# Rhadamanthys Stealer: Introduces an AI feature to extract seed phrases fr

Data: 2025-09-26 16:58:40

Autor: Inteligência Against Invaders

Redazione RHC**:26 September 2025 17:16**

Rhadamanthys is an advanced information stealer that first emerged in 2022. Featuring a rapid development cycle—with at least ten different releases since its inception—the malware is promoted and marketed on underground forums.

Despite a ban on its use against Russian and/or former Soviet republics, the product is still available on the black market; prices start at $250 for 30 days of access, a price that favors its spread among cybercriminals.

## Evasion features and techniques

Rhadamanthys is designed to collect a wide range of data: system information, credentials, cryptocurrency wallets, passwords stored in browsers, cookies, and data from numerous applications. It integrates numerous anti-analysis countermeasures that complicate code observation and hinder its execution in sandbox environments.

Recorded Future's Insikt Group acquired and analyzed the latest release, 0.7.0, highlighting several new features. The most significant innovation **involves the use of artificial intelligence: using optical character recognition (OCR)** , Rhadamanthys is now able *to automatically identify and extract cryptocurrency wallet seed phrases from images.* The function is divided into client and server components: the client identifies potential images containing seed phrases, and once they are exfiltrated to the command and control server, the backend performs the complete extraction.

Among other additions, version 0.7.0 **allows threat actors to execute and install Microsoft Installer (MSI) packages,** a vector that can bypass traditional security controls because MSI files are often associated with legitimate installations. Additionally, the developer has made the feature that prevents malware from re-executing within a configurable timeframe more robust and **tamper-proof** , updating it with encryption and hashing mechanisms.

## Distribution, author and sales channels

The malware is popular among the criminal community; its rapid evolution and emerging features make it a significant threat to organizations. The main developer, known under the pseudonym **"kingcrete2022,"** has been **banned from both XSS and Exploit Forums** due to allegations of targeting Russian and/or former USSR republics. Despite the bans, the author continues to advertise new versions through private messaging on TOX, Telegram, and Jabber.

The Insikt Group report outlines mitigation strategies organizations should adopt. It also *provides detections for Rhadamanthys, and as a preventative measure, it describes a “killswitch” based on setting known mutexes on uninfected systems to block its execution and protect at-risk machines.*

## Operational risks

Infostealers pose a significant threat to corporate security: the widespread practice of password reuse facilitates escalation from personal to professional settings. Credentials stolen from private accounts—for example, from a social network—can allow unauthorized access to work accounts, especially when professional email addresses are easily found on networking platforms. Furthermore, the mixed use of devices for personal and professional activities increases the risk of infection: opening malicious links or browsing compromised sites by employees or family members can expose corporate credentials.

For these reasons, the report emphasizes the importance of strong password policies, ongoing staff training on safe browsing practices, and rigorous access controls to reduce the impact of infostealers.

This article is based on information, in whole or in part, from the intelligence platform of Recorded Future , a strategic partner of Red Hot Cyber and a global leader in cyber threat intelligence. The platform provides advanced analytics to detect and counter malicious activity in cyberspace.

**Redazione**
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli