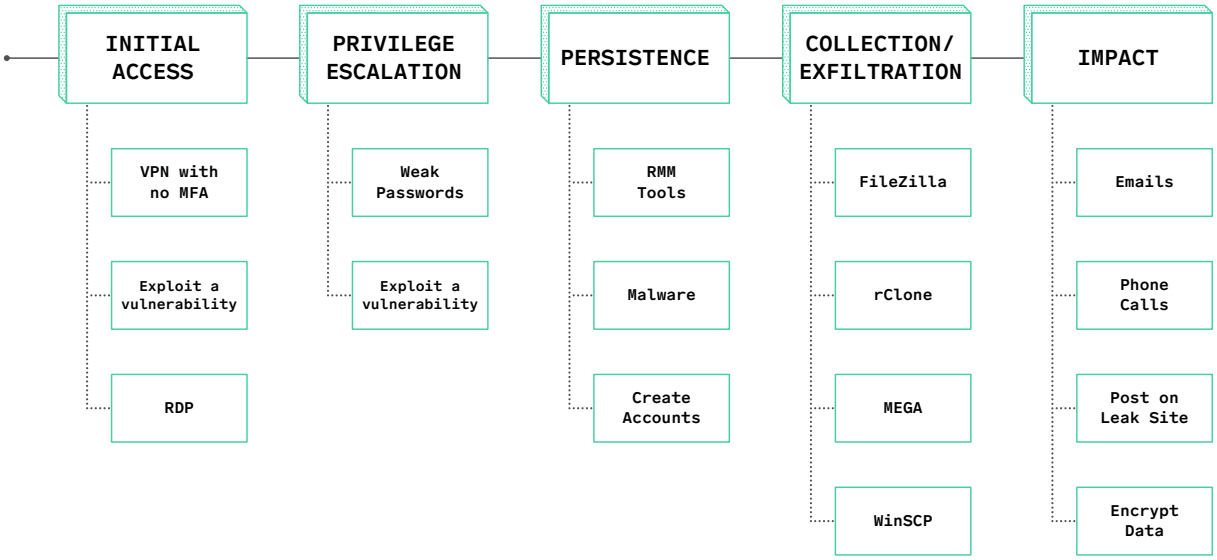
To ensure continued access, the attacker installs backdoors or other persistence mechanisms. This allows them to re-enter the environment if initial access points are discovered and closed.

Exfiltration

Sensitive data is exfiltrated to a server or file-sharing platform controlled by the attacker. This step is crucial in double and triple extortion tactics, where the threat of data exposure is used as leverage.

Impact

The attacker deletes or disables backups and deploys ransomware to encrypt data across the network. This final step often includes a ransom note demanding payment in cryptocurrency for the decryption key.



The average dwell time across all Triskele Labs' ransomware engagements for the 2023-24 financial year, which is the time between the initial access and the impact phase of a ransomware attack, is 33 days.

This prolonged period demonstrated the importance of a thorough investigation following such incidents. Simply restoring data from backups may not be sufficient to secure the network, as the Threat Actor may have already established persistent access points. These backdoors allow the attacker to re-enter the network even after apparent remediation efforts.

A comprehensive investigation is essential to completely purge the attacker from the environment. It enables the victim organisation to understand the full extent of the breach, ensuring all malicious activities and vulnerabilities are identified and addressed.

Additionally, this investigation helps determine which backups can be considered safe for restoration, as compromised backups could reintroduce the threat.

Understanding the breach in its entirety is also crucial for meeting regulatory obligations. Detailed knowledge of the attack helps in reporting to regulatory bodies, fulfilling compliance requirements, and informing stakeholders.

Moreover, it provides valuable insights to prevent future incidents by addressing and identifying weaknesses allowing for reinforcement of security measures. Thus, a thorough post-attack investigation is imperative for both immediate recovery and long-term cybersecurity resilience.

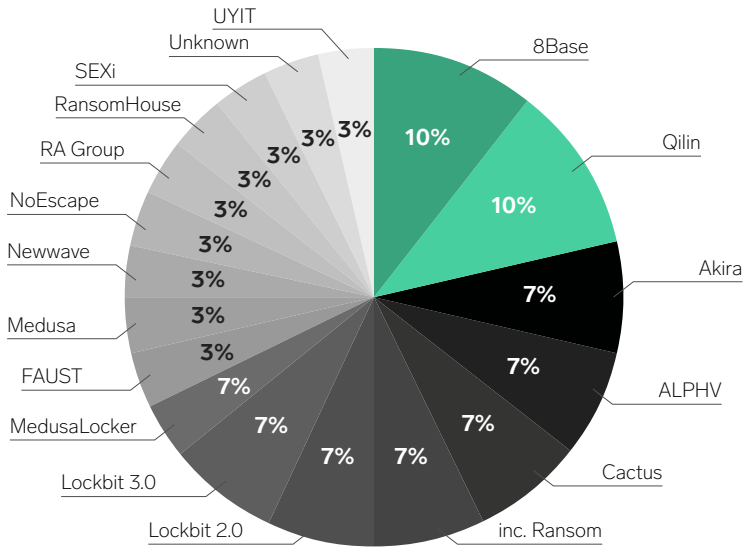
A thorough post-attack investigation is imperative for both immediate recovery and long-term cybersecurity resilience.

Ransomware Groups

During the 2023-24 financial year, the majority of the Digital Forensics and Incident Response (DFIR) Team's ransomware engagements involved Threat Actors previously investigated in either the current or the previous fiscal year.

This recurring involvement with known groups significantly enhanced our ability to handle these investigations efficiently. Our prior knowledge of these groups' Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs) allowed us to streamline our investigative processes and respond more swiftly to incidents.

Engagement by Threat Actors



Leveraging Prior Knowledge

One notable example of leveraging prior knowledge involved the ransomware group 8Base. Our familiarity with their operations, particularly their preference for using FTP for exfiltration to Eastern European VPS hosts, proved invaluable.

As soon as we accessed the organisation's firewall during the investigation, we ran a query based on this known behaviour and promptly confirmed that data exfiltration had indeed taken place.

This early identification enabled us to notify key stakeholders about the data exfiltration at the onset of the investigation, allowing for timely decisions and actions to mitigate further damage.

Confirming and Disproving Data Exfiltration Claims

While ransomware groups commonly claim data exfiltration as a tactic to pressure victims into paying ransoms, our investigations often confirmed these assertions.

