Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

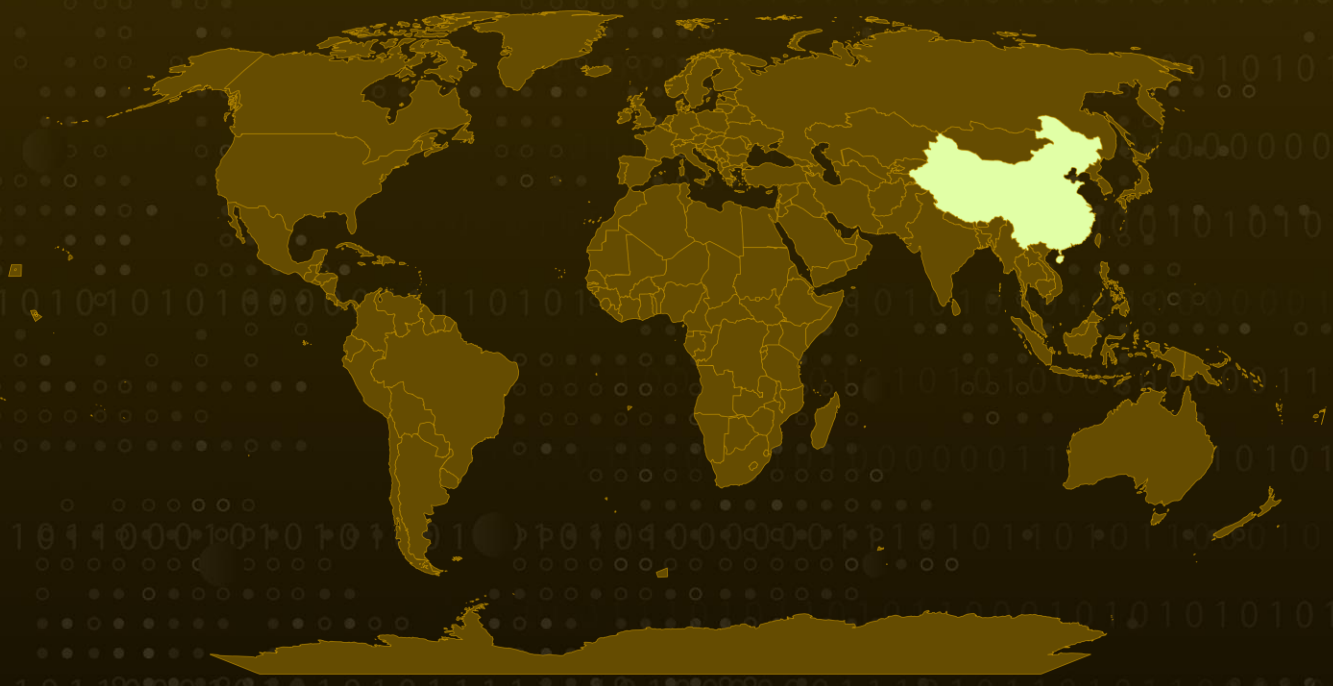
Malicious Google Ads Target Chinese Users, Covertly Delivering RATs

Date of Publication	Admiralty Code	TA Number
January 30, 2024	A1	TA2024038

Summary

Attack Discovered: January 2024
Attack Region: China
Targeted Platform: Telegram, LINE
Malware: PlugX, Gh0st RAT
Attack: Chinese-speaking users are being targeted in an ongoing malvertising campaign that leverages Google ads. The threat actor employs Google advertiser accounts to create deceptive ads that lure users into downloading Remote Administration Trojans (RATs). The malicious ads are designed to mimic popular messaging platforms, redirecting users to pages where the unsuspecting victims inadvertently download the RATs.

Attack Regions



Attack Details

#1 Chinese-speaking users have been targeted in a continuous campaign of malicious advertisements masquerading as popular messaging services such as Telegram or LINE. These deceptive ads aim to trick users into downloading malware. It's worth noting that apps like Telegram have faced strict restrictions and were previously banned in China.

#2 The threat actor is leveraging Google advertiser accounts for malicious activities, creating deceptive ads that lead unsuspecting users to pages where they unwittingly download Remote Administration Trojans (RATs). Through these programs, attackers can gain full control of a victim's computer and potentially install additional malware.

#3 Notably, a sponsored search for 'telegram' displays numerous ads, hinting at potential takeover by threat actors. These actors exploit Google infrastructure, to download links or redirect users to other controlled websites.

