ZEROFOX INTELLIGENCE

Flash

Possible ShinyHunter SSO Phishing Campaign Identified

F-2026-01-29b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Social Engineering, Vishing, Threat Actor, Single Sign-On (SSO)

January 29, 2026

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 8:30 AM (EST) on January 29, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Possible ShinyHunter SSO Phishing Campaign Identified

| Key Findings

- In late January 2026, actors claiming to be well-known threat collective "ShinyHunters" are reportedly orchestrating extortion-focused voice phishing or vishing attacks targeting single sign-on (SSO) accounts hosted by Okta, Google, and Microsoft at several major organizations.
- Concurrently, ZeroFox has observed that a leak site associated with threat collective "Scattered Lapsus$ Hunters" has been recently renamed to ShinyHunters and lists six organizations as victims.
- Given the fact that some of the companies listed on the leak site have disclosed intrusions but not exfiltration of sensitive data, it is very likely that the threat actors are advertising either recycled data or data that is not sensitive and is available in the open source.

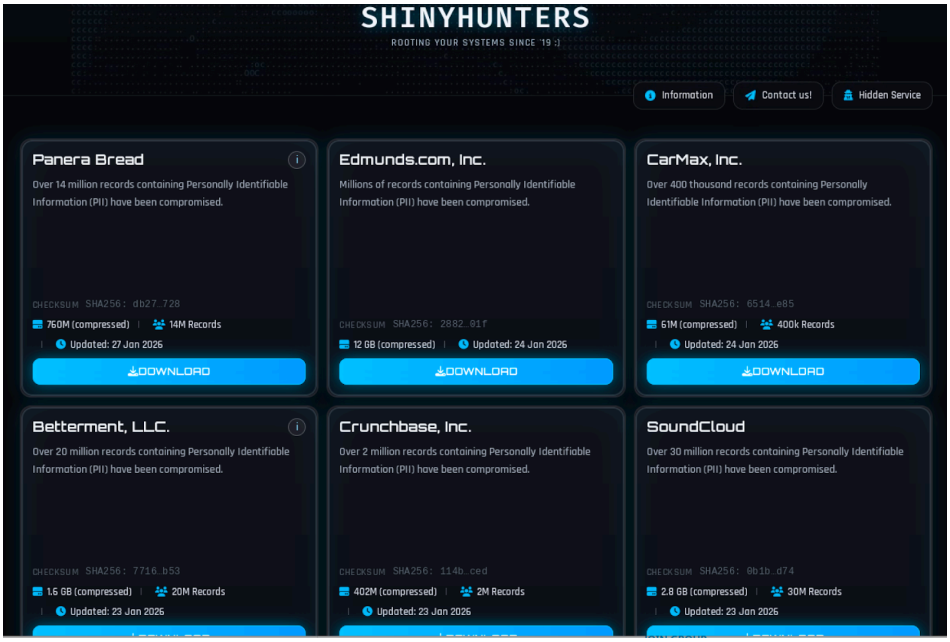
Details

In late January 2026, actors claiming to be well-known threat collective ShinyHunters are reportedly orchestrating extortion-focused voice phishing or vishing attacks targeting SSO accounts hosted by Okta, Google, and Microsoft at several major organizations.[1] Okta has acknowledged being targeted by custom phishing kits, made available on an as-a-service basis, in the vishing campaign.[2]

- The phishing kits reportedly use a web-based control panel that enables attackers to update fake sites in real time. The actors then use these sites to walk victims through login and multi-factor authentication (MFA) approvals during vishing phone calls.

Concurrently, a leak site associated with threat collective Scattered Lapsus$ Hunters was renamed as ShinyHunters and lists six organizations as victims, including Crunchbase, Panera Bread, Betterment, Edmunds, CarMax, and SoundCloud. Crunchbase has reportedly confirmed a data breach, and both Betterment and SoundCloud have acknowledged cybersecurity incidents impacting their systems.[3][4][5]

[1] hXXps://www.bleepingcomputer[.]com/news/security/shinyhunters-claim-to-be-behind-sso-account-data-theft-attacks/
[2] hXXps://www.okta[.]com/blog/threat-intelligence/phishing-kits-adapt-to-the-script-of-callers/
[3] hXXps://www.securityweek[.]com/crunchbase-confirms-data-breach-after-hacking-claims/
[4] hXXps://www.betterment[.]com/customer-update
[5] hXXps://soundcloud[.]com/playbook-articles/protecting-our-users-and-our-service