However, there were instances where, despite our understanding of certain groups' tendencies to exfiltrate data, no evidence of such activity was found through both host-based and network-based forensic analysis.

This thorough verification process is crucial, as it ensures that responses are based on accurate and comprehensive assessments rather than assumptions, helping to build a clear picture of the attack and its impact.

Evolving Tactics: Direct Pressure Strategies

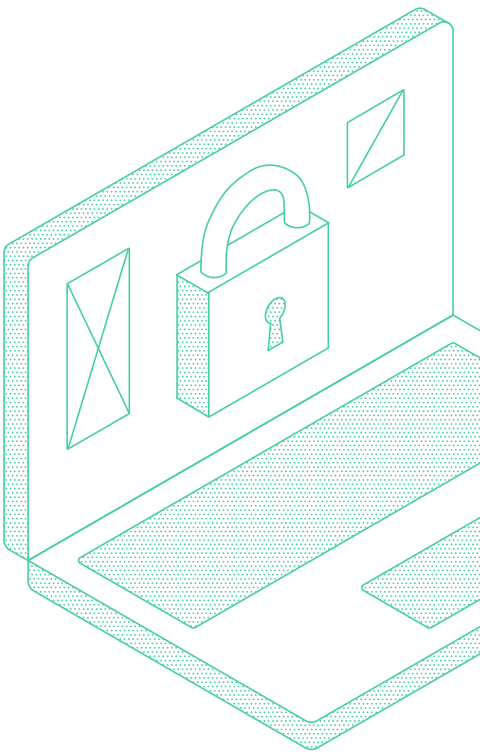
In addition to the technical aspects of ransomware attacks, we observed an increase in engagements where Threat Actors employed direct tactics to pressure victim organisations into paying ransoms.

One such tactic involved calling staff members directly to exert additional pressure. This rise in aggressive, direct-contact strategies by ransomware groups underscores the evolving nature of the threat landscape. It highlights the need for organisations to be prepared for a variety of intimidation tactics beyond traditional cyber threats.

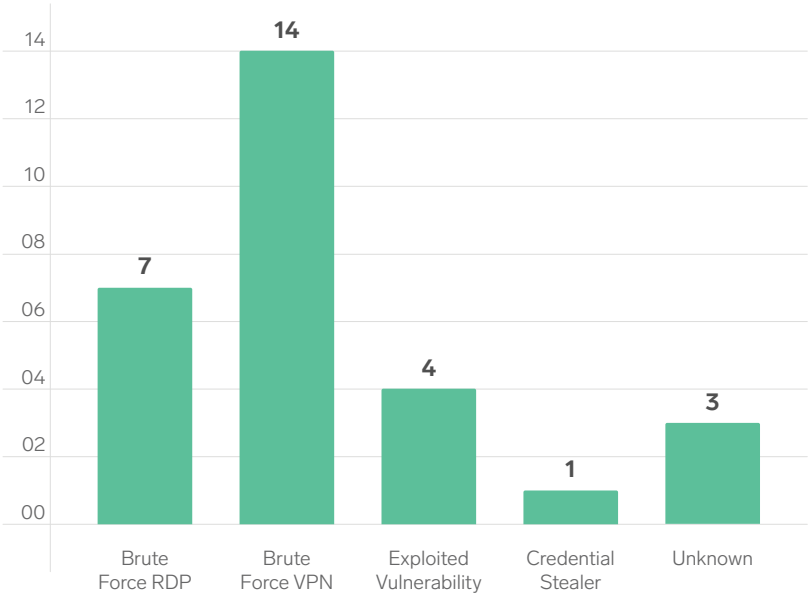
These direct pressure strategies are designed to create a sense of urgency and fear, aiming to force organisations into swift compliance with ransom demands.

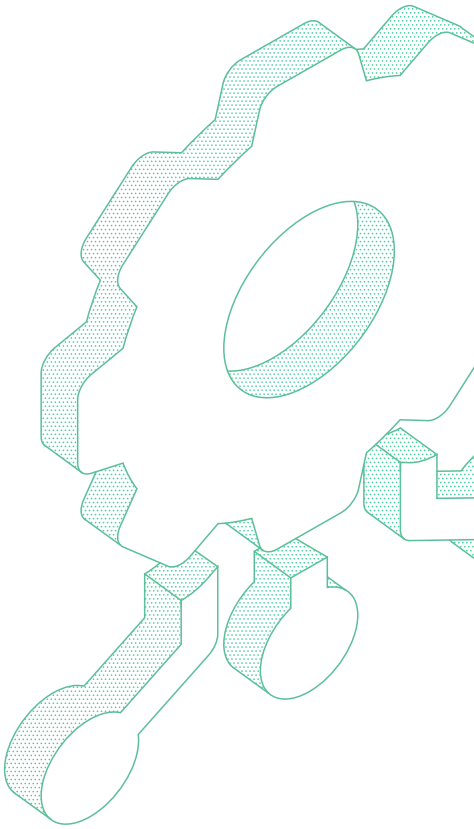
They reflect a broader trend of cybercriminals diversifying their methods to maximise their chances of success. As such, organisations must develop comprehensive response plans that address not only the technical aspects of a ransomware attack but also the psychological and social engineering tactics employed by Threat Actors.

These direct pressure strategies are designed to create a sense of urgency and fear, aiming to force organisations into swift compliance with ransom demands.



Initial Access





Over the 2023-24 financial year, Triskele Labs' Digital Forensics and Incident Response (DFIR) team identified key trends in cyber threats, particularly noting that brute force attacks on Virtual Private Networks (VPNs) and exposed RDP were the most exploited initial access vectors leading to ransomware incidents. This trend highlights that Threat Actors continue to prioritise easily exploitable targets.

When services such as VPNs and RDP are exposed to the internet without multi-factor authentication (MFA), they become prime targets for brute force attacks. These attacks are low in sophistication, making them accessible to less experienced Threat Actors. Moreover, potential targets are easily discoverable through public sources like Shodan.

Additionally, exploited vulnerabilities were another common tactic used by Threat Actors to gain initial access. The Triskele Labs DFIR team observed two distinct methods of vulnerability exploitation:

Mass Exploitation of New Vulnerabilities
Threat Actors quickly targeted critical vulnerabilities disclosed publicly, exploiting them before organisations could apply necessary patches.

Exploitation of Older Vulnerabilities
Even older, unpatched vulnerabilities remained attractive targets for Threat Actors seeking entry points into networks.

