

# Monthly Cyber Threat Intelligence Report

---

July 2024



# Contents

<b>1</b>	<b>Top Breach of the Month: Synnovis Cyber-Attack on the UK NHS</b>	<b>03</b>
<b>2</b>	<b>Updates on Ongoing Recent Breaches</b>	<b>05</b>
<b>3</b>	<b>Cyber security In Brief</b>	<b>06</b>
<b>4</b>	<b>Deep dive into a Threat Actor: ShinyHunters (or ShinyCorp)</b>	<b>09</b>
<b>5</b>	<b>Summary</b>	<b>12</b>

Welcome to our latest edition of the Monthly Cyber Threat Intelligence Report.

This month, we're discussing the recent cyber-attack on the UK NHS, a breach through a third party that resulted in the publication of sensitive data online and invalidated patient test data. We'll dissect what happened, who was affected, and the lessons we can draw from this incident.

We'll also provide updates on ongoing breaches and other notable cyber security stories and updates. Finally, we'll take a deep dive into the tactics of a well-known threat actor, offering insights to help you fortify your defences.

## Top Breach of the Month

### Synnovis Cyber-Attack on the UK NHS

On June 3, 2024, Synnovis, a major diagnostics and health data service provider for the UK's National Health Service (NHS), suffered a devastating cyber-attack. The attackers exploited Synnovis' network infrastructure vulnerability to gain unauthorised access to sensitive data. The breach remained undetected for several weeks, and on June 27, the stolen data was published on the dark web, exposing patient records, diagnostic results, and other confidential health information.



In response to the breach, Synnovis and the NHS have been working closely with cyber security experts and law enforcement agencies to contain the incident and prevent further damage. Emergency measures have been implemented, including enhanced network monitoring, additional security controls, and comprehensive vulnerability assessments.

As of June 2024, the hacking group which perpetrated this attack is still being determined, and no one has come forward to take responsibility.



#### Who was impacted?

The breach affected millions of NHS patients whose data was handled by Synnovis. This included personal information such as names, addresses, contact details, medical records, test results, and diagnostic information. The exposure of this sensitive information has serious implications for patient privacy and security.



### Lessons learnt

**Third-Party Risk Management:** This incident underscores the critical need for robust security measures when dealing with third-party vendors, especially those handling sensitive data.



### Vulnerability Management

The exploitation of a network vulnerability highlights the importance of regular vulnerability assessments and timely patch management.



### Enhanced Cyber Resilience

The delay in detecting the breach highlights potential weaknesses in Synnovis and the NHS's cyber resilience, particularly concerning their monitoring and incident response capability.

## Recommendations

#### Strengthen Third-Party Security

Implement stringent security requirements and regular audits for third-party vendors to ensure they adhere to best practices and are equipped to protect sensitive data.

#### Regular Vulnerability Assessments

For outsourced security services, ensure regular vulnerability scans, tabletop exercises and penetration testing are integral to the service. If security is managed internally, frequent vulnerability scans, tabletop exercises and penetration tests should be conducted to identify and address security weaknesses promptly. These measures are essential for maintaining an effective cyber security posture.

#### Enhanced Monitoring and Detection

Deploy advanced monitoring tools and anomaly detection systems to identify suspicious activities early and respond swiftly to potential breaches.

#### Data Encryption

Ensure sensitive data is encrypted both in transit and at rest to protect it from unauthorised access and exfiltration.

#### Advanced Threat Protection

Integrating technologies, including AI-based anomaly detection, endpoint detection and response (EDR), and threat intelligence strengthens cyber resilience. This capability ensures that threats are detected and responded to immediately, crucial for preventing malicious activity and maintaining system integrity and availability.

#### Incident Response Preparedness

Develop and regularly update incident response plans, conduct tabletop exercises, and ensure all staff are trained to respond effectively to cyber incidents.

