Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

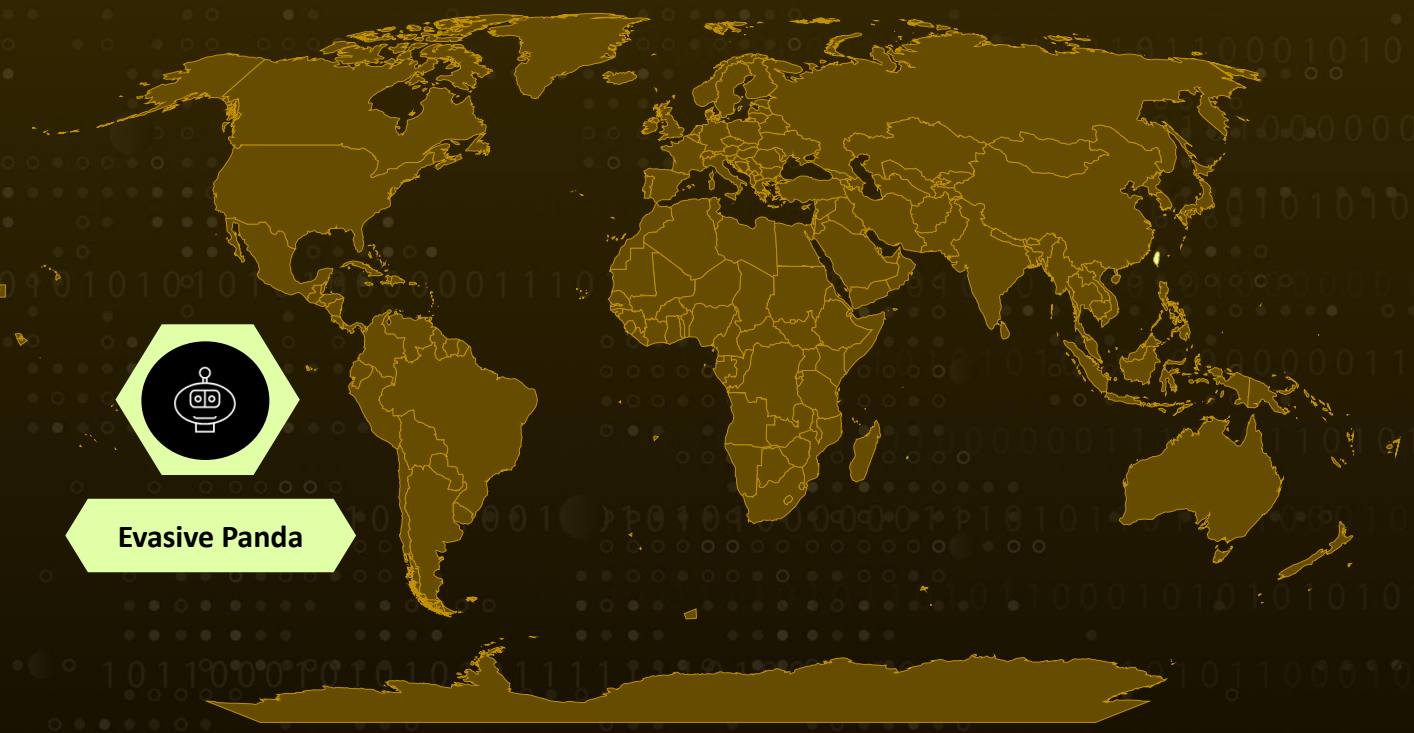
Evasive Panda's CloudScout: A Stealthy Threat to Cloud Security

Date of Publication	Admiralty Code	TA Number
October 30, 2024	A1	TA2024415

Summary

First Seen: 2022
Targeted Countries: Taiwan
Malware: CloudScout, MgBot, Nightdoor
Targeted Industries: Government and Religious organizations
Affected Products: Google Drive, Gmail, and Microsoft Outlook
Threat Actor: Evasive Panda (Bronze Highland, Daggerfly, Storm Cloud, StormBamboo)
Attack: Evasive Panda, a Chinese APT group, uses a toolset called CloudScout to infiltrate Taiwanese organizations by stealing session cookies from browsers. This technique bypasses authentication, allowing attackers to access cloud accounts like Gmail and Google Drive undetected. The attack starts with malicious executables that connect to command-and-control servers, deploying plugins to exfiltrate data. The modular, encrypted framework allows Evasive Panda to easily adapt and expand its capabilities. This shift to exploiting cloud platforms underscores the broader cybersecurity challenge as more organizations rely on these trusted services.

Attack Regions



Attack Details

#1 Evasive Panda, a Chinese APT group, has recently been deploying CloudScout, a toolset designed to infiltrate Taiwanese organizations by leveraging stolen session cookies from popular services like Google Drive, Gmail, and Outlook. This sophisticated approach enables attackers to bypass two-factor authentication, entering cloud accounts under legitimate-looking user sessions, making detection extremely challenging.

