Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

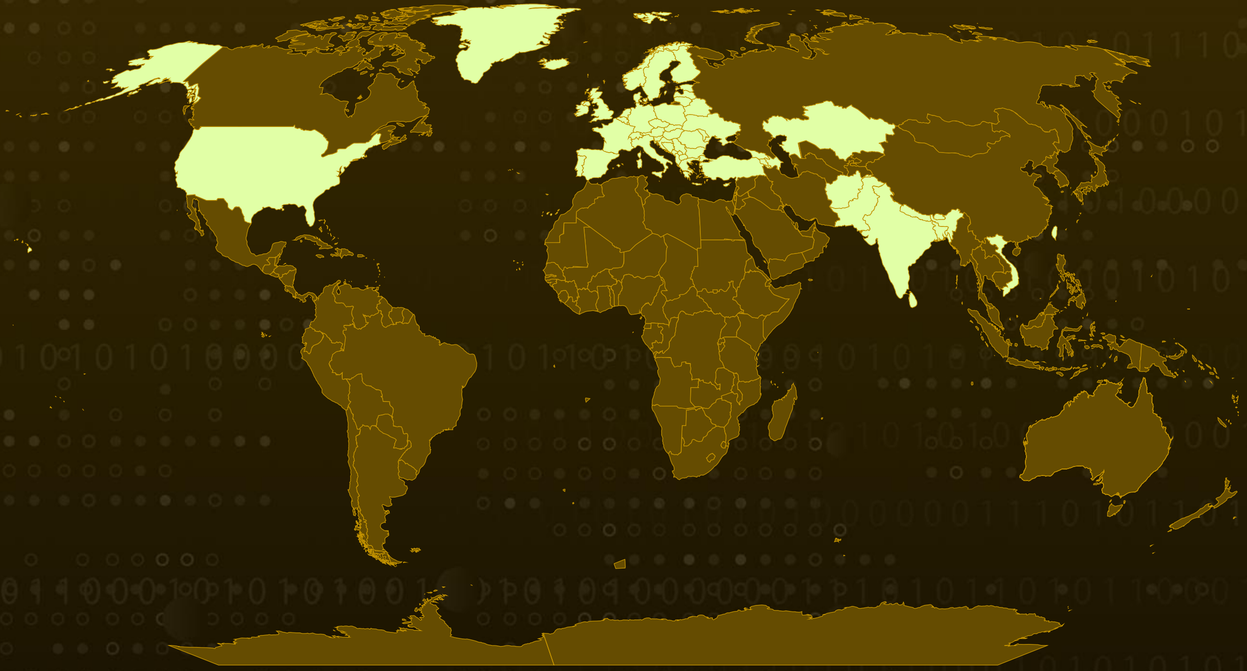
Cloud Services Transformed into Cyber Weapons: New Wave of Espionage

Date of Publication	Admiralty Code	TA Number
August 8, 2024	A1	TA2024304

Summary

Backdoor: GoGra, Grager, MoonTag, Onedrivetools
Targeted Regions: Afghanistan, Bangladesh, Bhutan, Hong Kong, India, Maldives, Nepal, Pakistan, Sri Lanka, Taiwan, Vietnam, U.S. and Europe
Targeted Industries: Media, IT, Military
Attack: Cybercriminals are increasingly leveraging legitimate cloud services like Microsoft OneDrive and Google Drive in their attacks, creating discreet and cost-effective infrastructures that evade detection. Recent campaigns have highlighted this trend, with malware such as GoGra, Grager, and MoonTag being deployed against organizations. This growing trend underscores the need for heightened scrutiny of cloud service traffic as cyber espionage groups continue to exploit these trusted platforms for malicious activities.

Attack Regions



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

Attack Details

#1 Adversaries are exploiting legitimate cloud services in their attacks, a pattern that has been accelerating as these actors recognize the advantages of using trusted platforms like Microsoft OneDrive or Google Drive. By leveraging such well-known services, attackers can establish a discreet and cost-effective infrastructure, making their activities less likely to attract attention.

#2 Traffic associated with these trusted services is often subject to less scrutiny compared to communications with attacker-controlled infrastructure, providing a significant operational advantage to these malicious entities. One notable campaign involved the deployment of a new backdoor named GoGra, written in the Go programming language, against a media organization in South Asia.

#3 GoGra interacts with its command-and-control (C&C) server through the Microsoft Graph API, hosted on Microsoft's mail services. This malware is believed to be the work of Harvester, a nation-state-backed group known for targeting organizations in South Asia.

#4 Additionally, a backdoor named Grager was used in attacks against organizations in Taiwan, Hong Kong, and Vietnam. Grager can execute a variety of commands, including file downloading/uploading, executing files, and gathering file system information. The use of Tonerjam malware as a launcher for Grager indicates a possible connection to UNC5330, a suspected Chinese espionage group.

#5 Another emerging backdoor called MoonTag, which appears to be in its early stages is based on code found in a Google Group and is likely associated with a Chinese-speaking threat actor, given the language and infrastructure involved. In the U.S. and Europe, a backdoor known as Onedrivetools has been deployed against IT services companies.