# Updates on Ongoing Recent Breaches

## MoveIT Breach

The MoveIT breach, which we have previously covered and initially reported in March 2024, continues to have widespread implications. For those who may have missed our previous updates, let's recap. MoveIT, a widely used file transfer service, was found to have a zero-day vulnerability actively exploited by threat actors. The attackers leveraged this vulnerability to infiltrate the networks of multiple organisations, leading to data theft and ransomware attacks.



In June 2024, NIST published details of the vulnerabilities exploited in this attack: CVE-2024-5805 and CVE-2024-5806. These vulnerabilities allowed attackers to bypass secure file transfer protocol (SFTP) authentication in the MOVEit Transfer file transfer software, granting unauthorised access to sensitive data.

### Why is this significant?

As of June 2024, and in light of the latest related MoveIT CVE, the breach has affected over 2,000 organisations, including the US Department of Health, IBM, Cognizant and various financial institutions, compromising sensitive data from millions of individuals. The CIOp ransomware group, known for its previous exploits, is believed to be behind these attacks.

Since the attack, researchers have seen active usage of these exploits in the wild, highlighting the urgency for organisations affected by these CVEs to apply patches immediately.

## Recommendations

Progress Software, the developer of MOVEit, has issued patches to address these issues. Organisations using MOVEit Transfer are strongly advised to apply the latest patches and implement additional security measures to protect against further exploitation. In addition, it is crucial to:

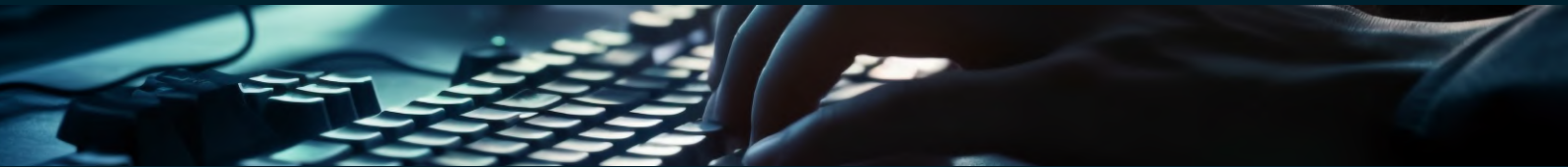
- **Ensure** all software and systems are updated with the latest patches and updates as soon as possible after release.
- **Implement** stringent vendor risk management practices to assess and mitigate risks associated with third-party services.
- **Strengthen** incident response plans to quickly address breaches involving third-party services and conduct regular drills to ensure preparedness.

# Cyber security In Brief

## Ticketmaster cyber security breach

Discovered in June 2024, the attack involved unauthorised access to a database containing sensitive customer data, including names, email addresses, and payment information. The breach was attributed to the notorious ShinyHunters hacking group, which exploited leveraged data from their attack on Snowflake to gain access to Ticketmaster's security infrastructure with stolen credentials.

The breach is significant due to the scale and sensitivity of the data involved. It highlights the vulnerabilities within large-scale digital platforms and the increasing sophistication of criminals. Ticketmaster, a well-known company that manages high-volume personal and financial data, was breached using data stolen in a third-party breach, which underscores the importance of continued security assessment and monitoring, not only of direct business but also of the supply chain, to ensure their cyber security posture matches your own. \*



## Crypto Phishing, which leveraged compromised mailer service

In January 2024, attackers compromised the email provider MailerLite to execute a phishing campaign targeting cryptocurrency users, resulting in the theft of over \$580,000 of cryptocurrency. The attackers utilised official email addresses from major Web3 companies such as Cointelegraph, WalletConnect, and Token Terminal to send phishing emails containing links to fake airdrop announcements. When clicked, the links directed victims to phishing sites to steal their cryptocurrency.

Investigation showed that the MailerLite servers were compromised, which allowed attackers to send emails that appeared authentic, bypassing typical phishing detection measures. The attackers leveraged a widespread service provider, amplifying their campaign's reach and potential impact across multiple platforms and users in the cryptocurrency community.

