Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

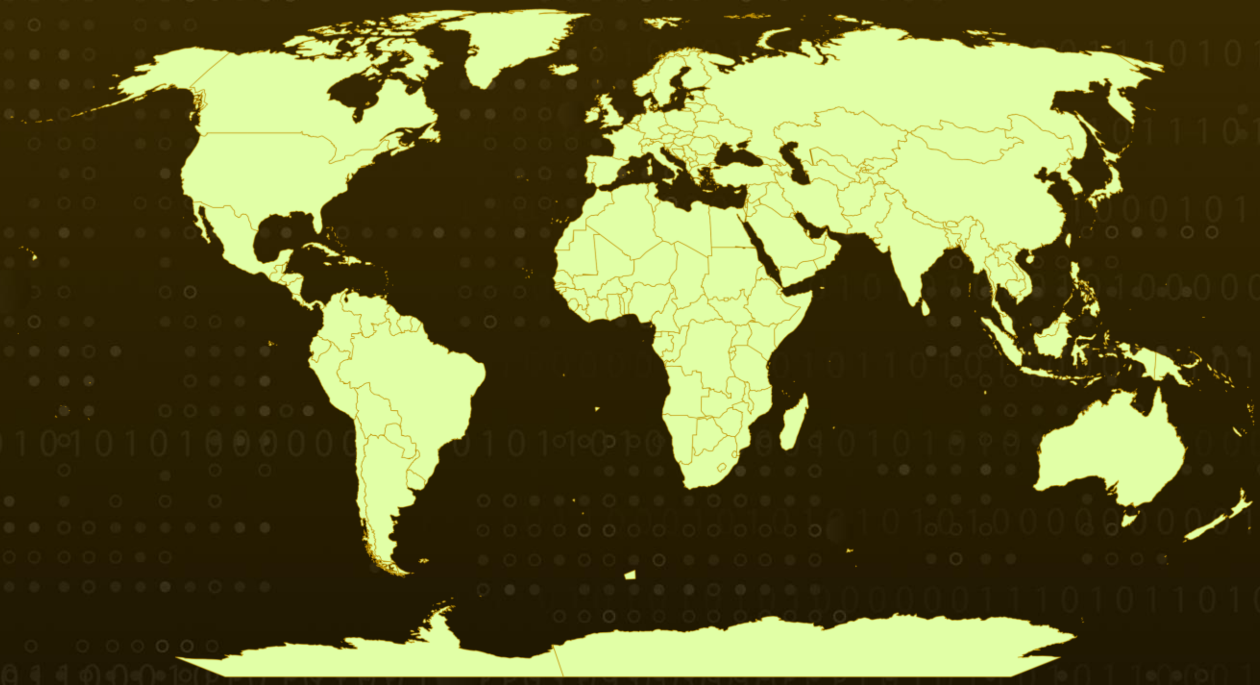
Malware Leveraging Google OAuth for Persistent Account Access

Date of Publication	Admiralty Code	TA Number
January 04, 2023	A1	TA2024003

Summary

First Seen: October 20, 2023
Malware: Lumma Infostealer, Rhadamanthys, Risepro, Meduza and Stealc Stealer
Attack Region: Worldwide
Attack: Information-stealing malware is actively exploiting an undisclosed Google OAuth endpoint called MultiLogin. This technique was initially disclosed by a threat actor named PRISMA on their Telegram channel and has subsequently been integrated into various malware-as-a-service (MaaS) stealer families.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 Information-stealing malware is taking advantage of an undisclosed Google OAuth endpoint called 'MultiLogin' to hijack authentication cookies and access users' accounts, even when the account password has been reset. Session cookies, a specialized type of browser cookie containing authentication data, allow individuals to log into websites and services seamlessly without needing to enter their credentials.

