SamsStealer stealers targeting Windows systems

Date: 24th May 2024 | Severity: High

Summary

"SamsStealer," represents a new wave of information stealers targeting Windows systems. This malicious executable, written in .NET, has been observed propagating in a Telegram channel named "SamsExploit". The information stealer exhibits behaviour designed to covertly extract sensitive information from victims' computers.

It collects system information and creates a Temp folder to store the extracted information in the folder as different text files.

Attack Vectors

- The stealer asynchronously steals information, session data, and wallet information, which constitutes cryptocurrency wallet data including private keys and addresses, IP and system information, Passwords, cookies, and session data from various sources, Discord account details, and Telegram data.
- It uses concurrency for efficiency and removes unnecessary files from stolen data.
- Targeted Browsers and Applications include Discord variants, Telegram, Chrome, Firefox, Opera, Brave, Chromium, EpicPrivacy, Opera, gaming browser OperaGx, Vivaldi, and Yandex.
- Targeted cryptocurrency wallets include Bitcoin, Zcash, Armory, Bytecoin, Jaxx, Exodus, Ethereum, Electrum, AtomicWallet, Guarda, and Coinomi.
- The malware employs a multi-step process to manage stolen data efficiently. It begins by compressing the gathered information into a ZIP file named "Backup.zip". Subsequently, it leverages the "gofile.io" online file-sharing platform to upload this compressed file.
- Finally, it utilizes the messaging service Telegram to dispatch the download link of the uploaded file to the attacker for retrieval.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hashes	• 83f94302ae92909bc3b2834a5342d4a5 • 824e149b9c2bdd5dbe37f472533230af • 1f913f8d71f0f4d65858b5ba0ea94a9c • 56acc1496d8e5bbc0e412c683971b809 • 631eacb4519fd49048491c9b5ec6bda5 • 64410e06f80e75b6503e5525c323243b • 7d63047a48fa8984f11544149c2f0e70 • da493648ca3b8fd9dbad7bbca659b796 • 02fe599ed41cc4bd54a1d6a3cc2d830a • cb95c77750732c0a4dd29c1d4feb6f69 • 11751f8d847764936b7bf014302da87f • 31c73ad35b23e4d98ed974e604b85e00

Recommendation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Emails from unknown senders should always be treated with caution.
- Never trust or open links and attachments received from unknown sources/senders.
- Updates for operating systems, applications, and firmware should be installed as soon as possible.
- Check the active directories, servers, workstations, and domain controllers for new or unfamiliar accounts.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://www.cyfirma.com/research/samsstealer-unveiling-the-information-stealertarge ting-windows-systems/

Copyright © Mphasis Corporation. All rights reserved