Credential stealers also played a significant role in providing initial access to victim environments. The DFIR team observed these malware types being installed on both corporate and personal devices, harvesting corporate credentials. These stolen credentials were then used to breach internet-facing services and gain unauthorised access.

To mitigate these threats, Triskele Labs DFIR recommends the following actions for organisations:

Review Exposed Hosts and Services
Regularly assess which hosts and services are exposed to the internet. Identify potential vulnerabilities and ensure that only necessary services are publicly accessible.

Enforce Multi-Factor Authentication
For any services requiring user authentication, implement and enforce MFA. This adds a crucial layer of security, making it significantly harder for Threat Actors to gain unauthorised access.

Stay Current with Patching
Keep up-to-date with vendor announcements and apply patches promptly. Critical vulnerabilities should be addressed immediately, even if it requires invoking emergency change procedures. This reduces the window of opportunity for Threat Actors to exploit these vulnerabilities.

Implement Robust Security Measures
Beyond patching and MFA, adopt comprehensive security measures such as network segmentation, regular security audits, and employee training programs to enhance overall cyber resilience.

By following these recommendations, organisations can significantly reduce their risk of falling victim to cyber incidents. The insights from Triskele Labs DFIR underscore the importance of proactive cybersecurity measures in protecting against the ever-evolving landscape of cyber threats. Prioritising security hygiene, staying vigilant with updates, and employing advanced authentication methods are essential steps in safeguarding organisational assets and data.

Data Exfiltration

During the 2023-24 financial year, the Digital Forensics and Incident Response (DFIR) team at Triskele Labs conducted 29 ransomware investigations.

Early identification of data exfiltration and the specific data involved is crucial for enabling stakeholders to prepare appropriately. This typically involves appointing legal counsel to navigate the legalities and obligations of notifiable data breaches.

Additionally, early detection allows the victim organisation to promptly notify impacted individuals, enabling them to take necessary precautions.

Out of the 29 ransomware engagements, evidence suggested that data exfiltration occurred in 19 cases, representing 65% of the total engagements.

Of these 19 cases, data from 9 organisations was listed on dark web leak sites, while an additional 2 were temporarily listed and then removed.

Forensic analysis revealed that an average of 406GB was exfiltrated during ransomware attacks, with an average of 78GB of data posted on dark web leak sites.

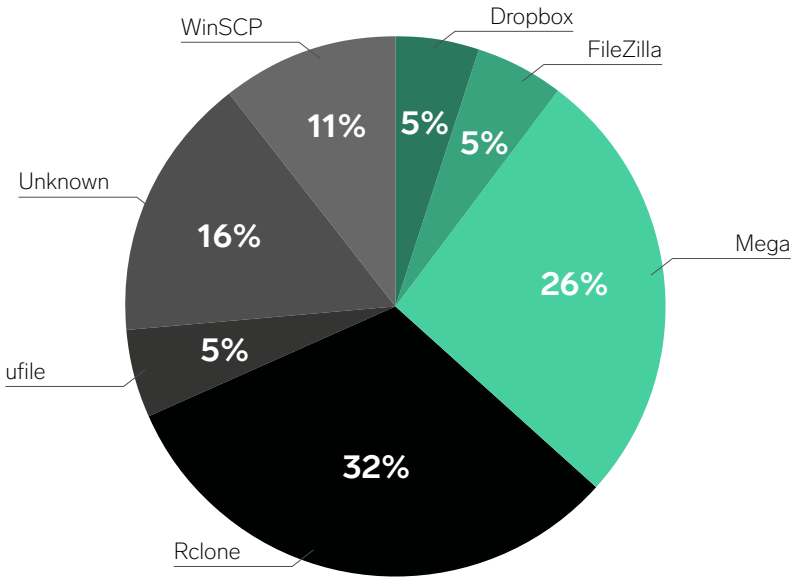
FTP was the most popular method for data exfiltration, with 50% of the engagements having evidence of data being exfiltrated via the FTP protocol.

Rclone was the most frequently used tool for data exfiltration, with other commonly used tools including FileZilla and WinSCP.

Additionally, 37% of cases involved Threat Actors exfiltrating data to popular file transfer sites such as Mega.co.nz, Dropbox, and UFile.

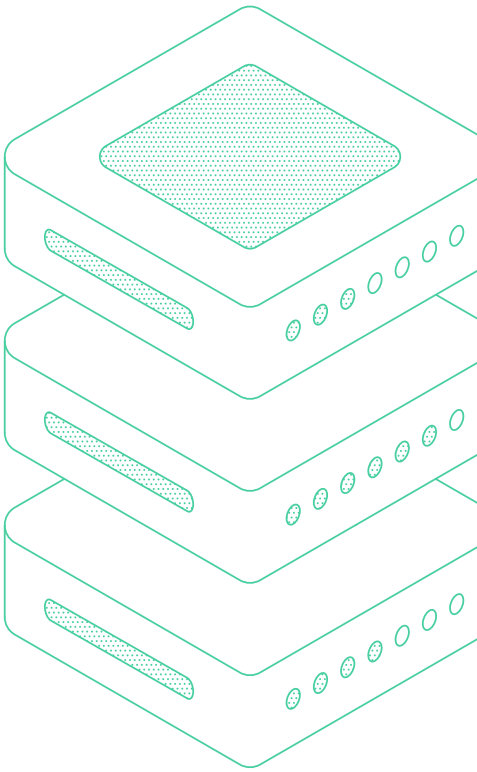
In 15% of cases, systems were fully encrypted, preventing analysis to determine the tools used by the Threat Actors.

Exfiltration Tools



During several engagements, Triskele Labs provided technical information to legal teams to aid in the takedown of Virtual Private Servers (VPS) used by Threat Actors to store exfiltrated data.

Data exfiltration occured in 65% cases, with an average of 406 GB exfiltrated during ransomware attacks.



Despite these successful takedowns, the exfiltrated data was often published on the Threat Actors' leak sites, either fully or partially. This indicates that Threat Actors typically maintain backups of the stolen data, making a single server takedown insufficient to prevent its publication. This underscores the need for comprehensive strategies beyond server takedowns to effectively mitigate the impact of data breaches.

The findings from these engagements underscore the importance of maintaining robust cybersecurity measures and timely detection capabilities.

Organisations must remain vigilant and proactive in addressing vulnerabilities and implementing comprehensive incident response strategies to mitigate the risks associated with ransomware attacks. This includes investing in advanced threat detection systems, regular security audits, and ongoing employee training to recognise and respond to potential threats.

