



| Flash |

Innovative Loader-as-a-Service Announced

F-2024-02-07b

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Malware, Deep & Dark Web, Threat Actors

February 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 (EST) on February 7, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Innovative Loader-as-a-Service Announced

> Key Findings

- Since its announcement on January 25, 2024, by untested actor “Null14”, an innovative malware loader-as-a-service offering has been gaining traction on the predominantly Russian-speaking dark web community exploit[.]in.
- The currently unnamed loader allegedly targets Windows operating systems and is signed using valid certificates, enabling its deployment to remain undetected by various Windows systems as well as VirusTotal.
- Although ZeroFox can neither confirm nor disconfirm the credibility of the service, positive indicators add credence to the legitimacy of this loader service as an innovative malware-spreading technique.
- Malware distribution based on emulating credible software is likely on an upward trajectory, and this trend is expected to continue in the first half of 2024.

| Details

Since its announcement on January 25, 2024, by untested actor Null14, an innovative malware loader-as-a-service offering has been gaining traction on the predominantly Russian-speaking dark web community exploit[.]in.

- Loaders are a crucial part of efficient malware-spreading campaigns, as they form the spearhead of actual malware introduction to a targeted system, establishing persistence and enabling follow-on malicious activity.

Null14 claimed the currently unnamed loader targets Windows operating systems and is signed using valid certificates. The actor's post stated the loader boasts sophisticated detection evasion capabilities as a result of it being signed with valid certificates.

- Null14 alleged that this enables operatives to deploy and execute any weaponized software via a direct link without being detected by Windows SmartScreen, User Account Control, Google Chrome, Windows Defender, and potentially Microsoft Edge. The actor also claimed that use of valid certificates would enable the loader to remain unflagged by VirusTotal.
- The loader is encrypted, with additional re-encryptions possible once per day.
- The offering also included established servers and domains which host the loader and can be used to generate phishing links to target victims.

N

Loader EXE+EV VALID CERTIFICATE

By Null14, January 25 in [Software] - malware, exploits, bundles, crypts

Null14

byte

•

N

Paid registration

0

9 posts

Joined

01/10/24 (ID: 160371)

Activity

Other

Deposit

0.020395 \$

Posted January 25

Loader ZIP EXE+EV VALID CERTIFICATE

Clean EXE in ZIP+EV VALID CERTIFICATE FUD VT Any Title Icons 🧑 Swap any original software via your direct link 🔄

SmartScreen ABSENT

UAC Green

Bypass Google Chrome

Bypass Bypass Edge 🚩🚩🚩🚩🚩

Bypassing WinDef

Protection from VirusTotal

Weight from 60 mb <

Trusted UAC

Repeat knock lock (optional)

Own servers, domains

Translated post announcing the launch of the new loader-as-a-service offering

Source: ZeroFox Intelligence

The loader is offered at a price of USD 490 per week; Null14's post specified that, should the certificate be revoked during this period, the remainder of the purchase period would be refunded.

- Buyers were prohibited from leaking information about the copyright holder of a certificate, as this would allow deanonymization of the certificate.
- Any buyer caught in the act will have their subscription canceled.

Although ZeroFox can neither independently confirm nor disconfirm the credibility of the service, positive indicators add credence to the legitimacy of this loader service as an innovative malware-spreading technique that moves the burden of bypassing detection from the coding skills of malware developers to relying on valid software-signing certificates.

- On February 5, 2024, vetted exploit[.]in user "boomking" claimed this new loader service is the best solution available for the price requested. The actor also claimed to have successfully bypassed Chromium and Windows Defender using it.
- Null14 posted a screenshot that included a highlighted certificate for the WinRar application, indicating that a certain instance of the WinRar executable was likely weaponized.
- Null14 did not specify the origin of the certificates, but software-signing services and valid certificates have regularly been observed for sale in predominantly Russian-speaking communities since 2021.

Malware distribution based on emulating credible software is likely on an upward trajectory, and this trend is expected to continue in the first half of 2024.

Recommendations

- Implement secure password policies with phishing-resistant multi-factor authentication, complex passwords, and unique credentials.
- Configure ongoing monitoring for Compromised Account Credentials.
- Proactively monitor for compromised accounts being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of malware threats;

their associated tactics, techniques, and procedures (TTPs); and Indicators of Compromise (IOCs).

- 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.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege.
- Implement network segmentation to separate resources.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management system, and ensure all business IT assets are updated with the latest software as quickly as possible.
- Should your organization be impacted by a data breach, utilize ZeroFox Incident Response Services to swiftly deploy IDX data breach products and services to mitigate the impact to you and your customers.

| 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%