AL2024_10 Fake Google Chrome errors trick you into running malicious PowerShell scripts (18th June 2024)

Description

A new malware distribution campaign has emerged, using fake Google Chrome, Microsoft Word, and OneDrive errors to trick users into executing malicious PowerShell scripts. This campaign has been identified as multiple threat actors, including ClearFake, ClickFix, and TA571, known for spreading malware and ransomware through large-scale spam emails. The campaign employs sophisticated social engineering techniques, presenting seemingly legitimate error messages that prompt users to run harmful scripts under the guise of fixing browser or application issues.

Attack Details

The attack leverages website overlays and compromised websites to display fake error messages. These messages instruct users to copy and paste a PowerShell "fix" into a Windows PowerShell (Admin) prompt. The attack requires significant user interaction, relying on clever social engineering to appear legitimate.

Proofpoint analysts have identified three distinct attack chains:

1. **ClearFake Campaign:**

   Users visit a compromised website loading a malicious script hosted on the blockchain via Binance's Smart Chain contracts.

   The script checks the device and displays a fake Google Chrome warning, prompting users to install a "root certificate" via a PowerShell script.

   When executed, the script flushes the DNS cache, removes clipboard content, displays a decoy message, and downloads additional payloads, including info-stealers.

2. **ClickFix Campaign:**

   Uses iframe injections on compromised websites to overlay fake Google Chrome errors. Users are instructed to open "Windows PowerShell (Admin)"

and paste provided code, leading to infections with various malware, including DarkGate, Matanbuchus, and others.

3. **Email-Based Infection Chain:**

   HTML attachments in spam emails resemble Microsoft Word documents.Users are prompted to install the "Word Online" extension or follow "How to fix" instructions, copying a base64-encoded PowerShell command. The command downloads and executes an MSI file or a VBS script, leading to Matanbuchus or DarkGate infections.

Indicators of Compromise (IOCs)

Below are some of the methods of detecting this malicious campaign:

- Malicious Domains and websites hosting fake error messages and PowerShell scripts.
- Malicious URLs involved in downloading additional payloads.
- PowerShell commands instructing users to run scripts that modify system settings, download malware, or install certificates.
- Payloads such as DarkGate, Matanbuchus, NetSupport, Amadey Loader, XMRig, clipboard hijackers, Lumma Stealer.
- File Types such as HTML attachments in spam emails, Base64-encoded PowerShell commands, and MSI and VBS files are used in infection chains.

Recommendations

To protect against these sophisticated malware campaigns, the Guyana National CIRT recommends that users and organizations should take the following precautions:

1. User Awareness and Training:
   - Educate users about the dangers of executing PowerShell commands from untrusted sources.
   - Highlight the risks associated with downloading and running scripts from error messages.
2. Email Security:
   - Implement robust email filtering to detect and block malicious attachments and links.

- Regularly update and configure email security solutions to recognize the latest phishing tactics.

3. Browser and System Security:
   - Enable security features in browsers to block malicious scripts and overlays.
   - Keep software, browsers, and operating systems updated with the latest security patches.
4. Endpoint Protection:
   - Deploy advanced endpoint protection solutions that can detect and block malicious PowerShell activity.
   - Regularly update antivirus and anti-malware software.
5. Network Security:
   - Monitor network traffic for signs of unusual activity, such as unexpected PowerShell executions or connections to known malicious domains.
   - Use firewall rules and intrusion detection systems to identify and block suspicious behaviour.

Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2024, June 17). Fake Google Chrome errors trick you into running malicious PowerShell scripts. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/fake-google-chrome-errors-trick-you-into-running-malicious-powershell-scripts/
- The Hindu Bureau. (2024, June 18). Cybercriminals use fake Google Chrome, Microsoft Word errors to spread info-stealing malware. Retrieved from The Hindu. https://www.thehindu.com/sci-tech/technology/internet/cybercriminals-use-fake-google-chrome-microsoft-word-errors-to-spread-info-stealing-malware/article68303710.ece#:~:text=The%20campaign%20uses%20error%20messages,malware%20onto%20a%20user's%20device.