



| Flash |

New Tax Fraud Scheme Leveraging Employer Identification Numbers

F-2024-02-14a

Classification: TLP:CLEAR

Criticality: Medium

**Intelligence Requirements: Social Engineering, Deep & Dark Web, Threat
Actors**

February 14, 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 (EST) on February 14, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | New Tax Fraud Scheme Leveraging Employer Identification Numbers

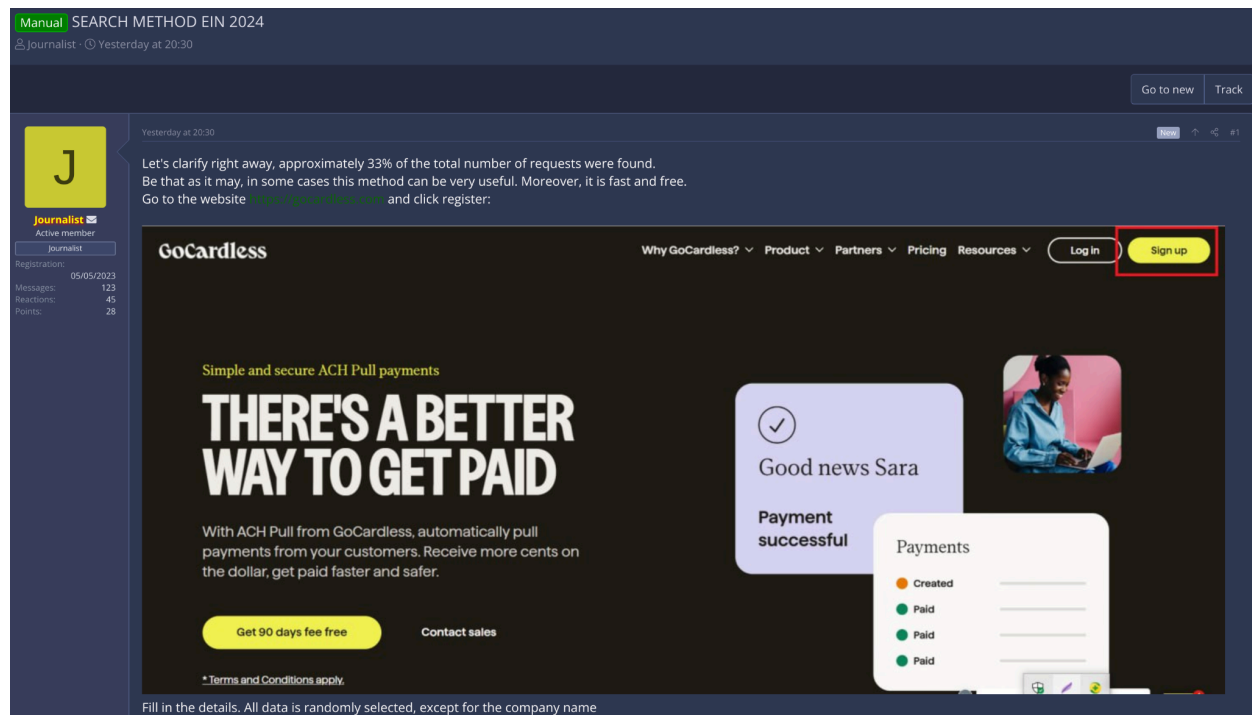
> Key Findings

- On February 11, 2024, well-regarded Russian-speaking threat actor “Journalist” disclosed a method of leveraging the legitimate gocardless[.]com service to identify corporate employer identification numbers (EINs) on the Russian-speaking community “Coockie Pro.”
- Threat actors can use EINs to create fake tax returns and raise fraudulent tax refund claims on behalf of U.S. companies.
- Journalist provided screenshots of the method in action, seeming to successfully obtain the EIN for a U.S.-based construction company.
- ZeroFox anticipates schemes of this nature will continue to propagate amongst financially-motivated actors ahead of the April 15, 2024 U.S. tax return deadline. Tax refund and related schemes surge on the deep and dark web (DDW) in the run up tax season in the U.S. year-on-year.

Details

On February 11, 2024, well-regarded Russian-speaking threat actor “Journalist” disclosed a method of leveraging the legitimate gocardless[.]com service to identify corporate employer identification numbers (EINs) on the Russian-speaking community “Cookie Pro.”

- The method involves obtaining and leveraging an organization’s EIN to conduct tax fraud schemes.
- Threat actors can use the EIN to create fake tax returns and raise fraudulent tax refund claims.
- Journalist advised leveraging gocardless[.]com, a service offered by a financial technology company specializing in online payment solutions, to register an account for free in the name of a targeted company in order to obtain their EIN.