Furthermore, organisations should develop and maintain comprehensive incident response plans that outline the steps to be taken in the event of a ransomware attack. This includes not only technical responses but also legal and communication strategies to manage the fallout from data breaches.

Ransom Payments

In 13% of the ransomware engagements undertaken by the Triskele Labs DFIR Team, the affected organisations decided to pay the ransom.

The average ransom payment was $115,000 USD. This marks a decrease from the previous 2022-23 financial year, when ransoms were paid in 14% of cases, with an average payment of $130,000 USD.

Paying the ransom is never the recommended way to resolve a ransomware attack. This approach encourages Threat Actors, funds their operations, and offers no guarantee of data recovery.

Despite these significant drawbacks, some organisations find themselves with no viable alternatives. In each case involving the Triskele Labs DFIR team, paying the ransom was the very last available option for victim organisations to regain access to their data.

These dire situations arose due to backups being compromised or deleted by the Threat Actors or not existing at all. The decision to pay the ransom is never taken lightly, as it involves not only a significant financial outlay but also potential legal and ethical ramifications.

The slight reduction in both the frequency and average amount of ransom payments suggests a possible improvement in organisational

Threat Actors typically maintain backups of the stolen data, making a single server takedown insufficient to prevent its publication.

resilience. More organisations may be adopting better preventive measures, such as regular backups and robust cybersecurity practices, thereby reducing their reliance on paying ransoms.

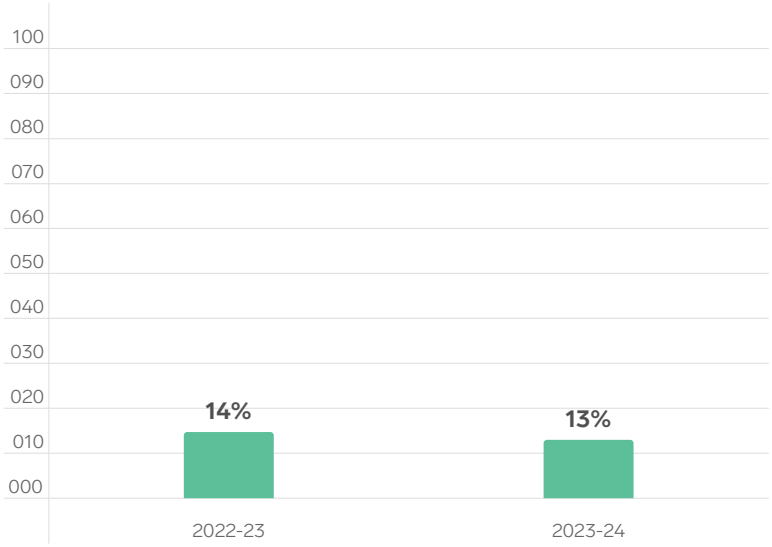
However, the persistent need to resort to ransom payments highlights the ongoing challenges organisations face in ensuring robust data protection and recovery strategies.

This trend underscores the critical importance of having secure, redundant backup systems and effective incident response plans to mitigate the impacts of ransomware attacks.

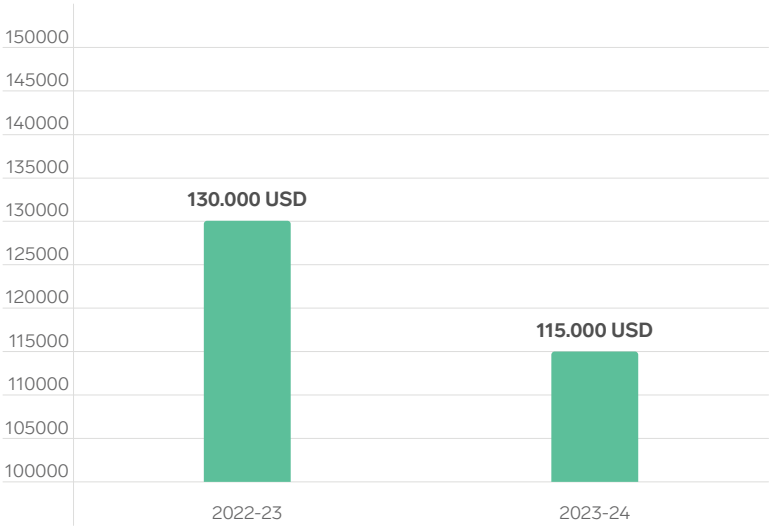
Organisations must invest in comprehensive cybersecurity strategies, including advanced threat detection, regular security audits, and continuous employee training. Ensuring that backups are not only frequent but also stored securely and independently from the main network is essential in preventing data loss.

These dire situations arose due to backups being compromised or deleted by the Threat Actors or not existing at all.

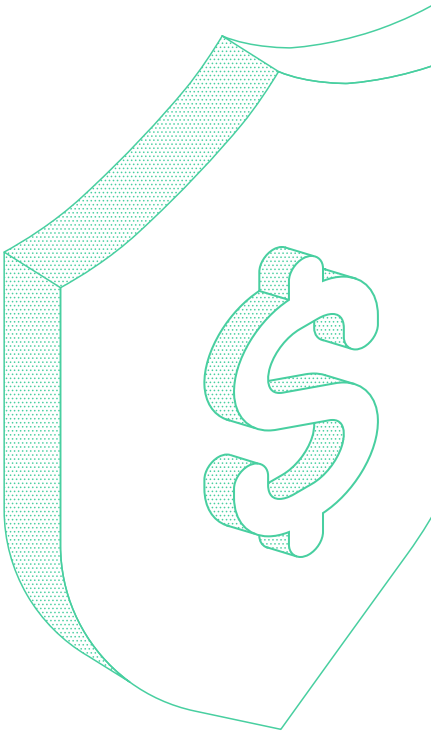
% of ransoms paid



Average ransom payment



Business Impact



The impact of a ransomware incident on businesses can be significant and far-reaching. Some organisations experience cascading failures, each exacerbating the overall impact, potentially leading to those organisations ceasing operations entirely.

The multifaceted effects of a ransomware attack touch on financial, reputational, and technological aspects, and the road to recovery can be prolonged and arduous.

Financial Impact

Operational downtime is one of the most immediate consequences of a ransomware attack, disrupting normal business operations. This disruption leads to significant financial losses due to halted production, missed sales, and delayed service delivery.

Recovery costs further add to the financial burden as victim organisations need to acquire new, clean infrastructure to rebuild their IT capabilities and restore data. This process often involves substantial expenditure on new hardware, software, and professional services for secure reconfiguration and data recovery.

