



# **PROFILE**

## **RISEPRO STEALER**

**ZEROFOX INTELLIGENCE**

P-2023-01-11a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Malware

**January 11, 2023**



## 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 8:00 AM (EST) on December 23, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# RisePro Stealer

## Executive Summary

RisePro Stealer is a malware typically used to steal sensitive information from infected computers. It has been spreading via PrivateLoader infections since late December 2022.<sup>1</sup> (PrivateLoader malware is designed to deliver secondary payloads such as RisePro Stealer through fake software cracks.) RisePro Stealer is capable of targeting several web browsers for saved credentials, credit cards, cookies, history, and many extensions that deal with cryptocurrency. In addition to browsers, RisePro targets cryptocurrency wallets through desktop applications and files matching attacker-configured patterns; it is also capable of acting as a loader for secondary payloads. Good cyber hygiene practices and avoiding the use of pirated software may combat the risks posed to individuals and organizations.

## Capabilities

### Obfuscated Files or Information [T1027]

RisePro Stealer obfuscates its strings.

### Obfuscated Files or Information: Dynamic Application Programming Interface (API) Resolution [T1027.007]

RisePro Stealer may dynamically retrieve or extract dynamic link library (DLL) dependencies. It also obfuscates API imports.

### System Information Discovery [T1082]

RisePro Stealer gathers information about the infected host using the following registry keys:

- SOFTWARE\Microsoft\Cryptography
- SOFTWARE\Microsoft\Windows NT\CurrentVersion
- HARDWARE\DESCRIPTION\System\CentralProcessor\0
- SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

---

<sup>1</sup> [hXXps://blog.sekoia\[.\]io/new-risepro-stealer-distributed-by-the-prominent-privateloader/](https://blog.sekoia.io/new-risepro-stealer-distributed-by-the-prominent-privateloader/)



## Screen Capture [T1113]

RisePro Stealer saves a screenshot of the infected host as “screenshot.png” in the same directory in which the malware was run.

## Credentials from Password Stores: Credentials from Web Browsers [T1555.003]

RisePro Stealer targets a large number of web browsers to obtain credentials and other sensitive data.

### Targeted browsers:

- 7start
- Amigo
- Atom
- BlackHaw
- Brave
- CatalinaGroup Citrio
- CentBrowser
- Chedot
- ChomePlus
- Chromium
- Chromodo
- Comodo
- Coowon
- CryptoTab
- Elements
- Firefox
- Google Chrome
- IceDragon
- Iridium
- K-Melon
- Maxthon3
- Netbox
- Nichrome
- Opera
- Orbitum
- Pale Moon
- QIP Surf
- Sputnik
- Torch
- Uran
- Vivaldi
- Yandex



## **Automated Collection [T1119]**

RisePro Stealer can be configured to steal files based on attacker-provided patterns.

## **Data Obfuscation [T1001]**

RisePro Stealer obfuscates its command and control (C2) server communications to hinder detection and analysis.

## **User Execution: Malicious File [T1204.002]**

RisePro Stealer can be configured to download and execute secondary payloads.

## **Recommendations**

RisePro Stealer is known to be distributed via PrivateLoader infections, which are typically spread via fake software cracks. ZeroFox Intelligence highly recommends that organizations discourage the use of pirated software to prevent infection.

Organizations with a central authentication mechanism in place, such as Active Directory, may also wish to restrict account privileges to prevent unauthorized software installations.

ZeroFox Intelligence also recommends proactively utilizing the unique data sets available within ZeroFox's Threat Intelligence Feeds to correlate alerts in your environment with indicators of attack/compromise and prepare appropriate security team responses in order to get ahead of threat actor activity. More information about which feeds are offered on the [API Data Feeds](#) page is available in the ZeroFox platform.



## Appendix 1: Indicators of Compromise (IOCs)

### C2 Domains

- 108.174.99[.]249
- 108.174.200[.]11
- 108.174.198[.]132
- my-rise[.]cc
- api.my-rise[.]cc

### SHA256 Hashes

- 057b33d69a28fb08733bb710ca22036aaee853791b958e8c4e0c81ae5eed6fcd
- 28820e270265796566d6651f16651a5fd6c412b9290be07d2829c444d9392a02
- 2d34e214cbb14456357d2e3381692d188b1004d8ff26280e430c716e6e3730b6
- 3e38c14c9a27966b7768fa6a61a0bc86b79fdf8f554d232c26d0a13cd8dc36
- 3fea5da905fb8cdb9ef203f85a2b0d37d9cbc8067fbf64d3e1849e84d99de3ee
- 4107f3166ce3c67f375514ed039d663f197261126724f229e8d3cda2e62728d0
- 440cecldd86d03c4e9a29a7b297a30a211f17d48828934a5a7121flf4b97ef43
- 478e97b727eb82979087cld4c2450be18c2d3413ca8c648e7e2a067595ef8511
- 49fea24c6d2f6340755a22687a6daf63ff2692fe81e6e067b8b2465bc21f49f9
- 58b1210213aclcb9c4efe63d43390dfd43bf094408b16033f176e6700ad0fb29
- 5facf25f6b0d35a79444949b3175fabf3d788cbfbbbbb6551a867elddceb00a5
- 75b395cc766351e6f44f36dcdbfabc2c4b43ef6fb26f845fb55569a57ebdbdd
- 9564a7f5d7132fe8a97450e0fa4b628b7d802c885f034dc5d094260ff6a76716
- aa80643e117a896314fe6b1785cb65ab53561f66f5b679ba9f16a05f36e28674
- ad75f79f985b4ec690fe9280108ae51ceec8ef1650581ed4e26497a5e2c2f3ef9
- ae8becfd65df0625c7e4f2069cb57e6f3c022aff24db51666b4d8b8c6ab15a15
- b295631063a6186a09a9dfee224bca7af6d4ab1650e9d63cdc325cf3felcd3d6
- c70e26edeacbf1fa052f073959403ee9337a4aed13833553f8a3856fae013c9e
- ffae7d880fcb139d03941elbc658ce463e179435f438d945c74067fe291beeb23



## Appendix 2: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:RED</b> 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. | <b>Sources may use</b><br><b>TLP:AMBER</b> 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?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> 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.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |