



| Flash |

ShinyHunters: An Insight into Future Extortion Tactics?

F-2024-06-07a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Deep and Dark Web, Data Leak, Threat Actor

June 7, 2024

Scope Note: ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on June 7, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | ShinyHunters: An Insight into Future Extortion Tactics?

› Key Findings

- Threat actors have allegedly stolen the data of an unknown number of organizations via an alleged compromise of the cloud data platform Snowflake. ZeroFox cannot yet independently confirm or deny the extent to which Snowflake is involved or how the alleged accessing of a demo environment could lead to the breach of multiple downstream customers.
- To date, at least three organizations are alleged to be victims of this breach, with data being sold in deep and dark web (DDW) forums. ZeroFox anticipates there is a likely chance that other as-yet-unnamed organizations have also had data leaked but may have chosen to buy back their data, or threat actors have yet to list it.
- The alleged breach of the cloud data platform Snowflake and subsequent sale of data from alleged customers may provide threat actors with a blueprint for the development of digital extortion tactics in the near future.
- The omission of encrypting payloads from extortion attacks will likely become increasingly popular amongst established extortion collectives—and will likely facilitate a larger pool of threat actors not historically involved in extortion to enter the digital extortion space.

The Alleged Snowflake Breach

Threat actors have allegedly stolen the data of an unknown number of organizations via a compromise of the cloud data platform Snowflake. ZeroFox cannot yet independently confirm or deny the extent to which Snowflake is involved or how the alleged accessing of a demo environment could lead to the breach of multiple downstream customers. ZeroFox can also neither independently confirm nor deny claims made by Hudson Rock in an article that a CSV file was shared with them listing victims.¹ This article has since been taken down, reportedly following a formal legal notice filed by Snowflake. ZeroFox has not identified a copy of this CSV file.

On May 23, 2024, U.S.-based cloud computing company Snowflake announced its observation of potential unauthorized network access that had occurred over previous weeks.² The organization's statements assert that threat actors obtained access via credentials belonging to current or former employees that had not implemented multi-factor authentication (MFA).³ This would be an unusual initial access vector to breach an organization of this size.

Snowflake identified evidence of unauthorized access to a demo account belonging to a former Snowflake employee. Snowflake claimed the demo account did not contain sensitive data or customer data. The demo account was allegedly not protected by Okta or MFA, unlike Snowflake's corporate and production systems. Snowflake claims this is a targeted campaign aimed at users with single factor authentication and has issued a summary and recommendations.

To date, at least three organizations are alleged to be victims of this breach, with data being sold in DDW forums. ZeroFox anticipates there is a likely chance that other as-yet-unnamed organizations have also had data leaked but may have chosen to buy back their data, or threat actors have yet to list it.

¹ [hXXps://www.linkedin\[.\]com/pulse/snowflake-breach-deep-dive-data-heist-xqmsg-0snic?trk=public_post](https://www.linkedin.com/pulse/snowflake-breach-deep-dive-data-heist-xqmsg-0snic?trk=public_post)

² [hXXps://www.secureworld\[.\]io/industry-news/snowflake-data-breach](https://www.secureworld.io/industry-news/snowflake-data-breach)

³

[hXXps://community.snowflake\[.\]com/s/question/0D5VI00000EymI00AB/detecting-and-preventing-unauthorized-user-access](https://community.snowflake.com/s/question/0D5VI00000EymI00AB/detecting-and-preventing-unauthorized-user-access)

| Details

The alleged breach of the cloud data platform Snowflake and the subsequent sale of data from alleged customers may provide threat actors with a blueprint for the development of digital extortion tactics in the near future. Although presented as a typical data breach and sale of data, the incident likely represents an atypical digital extortion attempt aimed at pressuring Snowflake and its impacted customers into buying back their data before it can be purchased by other interested parties. The advertisement of victims' data is most likely intended to serve as proof of authenticity and is unlikely to represent a realistic attempt to attract buyers from the broader threat actor community due to:

- Information disclosed about the nature of the initial access;
- Alleged initial approaches to victims to purchase their stolen data;
- The exceptionally high cost of the data for sale;
- The likely use of threat actor burner accounts to sell access; and
- The nature of the particular forums used to advertise the data.

The incident bears many of the hallmarks of a traditional ransomware attack, with the exception of the deployment of encrypting payloads and privately held negotiations. The reported prices set for the purchase of the victims' data are almost certainly exorbitant and surpass the financial expectations for a sale of this type of data. This is very likely indicative of the victims being the intended buyers rather than other interested parties found in DDW forums. BreachForums is known to be dominated by threat actors that typically purchase for lower amounts and is an unlikely forum to be used for exceptionally high-value data sales to the wider threat actor community. This therefore represents a form of digital extortion; the actor likely aims to generate media attention in order to exacerbate pressure on the victims to buy back their own data before other threat actors purchase it.

