RedLine Stealer Malware Deployed Via ScrubCrypt Evasion Tool

By James Coker

Published: 2023-11-30 · Archived: 2026-04-05 20:34:18 UTC

A new version of the ScrubCrypt obfuscation tool is being used to target organizations with the RedLine Stealer malware, fraud sensor network Human Security has warned.

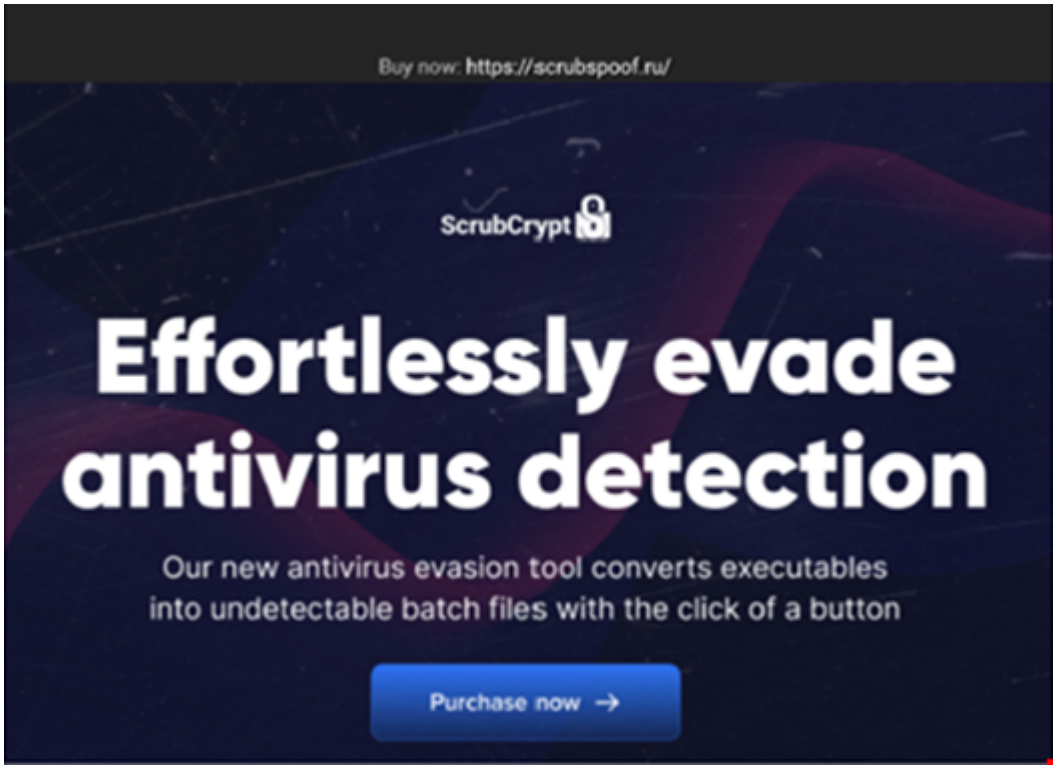
Human's Satori Threat Intelligence Team said it has uncovered the new build of ScrubCrypt for sale in dark web marketplaces, and observed it being used to launch account takeover and fraud attacks on its customers via RedLine Stealer.

How the New ScrubCrypt Build Works

ScrubCrypt is a tool used by threat actors to avoid detection by converting executable files into batch files. In March 2023, it was found to be used by the '8220 Gang' threat actor to target an exploitable Oracle Weblogic Server.

The researchers said the website selling and hosting this new ScrubCrypt build is registered and hosted in Russia to stay out of the reach of law enforcement agencies in regions like the US and EU.

However, the command-and-control (C2) server sending instructions and receiving the stolen credentials from the associated RedLine Stealer sample is hosted by an American provider of data center proxies and virtual servers. This approach is likely designed to help threat actors avoid certain firewall protections by having the malware phone home to a server located within the country of the target.



Banner ad promoting ScrubCrypt on a dark web marketplace. Source: Satori Threat Intelligence and Research Team

The researchers reversed engineered the attack to understand the new ScrubCrypt build's workings. To infect targets, a .bat file downloaded to a victim's device, often via a social engineering attack. This .bat file carries a base64-encoded payload and is peppered throughout with nonsensical repeating strings to obfuscate the payload.

After removing the strings and decrypting the AES-encrypted file, the researchers revealed the payload to be compressed gzip data.

Extracting the data stream of these files revealed an obfuscated .NET executable file. After deobfuscating this payload, the Satori team observed that the file loads an embedded resource called P . The sample then deobfuscates P using an XOR cipher with a key embedded in the .NET executable to get the final Windows executable payload.

The researchers found that the final payload was RedLine Stealer, although they noted other payloads can be encrypted and slipped past antivirus protections using the same method.

Redline Stealer is a well-known malware designed to compromise accounts through stealing cookies, browser login data, and locally-stored login information. This enables threat actors to conduct account takeover and account fraud attacks by logging in with the stolen credentials or reusing the cookies stolen from the browser.

The blog post stated: "This attack is emblematic of an alternative means of compromising accounts. Rather than relying on leaked/stolen credentials followed by a brute-force attack, some threat actors prefer a malware-based approach to account fraud using stealers like the RedLine Stealer payload in this attack."

How Organizations Can Mitigate this Threat

While Human Security acknowledged its customers had been targeted by RedLine Stealer before, this was the first instance incorporating this build of ScrubCrypt.

The firm said its findings is highlights how attackers are constantly evolving their techniques to stay ahead of improved defenses.

“As each new build of malware like RedLine Stealer or obfuscation tools like ScrubCrypt are unearthed and built into antivirus protections, threat actors go back to the drawing board to start designing the next build,” read the blog, published on November 30, 2023.

It recommended that organizations, particularly those with direct/private messaging capabilities native to their user platforms, take the following actions to mitigate this threat:

- Deploy protections that detect and mitigate cookie-stealing attacks
- Use tools that can flag users with credentials leaked or stolen in other threats
- Force compromised users to change their user credentials and confirm identity through two factor authentication (2FA)
- Stay up-to-date with threat research detailing evolving attack techniques

---