BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

January 4, 2024

Malware using Google MultiLogin Exploit to Maintain Access

SUMMARY

A hidden Google OAuth feature known as MultiLogin is being used to compromise and control user sessions, providing persistent access across Google services even after users reset their password. The discovery of this technique was initially identified by the hacker group PRISMA and posted on their Telegram channel on October 20, 2023. The exploit has since been integrated into multiple malware platforms, including Lumma, Rhadamanthys, Stealc, Meduza, RisePro, and WhiteSnake.

TECHNICAL DETAILS

Multiple malware strains are exploiting the "MultiLogin" vulnerability, reviving expired authentication cookies, granting unauthorized and persistent access to user accounts even after password changes. Session cookies contain vital authentication data and typically have a set lifespan to limit misuse. However, cybersecurity group CloudSEK performed an in-depth analysis to find that the intricate workings of this zero-day exploit uses a component of the Gaia Auth API, designed for seamless account synchronization across various Google services, including platforms like YouTube. CloudSEK's research also found that the restoration of chrome account credentials within browser authentication cookies worked for multiple Google domains.

The malware strains extract crucial details, such as the service (GAIA ID) and encrypted_token, from Chrome profiles associated with a Google account. These tokens are then decrypted by Chrome's 'Local State' file, which also deciphers saved browser passwords. With the token:GAIA pairs, threat actors use the MultiLogin endpoint to revive expired Google Service cookies, creating persistent unauthorized access to the compromised accounts.

Google's response was that users possess the capability to nullify these compromised sessions by simply logging out from the impacted browser or remotely revoking access via the user's device management page. Though Google disagreed with some of these findings, they advised users to activate Enhanced Safe Browsing in Chrome, modify passwords to thwart potential misuse, and diligently monitor account activities for any anomalous sessions originating from unfamiliar IP addresses or locations".

RECOMMENDATIONS

- Immediately change your Google account password to invalidate any potential compromise resulting from the exploit.
- Enable Enhanced Safe Browsing in Google Chrome to add an extra layer of protection against phishing attempts and malware downloads.
- Regularly monitor your Google account activity for any suspicious sessions or unauthorized access, especially from unfamiliar IP addresses or locations.
- If you suspect your account might be compromised, log out from all active sessions in the impacted browser. This will help invalidate any stolen sessions.
- Remotely revoke access to your Google account sessions through the user's device management page. This ensures that even if a session is compromised, you can revoke access remotely.
- Ensure that your web browser, especially Google Chrome, is up to date. Regularly update your operating system and security software to patch vulnerabilities and protect against potential exploits.
- Enable two-factor authentication for an additional layer of security. This ensures that even if your password is compromised, an extra verification step is required for access.

- Stay informed about security updates from Google and other relevant sources. Implement updates promptly to benefit from the latest security enhancements and patches.

REFERENCES

- https://www.cloudsek.com/blog/compromising-google-accounts-malwares-exploiting-undocumented-oauth2-functionality-for-session-hijacking
- https://www.bleepingcomputer.com/news/security/malware-abuses-google-oauth-endpoint-to-revive-cookies-hijack-accounts/#google_vignette
- https://thehackernews.com/2024/01/malware-using-google-multilogin-exploit.html