#4 Payloads were discovered in MSI format and were found to be employing DLL side-loading to evade detection and execute malicious code. These DLLs were digitally signed, with a certificate previously used to sign a PlugX RAT sample in a prior attack. While certain malware distributed in this campaign was new, others were variants of the Gh0st RAT observed in previous attacks.

#5 The threat actor persistently introduces new payloads and infrastructure for command-and-control, prioritizing quantity over quality. While online advertisements can be leveraged for targeting specific audiences, they are also susceptible to abuse by threat actors. The true intentions of the threat actor remain unknown, data collection and espionage appear to be among their potential motives.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
T1566 Phishing	**T1566.002** Spearphishing Link	**T1553** Subvert Trust Controls	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1036** Masquerading	**T1204** User Execution	**T1204.002** Malicious File
T1218 System Binary Proxy Execution	**T1218.007** Msiexec		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	telagsmn[.]com, teleglren[.]com, teleglarm[.]com, 5443654[.]site, 5443654[.]world

TYPE	VALUE
SHA256	63b89ca863d22a0f88ead1e18576a7504740b2771c1c32d15e2c04141795d79a, a83b93ec2a5602d102803cd02aecf5ac6e7de998632afe6ed255d6808465468e, acf6c75533ef9ed95f76bf10a48d56c75ce5bbb4d4d9262be9631c51f949c084, ec2781ae9af54881ecbbbfc82b34ea4009c0037c54ab4b8bd91f3f32ab1cf52a, c08be9a01b3465f10299a461bbf3a2054fdff76da67e7d8ab33ad917b516ebdc
IPs	47.75.116[.]234:19858, 216.83.56[.]247:36061, 45.195.148[.]73:15628

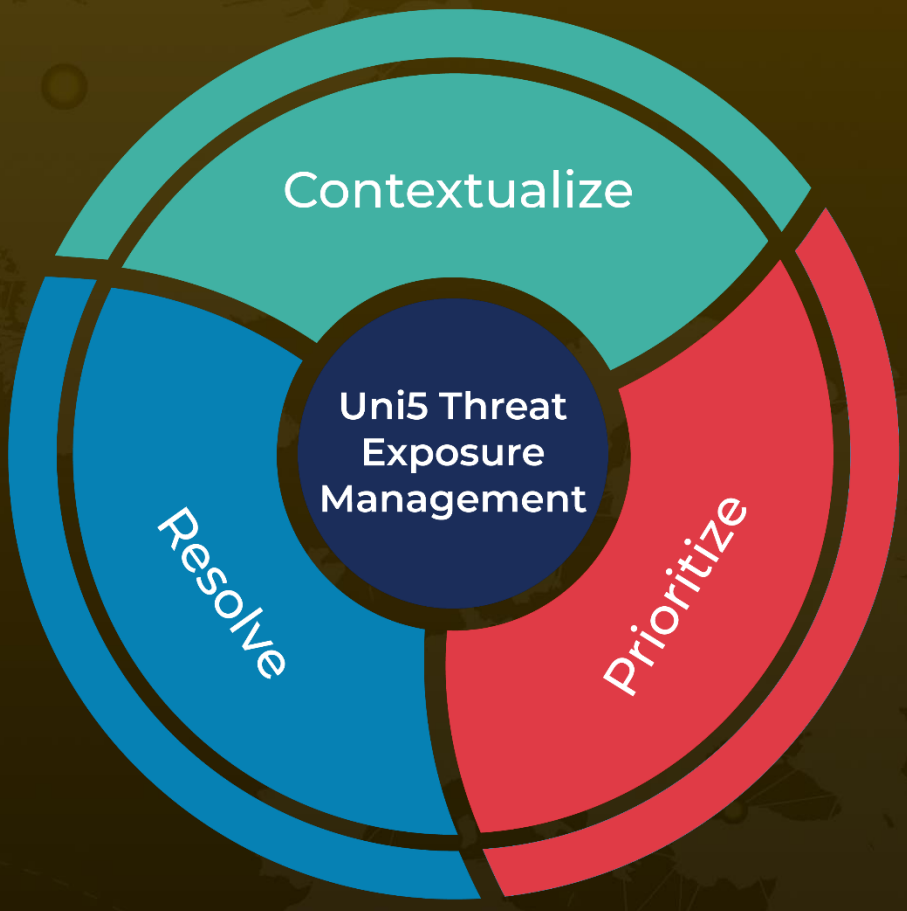
References

https://www.malwarebytes.com/blog/threat-intelligence/2024/01/malicious-ads-for-restricted-messaging-applications-target-chinese-users

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 30, 2024 • 4:00 AM

More at www.hivepro.com