- Traditionally, ransomware and digital extortion (R&DE) collectives deploy malicious ransomware strains that encrypt victims' files and servers. In recent years, this encryption has been ubiquitously coupled with sensitive data exfiltration, which is held to ransom under threat of public release. This is known as double extortion.

- However, some R&DE collectives have moved away from deploying payloads that encrypt victims' servers and files. In the alleged breach of Snowflake, there is no evidence to suggest threat actors used malicious code to encrypt the victim's files. Instead threat actors exfiltrated sensitive data.
- This is very likely due to the potential unreliability in the code executing effectively and the higher chance of victims enacting defensive measures. Additionally, with the ubiquity of double extortion tactics, threats of data disclosure are very likely perceived by threat actors as more of an incentive to pay ransoms than the disruption caused by encrypted files.

Parallels with Clop's 2023 Extortion Activity

During 2023, threat group Clop conducted two R&DE campaigns targeting managed file transfer (MFT) solutions companies GoAnywhere and MoveIt.⁴⁵ The exploitation of two zero-day vulnerabilities led to the subsequent theft of downstream customer data belonging to numerous victim organizations and resulted in Clop being the third-most prolific R&DE collective of 2023.⁶ These are widely regarded as two of the most successful extortion campaigns in recent years.

- Similarly to the recent ShinyHunters data breach, Clop omitted the use of encrypting ransomware against its victims, instead opting to exfiltrate the data before serving a ransom demand. This is likely perceived by R&DE threat groups as a lower-risk approach.
- Clop also exhibited extortion tactics very likely similar to those observed being used by ShinyHunters, whereby stolen information is partly leaked.
- Like Clop, ShinyHunters successfully targeted an organization that was almost certainly perceived to be in possession of data belonging to numerous client companies. This was almost certainly a deliberate choice of victim based on the large potential financial payoff of extorting numerous organizations.

⁴ [hXXps://www.infosecurityeurope\[.\]com/en-gb/blog/threat-vectors/what-to-know-moveit-hack.html](https://www.infosecurityeurope[.]com/en-gb/blog/threat-vectors/what-to-know-moveit-hack.html)

⁵ [hXXps://www.scmagazine\[.\]com/news/ransomware-gang-clop-zero-day-moveit-2021](https://www.scmagazine[.]com/news/ransomware-gang-clop-zero-day-moveit-2021)

⁶ [hXXps://www.blackfog\[.\]com/the-top-10-ransomware-groups-of-2023/](https://www.blackfog[.]com/the-top-10-ransomware-groups-of-2023/)

Each of the data breaches for sale allegedly resulting from Snowflake customers has been posted by threat actors operating three distinct handles. These actors are all likely non-Russian speakers and are most likely to be English-speaking.

Seller Handles	Details
ShinyHunters	- On May 29, 2024, advertised the data stolen from Ticketmaster in BreachForums for a cost of USD 500,000.⁷ - An English-speaking black hat threat group that has been operational within DDW forums for a significant length of time, carrying an established, albeit controversial, reputation. - Since its formation, has specialized in financially-motivated activity such as data breaches targeting numerous high-profile organizations. - Has previously fulfilled senior roles within BreachForums. - Since BreachForums disruption in May 2024, other threat actors are speculating that ShinyHunters is cooperating with unknown law enforcement (LE) entities in an unspecified capacity.
whitewarlock	- Untested threat actor with alias registered in the Exploit forum on May 24, 2024. No activity is associated with this account prior to this data leak. - Advertised the sale of data allegedly stolen from a Europe-based financial organization for USD 2 million. - ZeroFox assesses this is most likely a burner account for a well-established threat actor that typically operates under a different username.
Sp1d3r	- Untested threat actor with alias registered in the Exploit forum on May 30, 2024. No activity is associated with this account prior to this data leak. - Advertised the sale of data allegedly stolen from a U.S.-based automotive parts organization for USD 1.5 million. - ZeroFox assesses this is most likely a burner account for a well-established threat actor that typically operates under a different username.

⁷

[hXXps://www.reuters\[.\]com/technology/cybersecurity/live-nation-probing-ticketmaster-hack-amid-user-data-leak-concerns-2024-06-01/](https://www.reuters.com/technology/cybersecurity/live-nation-probing-ticketmaster-hack-amid-user-data-leak-concerns-2024-06-01/)

The alleged Snowflake breach was most likely conducted by a single, coordinated threat collective identical to—or associated with—ShinyHunters. The implication of multiple aliases in a single data breach would likely be an attempt to minimize the chances of exacerbating ongoing LE scrutiny.