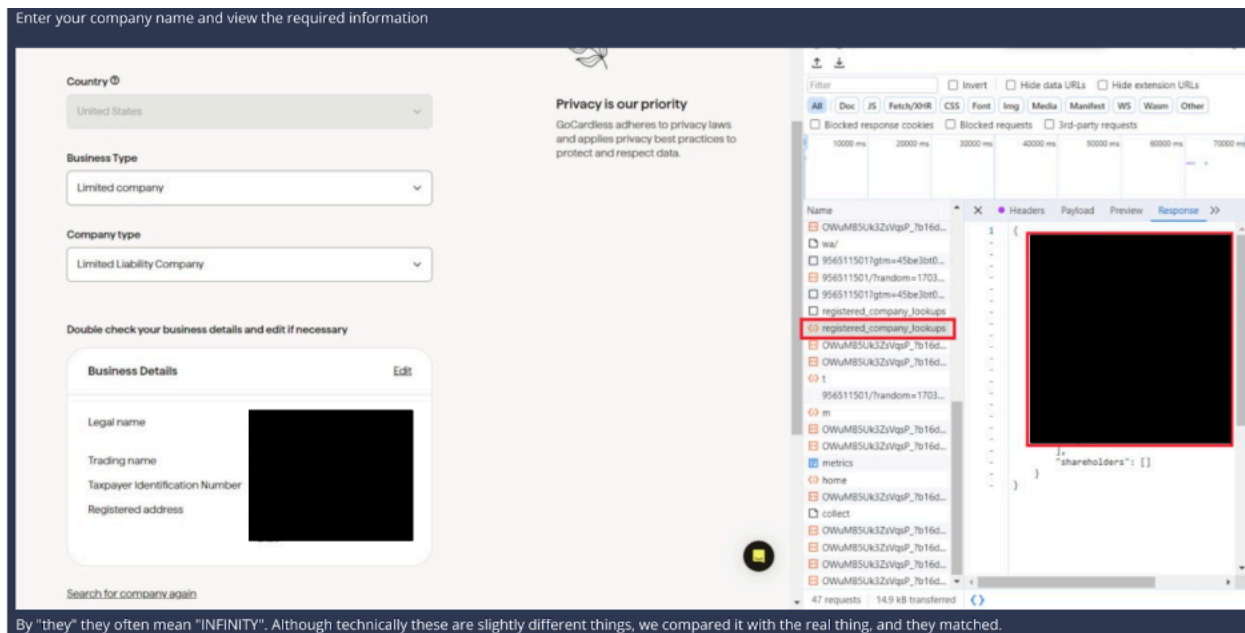


Translation of Journalist’s post outlining how to leverage GoCardless in tax return scams

Source: ZeroFox Intelligence

Journalist provided screenshots of the method in action, seeming to successfully obtain the EIN for a U.S.-based construction company, confirming the EIN’s authenticity by verifying it against another unnamed source.

- Journalist alleges to have obtained the EIN prior to paying for GoCardless' Pro Plan, circumventing any barriers to entry in providing a legitimate payment method that might disclose a threat actor's identity.



Translated and redacted screenshot showing the successful obtaining of the EIN for a U.S.-based construction company

Source: ZeroFox Intelligence

Tax refund and related schemes surge on the DDW in the run up tax season in the U.S. year-on-year, with Russian-speaking threat actors seeking to leverage innovative methods for financial gain. Journalists' method demonstrates how a legitimate fintech service can be leveraged for performing scams on behalf of U.S. organizations. ZeroFox anticipates schemes of this nature will continue to propagate amongst financially-motivated actors ahead of the April 15, 2024 U.S. tax return deadline.

Recommendations

- Conduct social engineering awareness training programs that educate staff on how to identify phishing attacks, emerging trends, and how personnel should report suspicious incidents.
- Ensure an organization-level system is in place that enables employees to report suspicious email communications, to bring awareness to ongoing campaigns and protect other users.
- Configure email servers to block emails with malicious indicators with macros disabled by default, and deploy authentication protocols to prevent spoofed emails.
- Scrutinize emails, even if appearing to have originated inside the organization. Look for incorrect or unusual grammar, spelling mistakes, mismatched hyperlink URLs, and illegitimate sender addresses.
- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a clear and comprehensive incident response strategy consisting of business resilience and continuity plans—including third party services' incident reporting procedures and key authorities.

| 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%