Moreover, financial loss does not stop with operational and recovery costs. Staff employed by the organisation, as well as third-party suppliers, still need to be paid during the downtime. This ongoing financial commitment can strain resources, especially for smaller businesses with limited cash flow.

Additionally, organisations may face fines and legal costs associated with data breaches, particularly if sensitive customer information is compromised.

Reputational Damage

Reputational damage is another severe consequence of ransomware attacks. Breaches can erode the trust of customers, leading to a loss of existing clients and making it difficult to acquire new ones.

For service providers, customers may refuse to connect to the organisation's infrastructure until it has been validated as clean by external cybersecurity experts. This loss of confidence can have long-term implications, affecting customer loyalty and the company's market position.

Many ransomware groups exfiltrate data before deploying encryption as a secondary means of extorting payment. Even if organisations manage to recover from backups, the threat of public exposure of sensitive data looms large.

While ransomware groups often claim that they will not misuse the stolen data if paid, there is never a guarantee that the data will not be sold or leaked in the future. This uncertainty can further damage an organisation's reputation and erode customer trust.

Technological Impact

Technologically, a ransomware attack can cripple an organisation's IT infrastructure. Encrypting critical systems and data renders them unusable, forcing organisations to operate in a degraded state or halt operations entirely.

Recovery efforts may involve reinstalling operating systems, reconfiguring networks, and restoring data from backups—if backups are available and uncompromised.

Even if a ransom is paid to acquire decryption software, there is no guarantee that the decryptor will work reliably or at all.

Decryption tools provided by Threat Actors can be faulty, leading to incomplete recovery of files or further data corruption. This technological uncertainty complicates and extends the recovery process.

Operational Impact and Employee Wellbeing

The average return time to normal operations can take weeks, depending on the severity of the attack and the organisation's preparedness. During this period, business continuity is significantly affected, impacting revenue and strategic initiatives. The prolonged recovery time can also lead to operational bottlenecks and reduced efficiency.

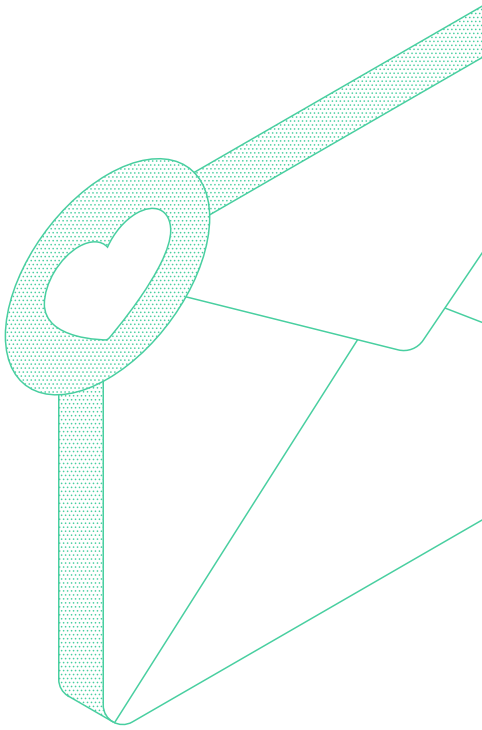
Furthermore, there is a risk to the wellbeing of employees during the response and recovery phases. Responders often work long hours with little rest, which can lead to burnout if not managed effectively. The stress and uncertainty caused by a ransomware attack can negatively affect morale and productivity, as employees worry about the stability of their jobs and the organisation's future.

The impacts of a ransomware attack on a business are extensive and multifaceted, affecting financial stability, reputation, technological infrastructure, and employee wellbeing. Organisations must prioritise robust cybersecurity measures, comprehensive incident response plans, and regular training to mitigate these risks and enhance their resilience against such attacks.

The stress and uncertainty caused by a ransomware attack can negatively affect morale and productivity, as employees worry about the stability of their jobs and the organisation's future.

Business Email Compromise

Business Email Compromise Overview



Business Email Compromise (BEC) incidents represented 46% of all incidents handled by Triskele Labs in the 2023-24 financial year. Although the operational impact of BEC incidents is generally less severe than that of ransomware attacks, the financial consequences can be substantial, especially when payment direction fraud is involved.

Understanding Business Email Compromise

A typical BEC incident begins with a Threat Actor gaining initial access to a cloud account, often through a phishing email. Once the Threat Actor has successfully infiltrated the account, they conduct thorough reconnaissance to understand the account owner's role within the business and identify any emails that could be leveraged for fraudulent activities.

BEC attackers are primarily financially motivated, seeking to perform payment redirection fraud. If they cannot achieve this with the compromised account, they will use it to send out additional phishing emails, aiming to capture credentials for other accounts and repeat the process.

Stages of a Business Email Compromise Attack

A BEC attack generally follows several stages:

Initial Access
The Threat Actor gains entry into the victim's email account, typically through a phishing email that deceives the user into providing their login credentials.

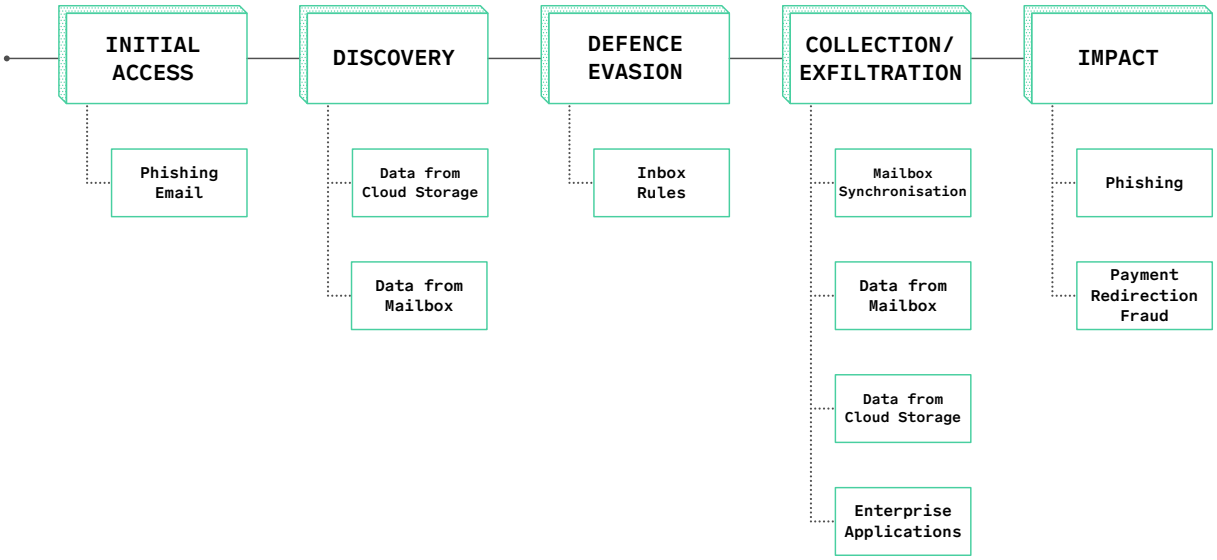
Discovery
After gaining access, the Threat Actor investigates the compromised account to understand the user's role and identify potential targets for exploitation, such as financial transactions or sensitive communications.