#2 In October 2023, a threat actor known as 'Prisma' disclosed a critical exploit that enables cybercriminals to illicitly access Google accounts even after legitimate owners have logged out, reset their passwords, or experienced session expiration. Several information-stealing malware strains, particularly Lumma and Rhadamanthys, have exploited this undisclosed flaw, claiming the ability to restore expired Google authentication cookies stolen during attacks.

#3 Consequently, other malicious entities like Risepro, Meduza, White Snake, and Stealc Stealer have embraced and implemented this technique. The Stealer specifically targets Chrome's 'token_service' table in WebData to extract tokens and account IDs associated with logged-in Chrome profiles.

#4 The compromise of stolen sessions can be resolved by simply signing out of the affected browser or remotely revoking access via the user's devices page. Currently, multiple malware-as-a-service (MaaS) stealer families are diligently working on updates, highlighting a concerning trend of rapid integration within various Infostealer collectives.

Recommendations

Check for Unusual Devices or Sessions: Periodically review the list of devices and active sessions associated with your Google account. If any unfamiliar devices or sessions are identified, take immediate action to remove and secure the account.

Monitor Account Activity: Regularly check your account activity and review your login history. If any suspicious activities are detected, take immediate action, such as changing the password and logging out of all devices.

Regularly Update Passwords: It is crucial to regularly update passwords for all online accounts. Change passwords every few months to minimize the risk of unauthorized access.

Enable Two-Factor Authentication (2FA): Implementing 2FA adds an extra layer of security to your accounts. A second form of verification is required, significantly reducing the chances of unauthorized access.

Review App Permissions: Regularly review the permissions granted to apps and services, especially those connected to Google accounts. Remove unnecessary or suspicious permissions to limit potential points of exploitation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1587.001 Malware	T1005 Data from Local System
T1140 Deobfuscate/Decode Files or Information	T1587 Develop Capabilities	T1588 Obtain Capabilities	T1555 Credentials from Password Stores
T1185 Browser Session Hijacking	T1550.004 Web Session Cookie	T1531 Account Access Removal	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	515ad6ad76128a8ba0f005758b6b15f2088a558c7aa761c01b312862e9c1196b, dfce2d4d06de6452998b3c5b2dc33eaa6db2bd37810d04e3d02dc931887cfddd, bb8bbcc948e8dca2e5a0270c41c062a29994a2d9b51e820ed74d9b6e2a01ddcf, 22a67f510dfb7ca822b5720b89cd81abfa5e63fefa1cdc7e266fbcbb0698db33, 4fd469d08c051d6997f0471d91ccf96c173d27c8cff5bd70c3f2c5008faa786f, 633b0fe4f3d2bfb18d4ad648ff223fe6763397daa033e9c5d79f2cae89a6c3b2,

TYPE	VALUE
SHA256	50b1f29ccdf727805a793a9dac61371981334c4a99f8fae85613b3ee57b186d2, 01609701a3ea751dc2323bec8018e11742714dc1b1c2dcb39282f3c4a4537c7d, a905226a2486ccc158d44cf4c1728e103472825fb189e05c17d998b9f5534d63, ed713454c20844522304c49cfe25fe1490418c300e5ab0c9fca431ede1e91d7b, f82ec2246dde81ca9edb69fb9c7ce3f7101f5ffcdc3bdb86fea2a5373fb026fb, ee4a487e78f23f5dffc35e73aeb9602514ebd885eb97460dd26635f67847bd16, fcb00beaa88f7827999856ba12302086cadbc1252261d64379172f2927a6760e, a87032195e38892b351641e08c81b92a1ea888c3c74a0c7464160e86613c4476, 3d010e3fce1b2c9ab5b8cc125be812e63b661ddcbde40509a49118c2330ef9d0, ecab35dfa6b03fed96bb69ffcecd11a29113278f53c6a84adced1167b66abe62, 5890b47df83b992e2bd8617d0ae4d492663ca870ed63ce47bb82f00fa3b82cf9, 2b6faa98a7617db2bd9e70c0ce050588c8b856484d97d46b50ed3bb94bdd62f7, f1f33618bbb8551b183304ddb18e0a8b8200642ec52d5b72d3c75a00cdb99fd4, e8b221cba5c3598522f1ebd2b5e52b2f45699a1965b5dd677a9b9d074677873e, 356019c5f0ab89bcaff1639b2b2a427d7777fcfa13c09f889ef5ea8eb1c031c7, 5aa9cbeb84e41ab814e989920c76278d94827fb490f05d7421082570d1a1a3bb, e6e1106fec7137b46da15bdd0853b1b9a6104bce649a24145793e4d451261c6b, d63a83fb534fd92df1de5373ce6fa7febf6ca715c7528a2a806de49da2889078
MD5	fa1ded1ed7c11438a9b0385b1e112850, 74ee6ac5aceaba962b45d8295db06823, 6fef55e48e2392dbe72df975eeaa5030, d8625b338b13c0a1703ae2cd0059540f

