



| Flash |

Threat Actor Linked to ShinyHunters Advertises Extortionate Data Breach

F-2024-06-12a

Classification: TLP:CLEAR

Criticality: Medium

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

June 12, 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 12, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Actor Linked to ShinyHunters Advertises Extortionate Data Breach

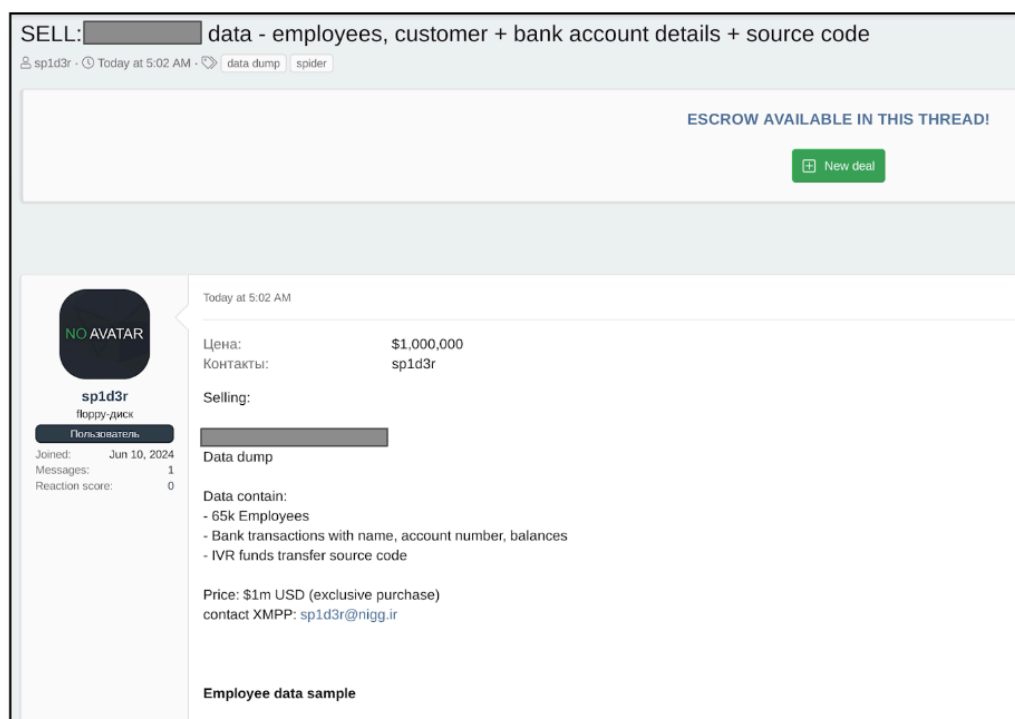
> Key Findings

- On June 11, 2024, untested threat actor “sp1d3r” advertised the sale of a notably-large leaked data set in the Russian-speaking dark web forum xss. The breach allegedly contains 65,000 records of data stolen from a U.S.-based financial organization that purportedly include both personal financial information (PFI) and personally identifiable information (PII).
- The owner of this stolen data is likely a victim of the ongoing fallout of the alleged breach of cloud-based service provider Snowflake. Since the alleged breach on May 23, 2024, several of Snowflake’s assumed customers’ data have been advertised on deep and dark web (DDW) forums.
- Sp1d3r is almost certainly synonymous with, or heavily associated with, threat actor “ShinyHunters”, who is very likely responsible for recent attacks against Snowflake customers.
- In the coming weeks, it is very likely that additional Snowflake customers will be implicated in data breaches, with the stolen information being advertised for sale in DDW forums.

Details

On June 11, 2024, threat actor sp1d3r advertised the sale of a notably large leaked data set in the Russian-speaking dark web forum xss. The breach allegedly contains 65,000 records of data stolen from a U.S.-based financial organization and is stated to include both PFI and PII. The asking price for the data is USD 1,000,000, exclusive to one buyer only. Although the advertisement does not specifically mandate the use of escrow, is it almost certainly a requirement for a transaction of this size to take place.

- The advertisement includes samples of the data, which are composed of account numbers, bank balances, interactive voice response (IVR) funds transfer source code, and details surrounding bank transactions.
- The PII included appears to contain large quantities of employee information, such as names, addresses, banking identification, and personal contact information.
- The offering of large and detailed information samples increases the authenticity of sp1d3r and the advertised data.



Sp1d3r's xss post, with victim anonymized by ZeroFox

Source: ZeroFox Intelligence

The owner of this stolen data has likely been implicated in the ongoing fallout of the alleged breach of cloud-based service provider Snowflake. Since the alleged breach on May 23, 2024, several of Snowflake's assumed customers' data has been advertised on DDW forums.

- Sp1d3r had previously advertised the sale of data allegedly stolen from a U.S.-based automotive parts organization for USD 1.5 million on DDW forum Exploit on May 30, 2024.
- On May 29, 2024, ShinyHunters advertised data stolen from Ticketmaster in the English-speaking DDW forum BreachForums for USD 500,000.
- On May 24, 2024, untested threat actor "whitewarlock" advertised the sale of data allegedly stolen from a Europe-based financial organization for USD 2 million on the DDW forum Exploit.

While information of this nature carries innate value in DDW forums and can be leveraged by threat actors wishing to conduct social engineering, blackmail, or fraudulent activity, the exorbitant advertised price is very likely reflective of the victim being the sole intended buyer, rather than the advertisement being a realistic attempt to garner interest from the broader xss community. In parallel to other recently-announced victims, this is very likely a digital extortion attempt rather than a traditional data breach.

Like whitewarlock, sp1d3r is almost certainly synonymous with (or heavily associated with) threat actor ShinyHunters, who is very likely responsible for recent attacks against Snowflake customers. Sp1d3r registered on xss forum on June 10, 2024, and carries no reputation on the forum.

- ShinyHunters is an English-speaking black hat threat group that has been active on dark web forums for a considerable period, garnering a well-known—albeit controversial—reputation.
- Until its disruption by law enforcement (LE) entities on May 15, 2024, ShinyHunters was a moderator of the popular hacking forum BreachForums.

As of the time of writing, BreachForums—which ShinyHunters has used in the past primarily to disseminate data leaks—is not operational. The consistent disruption of this

forum is very likely a contributing factor toward ShinyHunters' employment of multiple aliases and use of numerous DDW forums to advertise stolen data.

In the coming weeks, it is very likely that additional alleged Snowflake customers will be implicated in data breaches, with the stolen information being advertised for sale in DDW forums. There is a roughly even chance that these will be posted by further, as-yet-unseen aliases associated with ShinyHunters across an array of forums, as the threat actor seeks to avoid LE scrutiny. In the medium to long term, there is a roughly even chance that ShinyHunters will seek to establish reputation and credibility within a single DDW forum, where operations and sales can take place more reliably.

| Recommendations

- ZeroFox recommends that customers follow all guidance outlined by the Cybersecurity and Infrastructure Security Agency (CISA) and Snowflake's respective security teams.
 - <https://www.cisa.gov/news-events/alerts/2024/06/03/snowflake-recommends-customers-take-steps-prevent-unauthorized-access>
 - <https://community.snowflake.com/s/question/0D5VI00000Emyl00AB/detecting-and-preventing-unauthorized-user-access>
- Organizations of all sizes and industries should implement a company-wide comprehensive multi-factor authentication (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%