LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-02 12:02:04 UTC

Fake WinRAR downloads hide malware behind a real installer

Domain: 3

A recent discovery by web researchers has highlighted a malicious campaign involving fake WinRAR installers being distributed from various Chinese websites. The fraudulent installer, named "1winrar-x64-713scp1.exe," masquerades as the legitimate WinRAR application, which is a common method used to lower user suspicion. The presence of Chinese characters that translate to "install" suggests that these links are aimed at deceiving users into downloading the malware under the guise of legitimate software. This tactic of embedding malware within a legitimate installer can facilitate a range of cyber attacks, as users often trust well-known applications like WinRAR. This campaign emphasizes the importance of scrutinizing software downloads, as attackers frequently employ social engineering techniques to trick users into compromising their systems.

- 160 Subscribers

Fake WinRAR downloads hide malware behind a real installer

Domain: 3

A recent discovery by web researchers has highlighted a malicious campaign involving fake WinRAR installers being distributed from various Chinese websites. The fraudulent installer, named "1winrar-x64-713scp1.exe," masquerades as the legitimate WinRAR application, which is a common method used to lower user suspicion. The presence of Chinese characters that translate to "install" suggests that these links are aimed at deceiving users into downloading the malware under the guise of legitimate software. This tactic of embedding malware within a legitimate installer can facilitate a range of cyber attacks, as users often trust well-known applications like WinRAR. This campaign emphasizes the importance of scrutinizing software downloads, as attackers frequently employ social engineering techniques to trick users into compromising their systems.

- 160 Subscribers

Snake Evolution

FileHash-MD5: 27 | **FileHash-SHA1:** 27 | **FileHash-SHA256:** 35 | **Hostname:** 3

The Snake Keylogger, also referred to as the 404 Keylogger, is a malware variant categorized primarily as a keylogger but has evolved to include stealer functionalities, enhancing its capabilities significantly since its emergence in 2019. Analysts suggest that a considerable portion of its source code may be derived from the Matiex malware, although there is debate over the order of their development, with some claiming 404 was the original and that Matiex subsequently leveraged its code.

- 160 Subscribers

Microsoft Office Russian Dolls

CVE: 1 | **FileHash-MD5:** 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 2

Recent trends in cyber threats have seen a resurgence in malicious Microsoft Office documents, particularly leveraging vulnerabilities that allow for the exploitation of these files. One notable technique involves the use of Rich Text Format (RTF) documents that target CVE-2017-11882. This vulnerability relates to a specific security flaw in Microsoft Office that enables attackers to execute arbitrary code through crafted RTF files. Despite a reduction in malicious Office documents due to Microsoft's implementation of stricter rules to prevent the automatic execution of VBA macros, threat actors continue to utilize these RTF documents effectively. This attack vector reflects a broader pattern of adapting tactics in response to security enhancements in software applications. The use of RTF exploits serves as a reminder of the ongoing risks posed by vulnerabilities within widely-used applications, illustrating how cyber attackers can creatively circumvent protective measures.

- 160 Subscribers

- 258 Subscribers

- 840 Subscribers

Original State

CIDR: 1 | **CVE:** 1 | **FileHash-MD5:** 321 | **FileHash-SHA1:** 319 | **FileHash-SHA256:** 1242 | **SSLCertFingerprint:** 1 | **URL:** 712 | **Domain:** 365 | **Email:** 5 | **Hostname:** 560

- 218 Subscribers

- 224 Subscribers

Software Packing | Mirai • Emotet • Pottieq | Mercer Museum Library

CIDR: 1 | **CVE:** 1 | **FileHash-MD5:** 311 | **FileHash-SHA1:** 309 | **FileHash-SHA256:** 1044 | **SSLCertFingerprint:** 1 | **URL:** 230 | **Domain:** 260 | **Email:** 4 | **Hostname:** 429

Attacking Mercer Museum Research Library. Bucks County, Pa. Malicious redirect to 7034.sydneyplus.com. Attacks Nelson- Stratton and Brashears Families historical Doylestown presence. Thor 4 years ago Signature Match - THOR APT Scanner Detection ========== Rule: MAL_Unknown_Malware_May19_1 Rule Set: Malware 1 Rule Type: VALHALLA rule feed only Description: Detects unspecified malware noticed in 2019 Reference: Internal Research Author: Florian Roth Score: 75 Detection Snapshot ========== Detection Timestamp: 2019-10-30 17:30 AV Detection Ratio: 23 / 68 #unknown #malware1 #mal_unknown_malware_may19_1 More information: https://www.nextron-systems.com/notes-on-virustotal-matches/ Please report interesting findings via Twitter @thor_scanner

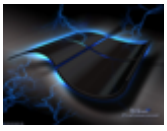
- 218 Subscribers

Venus Ransomware

FileHash-MD5: 4 | **FileHash-SHA1:** 4 | **FileHash-SHA256:** 4 | **Email:** 15

Exposed Microsoft Windows Remote Desktop Services were targeted by variants from the Venus ransomware family. The malware terminates processes, disables Data Execution Prevention, and deletes event logs and Shadow Copy Volumes. A "goodgamer" file marker is added to the end of infected files while the ".venus" extension is appended after encryption.

- 240 Subscribers



- 266 Subscribers

- 61 Subscribers

Threat Profile: RedLine Infostealer

FileHash-MD5: 308 | **FileHash-SHA1:** 308 | **FileHash-SHA256:** 307 | **URL:** 54 | **Domain:** 7 | **Email:** 1 | **Hostname:** 10

information stealer, named RedLine Stealer by the author, was identified being delivered through spam email campaigns, the malware is offered for sale on Russian dark web forums and as a tiered subscription allowing threat actors to use the information stealer, subscribe at different costs and purchase different access levels. In addition to being a password stealer, RedLine has the capabilities to steal login information, autocomplete data, passwords, and credit cards information from browsers.

- 240 Subscribers

Threat Profile: RedLine Infostealer

FileHash-MD5: 308 | **FileHash-SHA1:** 308 | **FileHash-SHA256:** 307 | **URL:** 54 | **Domain:** 7 | **Email:** 1 | **Hostname:** 10

information stealer, named RedLine Stealer by the author, was identified being delivered through spam email campaigns, the malware is offered for sale on Russian dark web forums and as a tiered subscription allowing threat actors to use the information stealer, subscribe at different costs and purchase different access levels. In addition to being a password stealer, RedLine has the capabilities to steal login information, autocomplete data, passwords, and credit cards information from browsers.

- 240 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

A new way to encrypt CC server URLs | Deutsche Telekom

A look at some of the highlights of Telekom’s work-life, as Thomas Barabosch looks back at how the German telecoms giant has evolved in the last five years. The malware downloader Smokeloader is one of the oldest malware families that is still in use today. A malware downloader is a typically small program that fingerprints a target system, downloads one or more additional malicious programs and executes them. Malware downloader forms part of the cybercrime ecosystem: there are cybercriminals that offer to distribute malware for other cybercriminals. They sell a number of installations for a couple of dollars, depending on several factors such as the geographic position of the target and its operating system.

- 96 Subscribers

- 1,098 Subscribers

Indicators Search

Show expired indicators

We've found 114 indicators

Source: https://otx.alienvault.com/browse/pulses?q=tag:Matryoshka