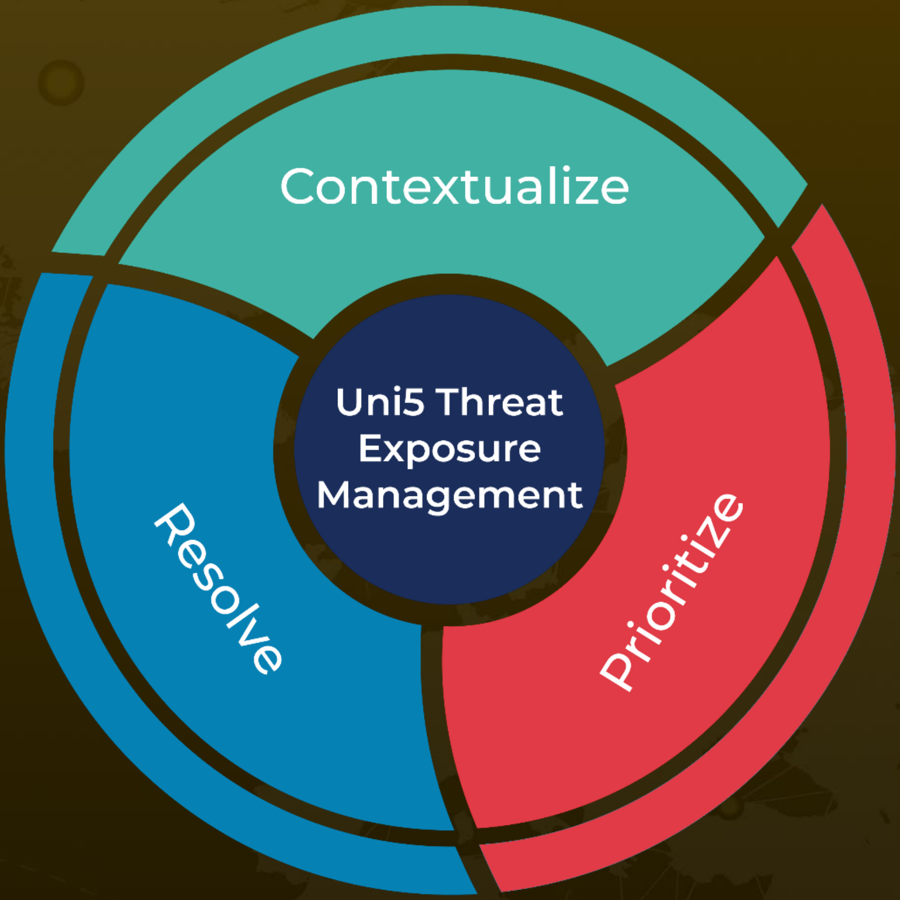
References

https://www.cloudsek.com/blog/compromising-google-accounts-malwares-exploiting-undocumented-oauth2-functionality-for-session-hijacking

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 4, 2024 • 1:00 AM

More at www.hivepro.com