Defence Evasion
To avoid detection, the Threat Actor may alter email forwarding rules, delete alerts, or use other techniques to maintain access and avoid raising suspicion.

Collection/Exfiltration
The attacker collects valuable information, such as financial data or credentials, which can be used to perform fraudulent activities or sold on the dark web.

Impact
The final stage is the execution of the fraud, often involving payment redirection where legitimate financial transactions are diverted to accounts controlled by the Threat Actor, resulting in significant financial losses for the business.

By understanding the stages and potential impacts of BEC incidents, businesses can better appreciate the severity of this prevalent and financially damaging threat.



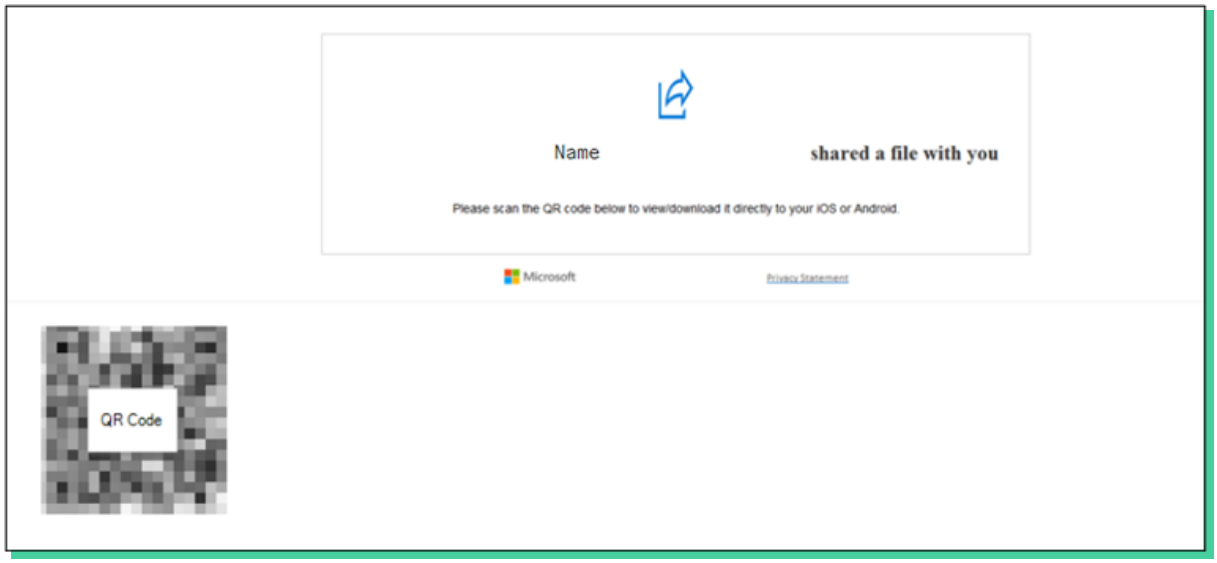
Initial Access Vectors

Phishing continues to be the primary method used by Threat Actors to gain initial access into cloud accounts during Business Email Compromise (BEC) attacks. The tactics and techniques employed in these phishing attempts can vary widely in their sophistication and delivery methods.

Common Phishing Techniques

Standard Phishing
Traditional phishing emails that deceive users into providing their login credentials. These emails often mimic legitimate communication from trusted entities, tricking recipients into clicking on malicious links or downloading harmful attachments.

QR Phishing
Although less common, QR phishing is a growing concern. In these attacks, Threat Actors embed malicious QR codes in emails or physical media. When scanned by a mobile device, these QR codes can bypass certain security controls and redirect users to credential-harvesting sites.



HTML Attachments
Some phishing emails include HTML attachments that, when opened, display convincing login forms designed to steal user credentials. These forms often closely resemble legitimate login pages, increasing the likelihood of success.

Evolving Phishing Sophistication

While the overall complexity of phishing emails has remained relatively consistent, the sophistication of the credential-harvesting techniques has significantly increased:

Advanced Credential Harvesters
Modern credential harvesters use advanced defence evasion techniques. For instance, they may redirect traffic away from known data centre IP ranges, such as those belonging to Microsoft or AWS, to avoid detection.

Captchas
Implementing captchas on phishing sites adds a layer of legitimacy and can thwart automated security tools from detecting the fraudulent activity.

Multiple Interactive Redirects
Some phishing schemes involve multiple redirects, making it more challenging for users and automated systems to identify the final malicious landing page. This increases the complexity of the attack and the difficulty of detection.

Impact of Advanced Tools

The advent of tools like ChatGPT has enabled Threat Actors to create more convincing and contextually accurate phishing emails.

These emails can be tailored to the target, using natural language processing to improve their effectiveness and likelihood of deceiving recipients.

In summary, while phishing remains the most prevalent initial access vector in BEC attacks, the methods and technologies employed by Threat Actors are continually evolving. This evolution underscores the importance of staying vigilant and implementing robust security measures to defend against these increasingly sophisticated threats.

Session Token Theft and MFA

As organisations have fortified their security measures, Threat Actors have adapted their techniques to gain access to accounts. Multi-Factor Authentication (MFA), once a robust defence against phishing attacks, is now being circumvented through a technique known as session token theft.