ShinyHunters posted versions of both whitewarlock's and Sp1d3r's data breach advertisements on BreachForums very soon after the original posts leveraging almost identical text. If reporting is true that access was obtained via credentials (and given the nature of the data sales and the history of these accounts), it is very unlikely the three threat actors described above are operating independently from each other.

- It is very unlikely multiple distinct or uncoordinated actors obtained credentials for Snowflake at or around the same time and are conducting very similar post-intrusion activity but are not working together.
- This is supported by the sellers' profiles bearing many of the hallmarks of burner accounts for actors that operate well-established handles elsewhere but want to maintain operational security/anonymity for these particular sales. This is likely to be an attempt to avoid the wrath of LE, especially given ShinyHunters operates the recently disrupted and relaunched BreachForums.
- There are very few identified instances of numerous, uncoordinated actors compromising the same victim via obtained credentials for data breaches at the same time. Typically, multiple actors compromising a victim at the same time is only seen in cases of CVE or zero-day disclosures.

BreachForums Disruption

On May 15, 2024, the popular English-speaking DDW forum and marketplace BreachForums was seized by LE agencies in an operation coordinated by multiple international agencies.⁸ According to a statement by ShinyHunters (senior figures in the BreachForums operation), this resulted in the seizure of digital infrastructure and the arrest of former BreachForums moderator, “Baphomet”, by LE.

Previous users of BreachForms began to announce “successor” forums, such as actor “USDoD”’s launching of Breach Nation. However, within two weeks, ShinyHunters announced that the [.]st BreachForums domain was back online, alongside a new DDW domain.⁹

Since its relaunch, rumors have circulated within DDW communities that this new BreachForums site is a honeypot set up for LE entrapment, claims that ZeroFox can neither confirm nor deny. BreachForums administrators are observed exhibiting behavior atypical of DDW forums, including banning new registrations that leverage Protonmail accounts but permitting Gmail sign ups—thereby removing anonymity from users.

ZeroFox anticipates similar pressure tactics will be used by an increasing number of threat actors in coming months. The omission of encrypting payloads from extortion attacks will likely become increasingly popular amongst established extortion collectives and will likely facilitate a larger pool of threat actors not historically involved in extortion to enter the digital extortion space.

ZeroFox has anticipated developments in extortion tactics for some time, with an observed sharp decrease in the number of ransom payments being made. Threat actor adversity breeds innovation and an evolution in tactics, and this very likely applies to pressure tactics in extortion incidents. Whereas in typical R&DE incidents, there is a period

8

[hXXps://www.malwarebytes\[.\]com/blog/news/2024/05/notorious-data-leak-site-breachforums-seized-by-law-enforcement](https://www.malwarebytes.com/blog/news/2024/05/notorious-data-leak-site-breachforums-seized-by-law-enforcement)

9

[hXXps://www.malwarebytes\[.\]com/blog/news/2024/05/data-leak-site-breachforums-is-back-boasting-live-nation-ticketmaster-user-data-but-is-it-a-trap](https://www.malwarebytes.com/blog/news/2024/05/data-leak-site-breachforums-is-back-boasting-live-nation-ticketmaster-user-data-but-is-it-a-trap)

where victims can settle negotiations before other threat actors can get their hands on victims' data, ZeroFox expects to increasingly see this done simultaneously and in public channels.

| Recommendations

- ZeroFox recommends that customers follow all guidance outlined by CISA and Snowflake's respective security teams.
 - [hXXps://www.cisa\[.\]gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access](https://www.cisa.gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access)
 - [hXXps://community.snowflake\[.\]com/s/question/0D5VI00000EmyI00AB/detecting-and-preventing-unauthorized-user-access](https://community.snowflake[.]com/s/question/0D5VI00000EmyI00AB/detecting-and-preventing-unauthorized-user-access)
- Organizations of all sizes and industries should implement a company-wide comprehensive MFA policy. Research suggests that, while approximately 87 percent of organizations with 10,000+ employees use MFA, only 34 percent of organizations with less than 100 employees do.
- Ensure employees receive training covering contemporary social engineering threats and the importance of correctly using MFA tools.
- As the most secure form of MFA, physical authentication devices should be used where possible. Devices such as USB and public key infrastructure (PKI) keys are the least susceptible to interception, tampering, or compromise.
- MFA challenges should be as regular as possible without causing significant disruption or the frustration likely to lead to misuse.
- Maintain a principle of least trust by ensuring access is continuously scrutinized and adjusted and implementing identity and access management (IAM) solutions, along with network segmentation.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%