Mphasis
The Next Applied

Fake Google Chrome Errors Trick You into Running Malicious Powershell Scripts

Date: 18th June 2024 | Severity: High

Summary

A new malware distribution campaign uses fake Google Chrome, Word, and OneDrive errors to trick users into running malicious PowerShell “fixes” that install malware.

The new campaign was observed being used by multiple threat actors, including those behind ClearFake, a new attack cluster called ClickFix, and the TA571 threat actor, known for operating as a spam distributor that sends large volumes of email, leading to malware and ransomware infections.

Attack Vectors

- In this first case, associated with the threat actors behind ClearFake, users visit a compromised website that loads a malicious script hosted on the blockchain via Binance’s Smart Chain contracts.
- This script performs some checks and displays a fake Google Chrome warning stating a problem displaying the webpage. The dialog then prompts the visitor to install a “root certificate” by copying a PowerShell script into the Windows Clipboard and running it in a Windows PowerShell (Admin) console.
- The second attack chain is associated with the ‘ClickFix’ campaign and uses an injection on compromised websites that creates an iframe to overlay another fake Google Chrome error.
- Users are instructed to open “Windows PowerShell (Admin)” and paste the provided code, leading to the same infections mentioned above.
- Finally, an email-based infection chain using HTML attachments resembling Microsoft Word documents prompts users to install the “Word Online” extension to view the document correctly.
- The error message offers “How to fix” and “Auto-fix” options, with “How to fix” copying a base64-encoded PowerShell command to the clipboard, instructing the user to paste it into PowerShell.
- Auto-fix” uses the search-ms protocol to display a WebDAV-hosted “fix.msi” or “fix.vbs” file on a remote attacker-controlled file share.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 9701fec71e5bbec912f69c8ed63ffb6dba21b9cca7e67da5d60a72139c1795d1 • 07e0c15adc6fcf6096dd5b0b03c20145171c00afe14100468f18f01876457c80
Domain	• hxxps://cdn3535[.]shop/1[.]zip • hxxps://lashakhazhalia86dancer[.]com/c[.]txt • hxxp://languangjob[.]com/pandstvx • hxxp://languangjob[.]com/pandstvx • hxxps://oazevents[.]com/loader[.]html • hxxps://rtattack[.]baqebei1[.]online/df/tt

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

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 Links

- https://www.bleepingcomputer.com/news/security/fake-google-chrome-errors-trick-you-into-running-malicious-powershell-scripts/
- https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn

Copyright © Mphasis Corporation. All rights reserved