> **Multi-Factor Authentication (MFA), once a robust defence against phishing attacks, is now being circumvented through a technique known as session token theft.**

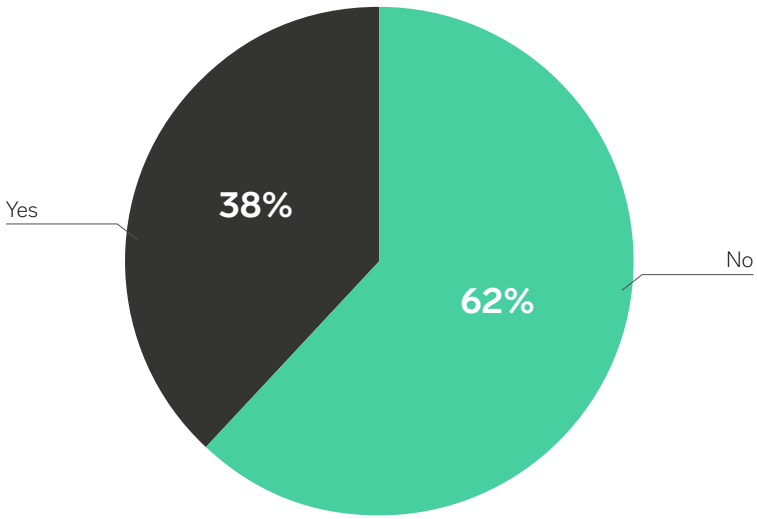
The Rise of Session Token Theft

Session token theft involves a Threat Actor gaining access to an authentication token used by an online service. These tokens are stored locally on a device and signal to the service that the user has recently authenticated, eliminating the need for repeated logins. By stealing these tokens, attackers can bypass MFA, gaining access to accounts without needing the second authentication factor.

Frequency and Impact

In recent compromises handled by Triskele Labs, it was noted that MFA was enabled in 19 out of 49 incidents. Despite this, attackers managed to bypass these protections, demonstrating the growing effectiveness of session token theft.

Multi-Factor Authentication Present



Techniques Employed by Threat Actors

Threat Actors often use man-in-the-middle attacks to steal session tokens. This method typically involves creating a malicious website that mimics a legitimate login page. Victims are directed to this site, usually via phishing emails, and upon logging in, their session token is transmitted to the Threat Actor's device. The attacker can then import this token into their browser, gaining full access to the victim's account.

An example scenario would include:

Phishing Email
A victim receives a convincing phishing email containing a link to a fake login page.

Login Attempt
The victim enters their credentials and completes the MFA process.

Token Capture
The session token, generated by the legitimate online service, is captured by the attacker's malicious website.

Unauthorised Access
The attacker uses the stolen token to access the victim's account without triggering MFA alerts.

Vulnerable MFA Methods

The MFA methods most susceptible to session token theft include:

- SMS: Easily intercepted or redirected.
- Voice Call: Can be intercepted or manipulated.
- Mobile Notifications: Prone to man-in-the-middle attacks.

Phishing-Resistant MFA

To mitigate these risks, organisations should consider adopting phishing-resistant MFA methods, such as FIDO 2.0 compliant devices, which offer stronger protection against token theft attacks.

Further Reading

For a comprehensive understanding of how session token theft is executed and defended against, Triskele Labs' Digital Forensics and Incident Response (DFIR) Team has recently released a detailed whitepaper[1]. This document outlines the methodologies used by

1 https://www.triskelelabs.com/understanding-token-theft

Threat Actors and provides actionable insights for enhancing security measures.

By staying informed about the latest threats and implementing advanced security protocols, organisations can better protect themselves against the evolving landscape of cyber threats.

Threat Actor Activity

During Business Email Compromise (BEC) incidents, Threat Actors employ various tactics to conceal their activities and exploit compromised accounts. One common technique is the creation of inbox rules designed to hide malicious actions and gather valuable information.

Inbox Rules for Concealment

Threat Actors create inbox rules to avoid detection and facilitate their activities within a compromised mailbox. These rules often move emails to rarely used folders like “Conversation History” or “RSS Feeds”, preventing the legitimate user from noticing the unauthorised activity.

The rules typically target specific email content or senders, enabling the Threat Actor to collect emails of interest, such as invoices or bank details, without raising suspicion.

```
New-InboxRule
-Name ..
-SubjectOrBodyContainsWords:
  → “spam”,
  → “hack”,
  → “change password”,
  → “postmaster”,
  → “undelivered”,
  → “bank”,
  → “invoice”,
  → “payment”
-MovetToFolder: “RSS Subscriptions”
-MarkAsRead: 1$True
-StopProcessingRules:$True
```

```
New-InboxRule
-Name …
-MovetToFolder: “Conversation History”
-MarkAsRead: $True
-StopProcessingRules:$True
```

In cases where the Threat Actor plans to send phishing emails from the compromised account, they may create additional inbox rules or modify existing ones to redirect all incoming emails.

This allows them to manage responses to the phishing emails, further concealing their presence and actions from the legitimate user of the compromised mailbox.

Average Dwell Time

The average dwell time, or the period between when Threat Actors obtain credentials and when they take action within the compromised mailbox, is on average 41 days. During this time, they gather information, identify email chains with payment information and/or invoices, and set up inbox rules to maximise their chances of success and minimise the risk of detection.

On average, it takes organisations 41 days to identify a BEC.

Challenges in Detection

Despite the implementation of security technologies, BEC incidents are rarely detected by these tools. Most organisations may enable Multi-Factor Authentication (MFA), but often fail to enforce it consistently or implement essential policies such as Conditional Access or Geoblocking. These oversights create vulnerabilities that Threat Actors can exploit, allowing them to bypass security measures and maintain access to compromised accounts.

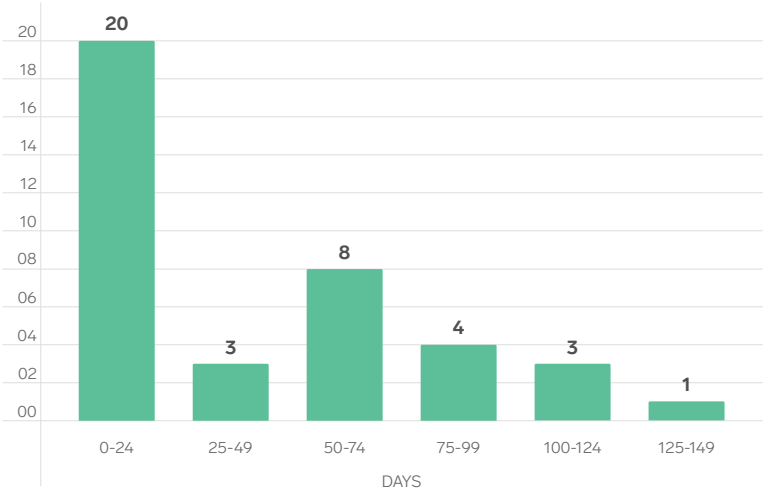
Time to Detect BEC

On average, it takes organisations 41 days to identify a BEC. The most common detection methods include:

Phishing Email
BECs are frequently identified when phishing emails are sent from an internal mailbox, prompting recipients to query the legitimacy of the communication.