This attack is significant because it appeared to use legitimate email addresses from well-known companies, increasing the credibility of phishing emails and the likelihood of users falling victim.

Since the attack, several companies, including De.Fi, have moved their databases to other providers, where they are better assured of user data safety. The attack is ongoing, and companies affected, including WalledConnect and CoinTelegraph, have issued public statements advising ongoing vigilance. \*\*

\* Reference: <https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/>  
<https://www.bbc.co.uk/news/articles/c899pz84d8zo>

\*\* Reference: <https://cointelegraph.com/news/coordinated-crypto-investor-phishing-campaign-email-alert>

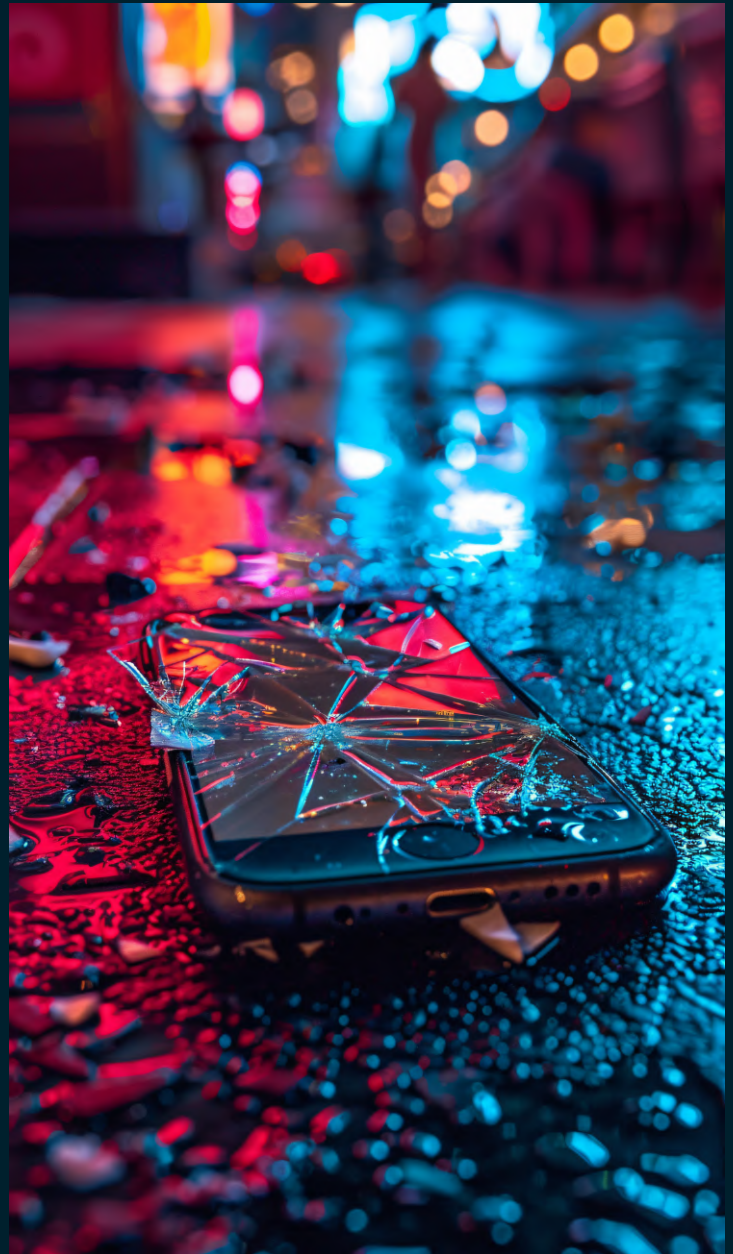
## T-Mobile Data Breach: What, Why and Who Was Impacted

T-Mobile recently experienced a significant data breach that compromised the personal information of 37 million customers. The breach involved unauthorised access to customer data, including names, addresses, and phone numbers. The breach was caused by a vulnerability in T-Mobile's network, allowing attackers to gather customer data without detection for an extended period.