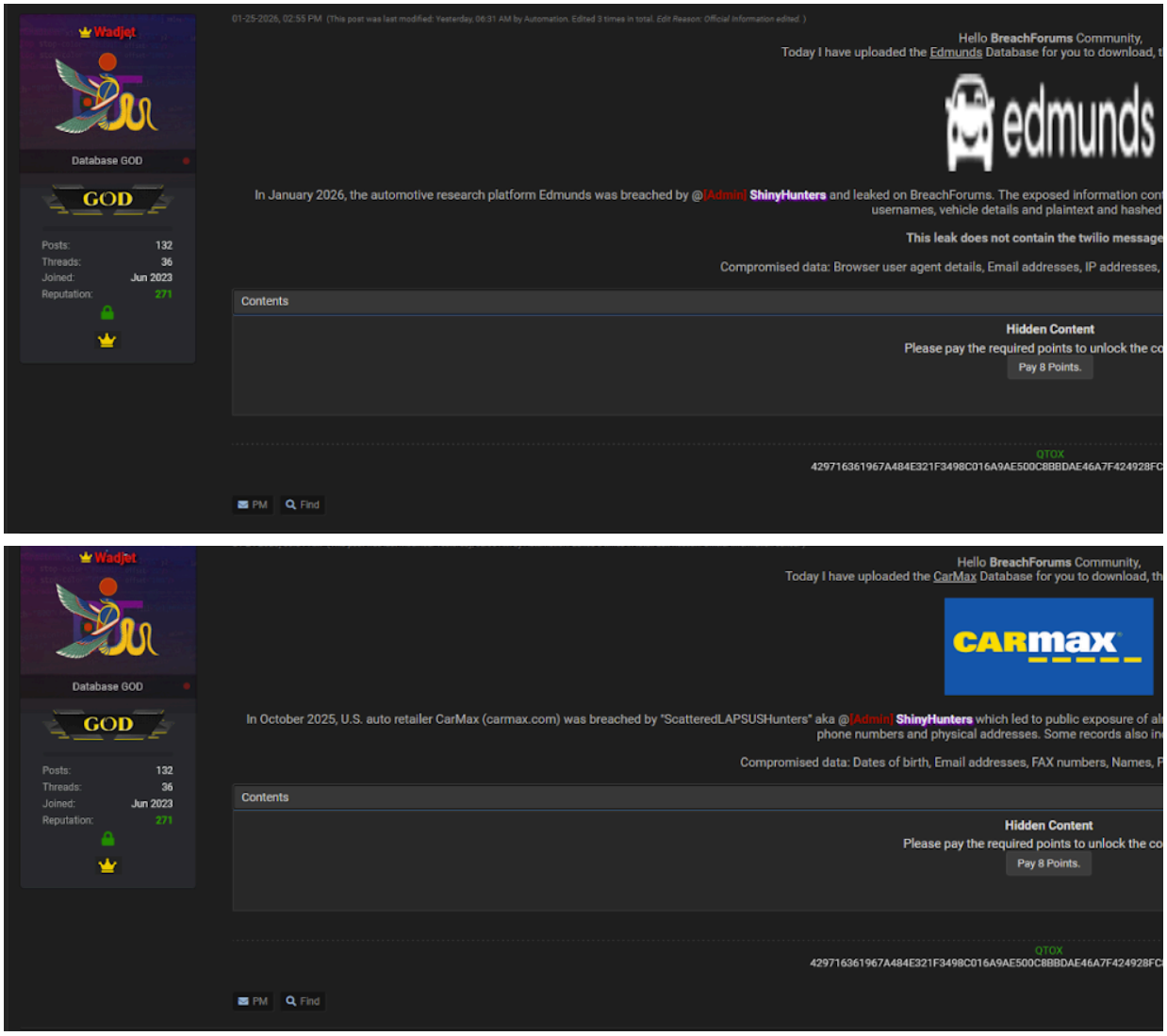


ShinyHunters leak site

Source: ZeroFox Intelligence

- Betterment stated that, on January 9, 2026, an unauthorized individual used social engineering and identity impersonation to access its third-party marketing and operations systems—without breaching its core technical infrastructure.[6]
- SoundCloud "detected unauthorized activity in an ancillary service dashboard" in December 2025.[7]
- Between January 24 and January 25, 2026, a threat actor on predominantly English-language dark web forum BreachForums named "Wadjet" advertised datasets allegedly belonging to Edmunds and CarMax. The posts stated that the datasets were sourced from breaches conducted by Scattered Lapsus$ Hunters.

[6] hXXps://www.betterment[.]com/customer-update
[7] hXXps://soundcloud[.]com/playbook-articles/protecting-our-users-and-our-service



Wadjet's BreachForums posts

Source: ZeroFox Intelligence

ShinyHunters is a financially motivated threat collective known for data leaks, extortion, and supply chain compromises, with alleged links to an infamous Telegram group called Scattered Lapsus$ Hunters (SLH) that ZeroFox first observed in August 2025. After a brief period of inactivity, SLH resurfaced on Telegram in November 2025, using leaks and public taunts to reassert its presence and signal continued operations.

- SLH has previously claimed dozens of victims, attributing compromises to alleged Salesloft Drift and Salesforce supply chain access.

- The group has experimented with monetization through Extortion-as-a-Service and promoted a planned ransomware offering, "ShinySp1d3r".
- SLH's Telegram leaks targeting CrowdStrike were later linked to screenshots shared by an internal insider.

Given the fact that some of the companies listed on the leak site have disclosed intrusions but have not confirmed exfiltration of sensitive data, there is a roughly even chance that the threat actors are advertising either recycled data or data that is not sensitive and is available in the open source.

- Betterment has confirmed that "no customer accounts were accessed and that no passwords or other log-in credentials were compromised."[8]
- SoundCloud has also stated that no sensitive data (such as financial or password data) was accessed.[9]
- CrunchBase has yet to disclose details of the data accessed by the intruders.
- The other listed organizations have not yet disclosed any data breach that occurred in the past four weeks.

However, it is likely that the targeted companies and their downstream entities will be subjected to social engineering and data breach attempts using the stolen credentials. Further, the vishing lures are likely to become more sophisticated if the actors incorporate artificial intelligence and deep fakes to replicate the voices of the targets' higher officials or trusted communicators, such as account managers.

[8] hXXps://www.betterment[.]com/customer-update
[9] hXXps://soundcloud[.]com/playbook-articles/protecting-our-users-and-our-service

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant MFA, and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

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%