Raccoon Stealer Detection: A Novel Malware Version 2.0 Named RecordBreaker Offers Hackers Advanced Password-Stealing Capabilities

socprime.com/blog/raccoon-stealer-detection-a-novel-malware-version-2-0-named-recordbreaker-offers-hackers-advanced-password-stealing-capabilities/

Veronika Telychko

The notorious Raccoon Stealer, which was earlier distributed under the Malware-as-a-Service (MaaS) model, comes back to the cyber threat arena as a new version 2.0 enriched with more advanced capabilities. Raccoon Stealer malware was previously reported to have been replaced with Dridex Trojan by the RIG exploit kit as part of an ongoing campaign that resulted in the temporary suspension of the malware operations in March 2022.

Cybersecurity researchers have recently unveiled a new malware family observed in the wild, which shares similarities with Raccoon Stealer 2.0. The novel malware named RecordBreaker is currently active in the information stealer market and hacker forums, enabling threat actors to take advantage of upgraded password-stealing functionality and enhanced malware capabilities.

Detect Raccoon Stealer 2.0

Ever-growing attack volumes require ultra-responsiveness from cyber defenders and accelerated speed to stay ahead of attackers. SOC Prime's Detection as Code platform empowers security experts with advanced cyber defense capabilities offering the latest detection content available in under 24 hours after threat discovery. To proactively protect against the new malware version of Raccoon Stealer 2.0 also known as RecordBreaker, reach the dedicated Sigma rule written by our prolific Threat Bounty Program developer, Osman Demir:

Suspicious Recordbreaker Stealer Command and Control by Detection of Associated User Agent (via proxy)

SOC Prime welcomes seasoned and aspiring individual researchers and Threat Hunters to join its crowdsourced Threat Bounty Program to enrich collective cybersecurity expertise with their professional skill set while gaining an opportunity for both self-advancement and monetizing their contributions.

The Sigma rule above is applicable to 19 SIEM, EDR, and XDR solutions supported by SOC Prime's platform and is aligned with the MITRE ATT&CK® framework addressing the Command and Control tactic with the corresponding Application Layer Protocol (T1071) technique.

To explore the comprehensive list of Sigma rules along with their translations to 25+ SIEM, EDR, and XDR solutions for Raccoon Stealer detection, click the **Detect & Hunt** button below. Please note that only registered users can access the dedicated rule kit. Looking for a streamlined way to search for related threats and instantly delve into contextual metadata, like CTI and MITRE ATT&CK references? Click the **Explore Threat Context** button and drill down to search results related to Raccoon Stealer malware using SOC Prime's search engine for Threat Detection, Threat Hunting, and CTI.

Detect & Hunt Explore Threat Context

Raccoon Stealer Malware Analysis

Starting from June 2022, the beta version of the Raccoon Stealer has been actively tested within the hackers' community, with Raccoon 2.0 already being offered for sale to a limited number of threat actors at a price of $275 per month.

The latest Raccoon Stealer version, aka RecordBreaker, is coded from scratch leveraging C/C++, with a brand-new back-end and capabilities to grab users' credentials and sensitive data.

According to the in-depth inquiry by Sekoia, Raccoon Stealer 2.0 is capable of stealing system fingerprints, browser data, cryptocurrency wallets, web browser extensions, individual files located on all disks, etc. Also, the new strain can take screenshots and grab

installed app lists. Although malware operators state that all the stolen details are encrypted, Sekoia researchers haven't observed this type of functionality.

Notably, the novel Raccoon version transfers data each time it collects a new piece of information. Although it significantly increases the risk of detection, such behavior ensures maximum effectiveness while flying under the radar.

Sign up for free at SOC Prime's Detection as Code platform for a safer future crafted with the industry's best practices and shared expertise. SOC Prime's platform in conjunction with the Threat Bounty Program enables security practitioners to boost their cyber defense operations by participating in top-tier initiatives, sharing detection content of their creation, and monetizing their input.
Join SOC Prime's Detection as Code platform to improve visibility into threats most relevant to your business. To help you get started and drive immediate value, book a meeting now with SOC Prime experts.

Join for Free Book a Meeting