Recommendations

Implement AV Solutions: Utilize Anti-Virus solutions to monitor and respond to suspicious activities on endpoints, providing real-time detection and automated responses to potential threats.

Monitor and Analyze Traffic: Implement advanced network monitoring tools to detect unusual traffic patterns that may indicate the abuse of services like Cloudflare Tunnels. Regularly review and analyze network traffic logs for anomalies or unauthorized use of tunneling services.

Utilize Application Control and Whitelisting: Implement application whitelisting to allow only approved applications to run on endpoints. Use application control solutions to monitor and block unauthorized or suspicious applications.

User Education and Awareness: Educate users about the risks of suspicious GitHub repositories and the importance of cautious behavior when receiving files and links. Promote awareness of the steps needed to enable the installation of unknown apps, highlighting the associated risks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	TA0010 Exfiltration	T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage
T1585 Establish Accounts	T1585.003 Cloud Accounts	T1608 Stage Capabilities	T1608.001 Upload Malware
T1608 Stage Capabilities	T1608.002 Upload Tool	T1059 Command and Scripting Interpreter	T1059.009 Cloud API

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f, f1ccd604fcdc0034d94e575b3709cd124e13389bbee55c59cbbf7d4f3476e214,

TYPE	VALUE
SHA256	9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9, ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985, 97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824, f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274, 582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede, 79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6, 4057534799993a63f41502ec98181db0898d1d82df0d7902424a1899f8f7f9d2, a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcba6, 527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14, fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb, 30093c2502fed7b2b74597d06b91f57772f2ae50ac420bcaa627038af33a6982
URL	hxxp[:]//7-zip[.]tw/a/7z2301-x64[.]msi, hxxp[:]//7-zip[.]tw/a/7z2301[.]msi
Domain	7-zip[.]tw, 30sof[.]onedumb[.]com
IPv4	103[.]255[.]178[.]200, 157[.]245[.]159[.]135, 89[.]42[.]178[.]13

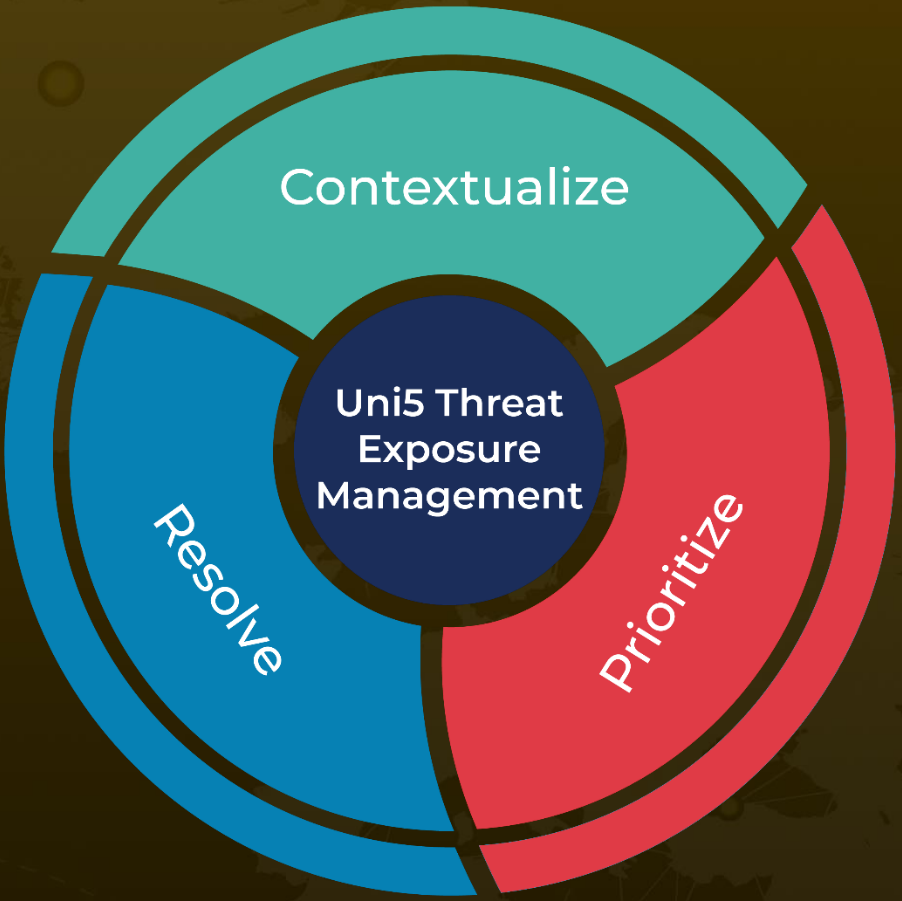
References

https://symantec-enterprise-blogs.security.com/threat-intelligence/cloud-espionage-attacks

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

August 8, 2024 • 9:00 PM

More at www.hivepro.com