Unpaid Invoices
Organisations may be alerted to a BEC when they receive notifications about unpaid invoices, indicating that payment redirection fraud has occurred.

The detection statistics highlight the challenges in identifying BECs promptly:



These figures underscore the importance of proactive monitoring and response strategies to reduce the dwell time and mitigate the impact of BECs. Understanding Threat Actor tactics and enhancing detection capabilities are critical steps in defending against these sophisticated attacks.

Payment Redirection Fraud

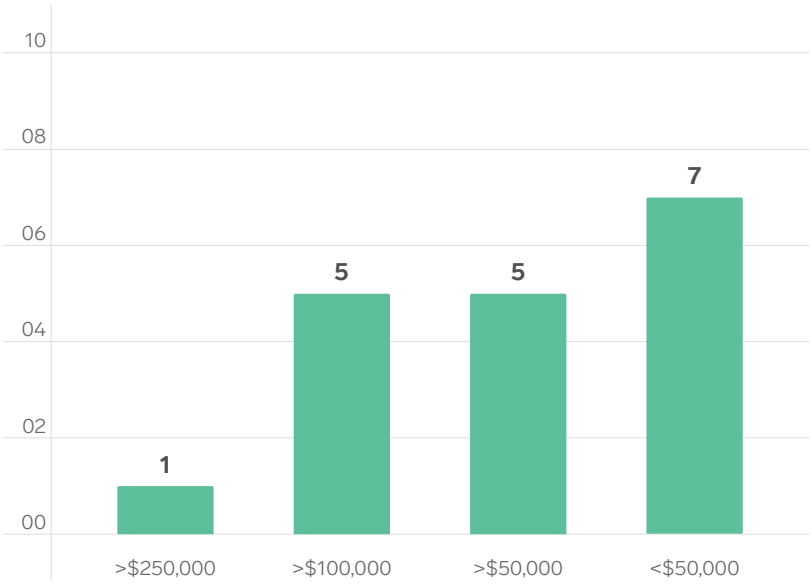
Payment Redirection Fraud is a sophisticated technique used by Threat Actors during Business Email Compromise (BEC) incidents. This type of fraud involves diverting legitimate financial transactions to accounts controlled by the attacker. By gaining access to a company's email system, Threat Actors can manipulate emails and payment instructions, leading to significant financial losses.

In the past 12 months, Triskele Labs has observed 18 instances of attempted and successful payment redirection fraud across various incidents. The amounts ranged from $3,300 to $530,000. The majority of these incidents involved payments of less than $50,000.

The financial impact of these incidents for the fiscal year 2023-24 was substantial, with a total of $1,673,857 included within the payment redirection fraud attempts. The average amount per incident was approximately $99,997. To better understand the scale of these frauds, the amounts were categorised into four sections:

- More than $250,000
- More than $100,000
- More than $50,000
- Less than $50,000

Payment Redirection Fraud Amount



The average amount per incident was approximately $99,997.

How Payment Redirection Fraud Occurs

Threat Actors typically begin by gaining access to a company's email system through phishing or other social engineering techniques. Once inside, they monitor communications to identify upcoming financial transactions. They then manipulate payment instructions by altering invoices or sending deceptive emails that redirect payments to their own accounts.

For example, a Threat Actor might intercept an email containing an invoice and change the bank account details to one they control. The unsuspecting company then transfers funds to the fraudulent account, believing they are paying a legitimate invoice.

The Impact of Payment Redirection Fraud

The financial consequences of payment redirection fraud can be devastating, especially for small and medium-sized businesses. In addition to the immediate financial loss, companies may face reputational damage, strained vendor relationships, and increased scrutiny from regulatory bodies.

The increasing prevalence of payment redirection fraud underscores the need for robust security measures and vigilance in handling financial communications. Organisations must implement multi-factor authentication, employee training, and stringent verification processes to mitigate the risk of such fraud.

Conclusion

The Triskele Labs DFIR team has observed a continuous rise in cyber incidents, with no signs of slowing down. Business Email Compromise (BEC) remains the most prevalent incident type, accounting for 46% of all cases, followed closely by ransomware incidents at 27%. The finance and healthcare industries were the most impacted, both comprising 32% of the incidents.

Ransomware and Remote Access Vulnerabilities

Ransomware groups frequently exploit Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) connections that lack Multi-Factor Authentication (MFA). The shift to remote work due to COVID-19 led many companies to hastily implement remote access solutions without adequate security measures. Consequently, Threat Actors found it easier to breach environments, with 65% of ransomware incidents involving data exfiltration. These groups often employ double and triple extortion tactics to maximise their financial gains.

BEC and Phishing Tactics

BEC attacks predominantly occur through phishing emails, exploiting the general lack of phishing awareness among employees. Threat Actors use these emails to steal user session tokens, effectively bypassing most MFA methods. Once inside an email environment, their primary goals are to distribute more phishing emails and perform invoice redirection fraud.

Mitigating Risks: People, Processes, and Technologies

Organisations can mitigate the risk of cyber compromise by focusing on three key areas: people, processes, and technologies.

People

- Investing in security training and awareness programs empowers employees to recognise and respond to potential threats.
- Cultivating a strong security culture ensures that staff know how to report incidents and prioritise data protection.
- Ensuring that the appropriately trained people are monitoring an environment.

Processes

- Developing robust processes, such as confirming payment details via phone calls, can protect against payment redirection fraud.
- Establishing comprehensive cyber incident response plans prepares organisations for effective action before, during, and after an incident.
- Ensure that the organisation has a patching process to mitigate vulnerabilities.

Technologies

- Identifying specific needs (e.g., backup solutions, malware detection) helps in selecting appropriate technologies.
- Essential technologies include backup systems, Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) and a Vulnerability Management Platform.

By addressing these areas, organisations can significantly enhance their security posture and reduce the risk of cyber incidents.

Triskele Labs

1300 24 CYBER
Level 16 Queen & Collins Tower
380 Collins St Melbourne VIC Australia
info@triskelelabs.com

triskelelabs.com