Takedown of GitHub Repositories Disrupts RedLine Malware Operations

The RedLine information stealer's operations have been disrupted after the takedown of GitHub repositories used by the malware's control panels, cybersecurity firm ESET reports.

A piece of commodity malware active since at least early 2020, the RedLine stealer is written in .NET and packs broad data exfiltration capabilities.

The malware targets system information, cookies and other browser data, login credentials for various applications and services, credit card information, and crypto wallets.

Available under the stealer-as-a-service business model, RedLine was seen being offered by 23 of 34 Russian-speaking groups that were distributing infostealers last year. Each of the groups had an average of 200 members.

RedLine is sold on underground forums and Telegram channels. Affiliates purchase access to an all-in-one control panel that acts as a command-and-control (C&C) server, allowing them to generate new samples and to manage stolen information.

Recently, threat actors were seen distributing the information stealer via the PureCrypter downloader, fake Adobe Acrobat Sign signature requests, and malicious Microsoft OneNote documents.

Working together with SaaS platform provider Flare, ESET discovered that RedLine's control panels use GitHub repositories as dead-drop resolvers.

The security researchers identified four such repositories and alerted the Microsoft-owned code collaboration platform. GitHub suspended the repositories, thus disrupting RedLine stealer's operations.

"No fallback channels were observed. The removal of these repositories should break authentication for panels currently in use. While this doesn't affect the actual back-end servers, it will force the RedLine operators to distribute new panels to their customers," ESET says.

Stealer-as-a-service is one of the top three crime-as-a-service categories likely to be prevalent in 2023, along with ransomware-as-a-service and victims-as-a-service.

Related:'Sys01 Stealer' Malware Targeting Government Employees

Related: Multi-Purpose Botnet and Infostealer 'Aurora' Rising to Fame

Related: Microsoft Build Engine Abused for Fileless Malware Delivery

Takedown of GitHub Repositories Disrupts RedLine Malware Operations