The nature and scale of this breach make it particularly significant. With millions of customers affected, exposing sensitive information such as names, addresses, and phone numbers presents a substantial risk of identity theft and fraud.

Although this breach occurred late in 2023, the impact is ongoing. It's the latest in a series of breaches at T-Mobile that have damaged the provider's reputation and raised concerns over its cyber security practice. As recently as January 2024, IntelBroker claimed to have gained access to T-Mobile and posted screenshots—although some claim that these are old information.

This incident has pressured other telecommunication providers to review security measures to prevent similar breaches. We also see calls for tighter enforcement around existing regulations to ensure that companies demonstrate continued investment and enhancement in cyber security infrastructure to ensure compliance.



Overall, this incident underscores the critical need for organisations to implement a continuously improving cyber resilience program to ensure the fastest detection and immediate response against threats.

## What can we learn from these breaches and attacks?

As we look at these breaches, a lot can be learned; not every recommendation is relevant to every organisation – but there's always something new that we can investigate, which could become useful one day. The following bullets, in addition to those from the Synnovis section above, are considerations across all the breaches in this section:



### Adopt a Cyber Resilience Program

Develop and maintain a proactive cyber security strategy that includes employee training, threat detection systems, and incident response plans.

Access Controls: Implement strict access controls, including multi-factor authentication (MFA) and role-based access on all accounts, and limit sensitive data and systems access.



### Employee Training

Conduct regular training sessions to educate employees on recognising phishing attempts and social engineering tactics. Users should be cautious when receiving emails that appear to offer free tokens or airdrops. Always verify the authenticity of such communications using official channels.



### Change Passwords Regularly

For this audience, this goes without saying. But a gentle reminder is always beneficial, if not for you but for your colleagues.



### Ongoing Enhancements to Security Measures

As threats change, our security measures should change with them. An agile approach to cyber security allows for continuous strengthening of aspects such as email protocols and supply chain security measures. Internally, agility can be difficult due to a multitude of factors, and this is an area where hybrid or outsourcing cyber solutions can be beneficial.

# Deep dive into a Threat Actor: ShinyHunters (or ShinyCorp)

ShinyHunters is a notorious criminal group that emerged in 2020 and has since established itself as a prominent player in the underground hacking community. Known for its aggressive data breaches and sale of stolen data on dark web marketplaces, the group operates with business-like efficiency, targeting large databases from high-profile companies. Their activities have led to substantial financial and reputational damage to numerous organisations globally.

