AL2024_24 Google Chrome Enhances Security with New Warnings for Risky Password-Protected Archives (25th July 2024)

Description

Google Chrome has introduced a new two-tier warning system aimed at improving user security when downloading password-protected files. This enhancement utilizes AI-powered malware verdicts from Google's Safe Browsing service to provide detailed alerts, helping users understand and respond to potential threats more effectively.

Details

Chrome's new system offers two levels of warnings: one for suspicious files with lower confidence verdicts and unknown risks, and another for dangerous files with high confidence verdicts and significant risks. These warnings are distinguished by different icons, colors, and text, allowing users to quickly identify and respond to threats. For users with Enhanced Protection enabled, Chrome now sends suspicious files to Google's servers for deeper scans, providing extra protection with minimal user friction.

Indicators of Compromise (IoCs)

- Suspicious File Warnings: Alerts for files with lower confidence verdicts indicating potential but uncertain risks.
- Dangerous File Warnings: Alerts for files with high confidence verdicts indicating significant threats.
- Password Requests: Prompts for entering passwords for encrypted files before scanning, ensuring the integrity of the scan process.

Remediation

- Enable Enhanced Protection: Users should enable Enhanced Protection mode in Chrome's Safe Browsing settings for optimal security.
- Respond to Warnings: Heed Chrome's warnings promptly and avoid bypassing alerts without thorough consideration.

- Password Management: Be cautious about sharing passwords for sensitive archives, especially in corporate environments. Train employees to handle such requests appropriately to prevent data leaks.
- Regular Updates: Ensure Chrome is regularly updated to benefit from the latest security enhancements and protections.
- These updates to Google Chrome aim to enhance user safety by providing clearer and more actionable warnings for potentially malicious downloads, thereby reducing the risk of security breaches and data compromises.

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

References

- Gatlan, S. (2024, July 25). Google Chrome now asks for passwords to scan protected archives. R from *BleepingComputer*. https://www.bleepingcomputer.com/news/google/google-chrome-now-warns-about-risky-password-protected-archives/
- The Hacker News. (n.d.). *New Chrome feature scans Password-Protected files for malicious content*. https://thehackernews.com/2024/07/new-chrome-feature-scans-password.html