Matanbuchus Malware

Date: 15th June 2024 | Severity: High

Summary

Researchers at eSentire have noticed a rise in observations of Matanbuchus malware. The loader-type malware known as Matanbuchus was first discovered in 2021. It has been used to launch several secondary payloads, including Danabot, Qakbot, and Cobalt Strike. In recent findings, malicious web-browser advertising (Malvertising) were utilized to drive viewers to threat actor-controlled web pages. Users were asked to download a ZIP file from the website. Matanbuchus is deployed after extracting and interacting with the ZIP file's contents. All recent instances were interrupted prior to the delivery of a secondary payload.

Attack Vectors

- In these incidents, when searching for "fund claim" related information, malicious Google ads directed users to an attacker-controlled page; it is suspected that users are prompted to enter personal information such as their name.
- Users are then directed to download a ZIP file; the downloaded file includes the user's name to add a sense of legitimacy to the download. Upon extracting and executing the JavaScript file from the ZIP archive, the script downloads and executes a Windows Installer package (MSI) which is used to deploy the Matanbuchus DLL payload. All incidents were identified and remediated at this point, as such, eSentire did not observe the deployment of secondary payloads.
- While Matanbuchus has previously led to the delivery of Danabot, Qakbot, and Cobalt Strike, it is possible that alternative malware would be delivered if the incident was not quickly remediated. It should be noted that Danabot, Qakbot, and Cobalt Strike are all known precursors to ransomware deployment.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 2981CCAE916613B8AADC9EF7F54EA5CA29A93558 • BDB194484F54FF4DC85DF6D9CE6C61DB1580C2AA • CD775E19BB053BB84BCFD5C8ABB30B8A1BF35EF1
URL	• hxxps[:]//]treasuryfinance[.]org/report

IP address	• 194[.]67[.]193[.]205 • 193[.]109[.]85[.]174 • 194[.]67[.]193[.]201 • 194[.]67[.]193[.]202 • 194[.]67[.]193[.]203 • 194[.]67[.]193[.]204 • 194[.]67[.]193[.]234 • 194[.]67[.]193[.]235 • 194[.]67[.]193[.]24	• 194[.]67[.]193[.]25 • 194[.]67[.]193[.]66 • 194[.]67[.]193[.]67 • 194[.]67[.]193[.]68 • 194[.]67[.]193[.]69 • 194[.]67[.]193[.]70 • 194[.]67[.]193[.]71 • 8[.]209[.]103[.]236 • 8[.]215[.]3[.]107

Recommendation

- Exercise caution when visiting websites or downloading content from the Internet Where possible, avoid visiting sponsored links.
- Educate users regarding browser-based malware delivery methods such as malvertising Fake “fund claim” website lured users to download malicious ZIP file in the recent Matanbuchus incidents.
- Avoid extracting malicious ZIP archives, and executing LNK files, or script files without conducting thorough analysis to mitigate the risk of malware infiltration.
- Stay vigilant against recent campaigns that entice users to download malicious ZIP archives containing JavaScript (JS) files, implementing safeguards to block such downloads.
- Ensure defense measures are in place to detect and flag arbitrary MSI file downloads and executions initiated by untrusted scripts.
- Implement robust defense-in-depth measures, to effectively detect any secondary payload or malware loaded by Matanbuchus, including: EDR solutions, Network defense Event data logging.

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.esentire.com/security-advisories/matanbuchus-malware