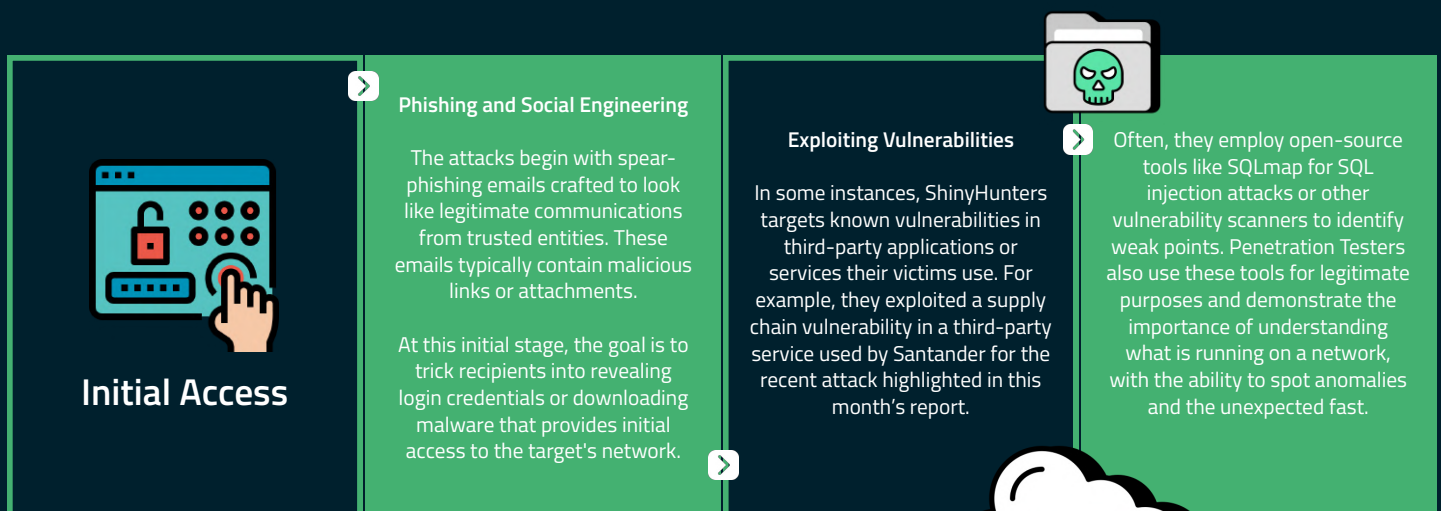
ShinyHunters' recent activities, particularly their involvement in the Snowflake breaches affecting major companies, underscore the group's evolving tactics. Their capability to exploit vulnerabilities in third-party services and cloud platforms has led to widespread data exfiltration, a serious concern. The attacks on Santander and TicketMaster compromised sensitive customer information, disrupted operations, and will have eroded trust in these organisations.

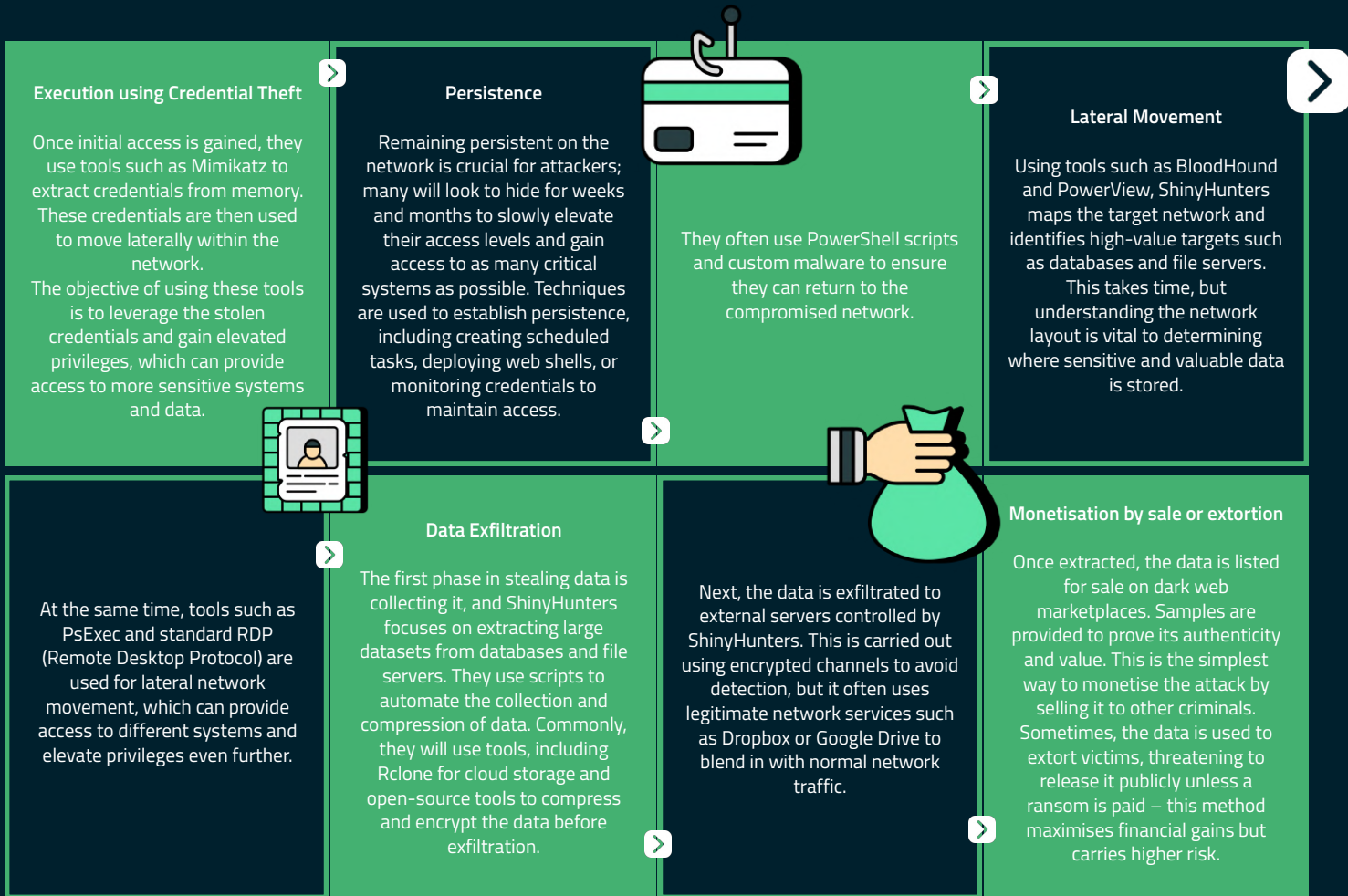


## TTPs They Are Known to Use and What They Are Known For

ShinyHunters is infamous for employing sophisticated tactics, techniques, and procedures (TTPs) to breach security defences and exfiltrate data.

Here's a breakdown of a typical ShinyHunters attack:





## Who They're Actively Targeting

ShinyHunters' targets are diverse, spanning multiple industries. They have a particular focus on sectors where large databases of personal and financial information can be accessed, including:



### Financial Service

The recent Santander breach highlighted their interest in financial institutions.



### E-commerce and Technology

Companies like Microsoft and Tokopedia have fallen victim to their attacks, indicating a focus on firms with substantial user bases and valuable data.



### Healthcare

Although less publicised, there are indications that healthcare organisations are also at risk due to the high value of medical data.

## Recommendations for detection and mitigation

Organisations can act based on lessons learned from ShinyHunters' attack strategies to enhance cyber security resilience and prevent the spread of breaches.



Comprehensive vulnerability management and proactive network monitoring are crucial in maintaining system security and spotting when malicious scanning tools could be used on the network.



Continuous vulnerability assessments and timely patch management help ensure that systems and third-party services remain secure and reduce potential exposure to zero-day threats or active CVE usage in the wild.



Advanced intrusion detection systems (IDS) and endpoint detection and response (EDR) monitor network traffic to identify unusual activities indicative of a breach, including unusual authentication patterns or data transfers.



Encrypting sensitive data at rest and in transit, with strict access controls and multi-factor authentication (MFA), protects critical information.

By integrating these measures and setting up alerts for suspicious behaviours, organisations can quickly respond to potential threats, mitigating the impact and preventing the spread of breaches initiated by sophisticated threat actors.

If you would like to discuss how e2e-assure can help to develop a cyber resilient approach to security, don't hesitate to contact us at [cti@e2e-assure.com](mailto:cti@e2e-assure.com). One of our team will assist you.



## Let's connect!

That concludes this month's edition of our cyber security newsletter. We hope you found the insights and updates in this report useful.

Stay tuned for next month's newsletter, where we will bring you the latest developments, in-depth analyses, and expert advice to help you stay ahead in cyber security. We can't wait to share more with you. Until then, remain vigilant and proactive in your defence strategies.

We always look for ways to improve and would love your feedback. Your suggestions and the topics you want us to cover in future editions are important. Please email us at [cti@e2e-assure.com](mailto:cti@e2e-assure.com)