#2 The attack begins with the compromise of a host machine via malicious executables like doc.exe, 2.exe, and 3.exe, which deploy malware components such as Nightdoor and MgBot. These establish a connection with a command-and-control (C&C) server, which subsequently deploys additional modules (Gmck.dll and CGM.dll), including CloudScout. These modules extract browser cookies, store them in a configuration file, and use msvc_4.dll to consume and exfiltrate this data to Gmail for covert data theft.

#3 CloudScout operates through Evasive Panda's main malware, MgBot, which installs various C++ plugins to execute specific tasks. For instance, certain plugins specifically target Google Drive, Gmail, and Outlook by extracting cookies stored in browsers. Once obtained, these cookies give attackers access to sensitive data without requiring credentials.

#4 The CloudScout framework is modular and written in C#, enabling the group to tailor its functionalities precisely to the target environment. This modularity means Evasive Panda can add or adapt tools as needed, with current evidence suggesting that other undisclosed modules could further expand their operational reach. To stay undetected, the malware encrypts its configuration files with RC4, adding another layer of stealth.

#5 Active since at least 2012, Evasive Panda (also known as BRONZE HIGHLAND or StormBamboo) has a history of adaptive tactics in its cyber-espionage campaigns, evolving from supply-chain attacks to cloud-service exploitation. The development timeline of CloudScout, around 2020, aligns with other tools the group has employed, underscoring a long-term commitment to advancing its malware capabilities.

#6 This shift towards leveraging cloud services exemplifies the broader cybersecurity challenge posed by APT groups. As more organizations adopt cloud platforms, the risk of such targeted attacks increases, stressing the importance of robust monitoring and user education on credential security.

Recommendations

Strengthen Authentication Mechanisms: Ensure that all users utilize MFA, especially for accessing cloud services. This adds an extra layer of security beyond just passwords and can significantly reduce the risk of unauthorized access. Encourage the use of complex passwords that are unique to each account. Implement password management tools to help users manage their credentials securely.

Monitor and Manage Session Cookies: Establish policies for session timeouts and cookie expiration to limit the lifespan of session cookies. This can help minimize the window of opportunity for attackers. Provide training on the importance of not sharing session cookies and recognizing phishing attempts that may target cookie theft.

Enhance Cloud Security Posture: Implement cloud security solutions that offer monitoring, threat detection, and anomaly detection capabilities to identify suspicious activities in real time. Perform periodic audits of cloud configurations and access controls to ensure they adhere to best practices and compliance requirements.

Regular Software and System Updates: Ensure that all software, including operating systems, applications, and security solutions, are kept up to date with the latest patches. Regular updates close vulnerabilities that attackers can exploit, thus reducing the attack surface. Automated patch management solutions can assist in maintaining current versions across all systems.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0042 Resource Development	TA0004 Privilege Escalation	TA0002 Execution
TA0007 Discovery	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0005 Defense Evasion	T1543.003 Windows Service	T1082 System Information Discovery

T1114.002 Remote Email Collection	T1114 Email Collection	T1095 Non-Application Layer Protocol	T1041 Exfiltration Over C2 Channel
T1548 Abuse Elevation Control Mechanism	T1027 Obfuscated Files or Information	T1550.004 Web Session Cookie	T1550 Use Alternate Authentication Material
T1548.002 Bypass User Account Control	T1140 Deobfuscate/Decode Files or Information	T1036.005 Match Legitimate Name or Location	T1036 Masquerading
T1560.001 Archive via Utility	T1569.002 Service Execution	T1543 Create or Modify System Process	T1185 Browser Session Hijacking
T1539 Steal Web Session Cookie	T1560 Archive Collected Data	T1530 Data from Cloud Storage	T1583.004 Server
T1583 Acquire Infrastructure	T1587.001 Malware	T1587 Develop Capabilities	T1569 System Services
T1106 Native API			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	C70C3750AC6B9D7B033ADDEF838EF1CC28C262F3, 812124B84C5EA455F7147D94EC38D24BDF159F84, AD6C84859D413D627AC589AEDF9891707E179D6C, 3DD958CA6EB7E8F0A0612D295453A3A10C08F5FE, 547BD65EEE05D744E075C5E12FB973A74D42438F, 348730018E0A5554F0F05E47BBA43DC0F55795AC, 9B6A473820A72111C1A38735992B55C413D941EE, 621E2B50A979D77BA3F271FAB94326CCCBC009B4, C058F9FE91293040C8B0908D3DAFC80F89D2E38B, 4A5BCDAAC0BC315EDD00BB1FCCD1322737BCBEEB, 67028AEB095189FDF18B2D7B775B62366EF224A9, B3556D1052BF5432D39A6068CCF00D8C318AF146, 84F6B9F13CDCD8D9D15D5820536BC878CD89B3C8,

TYPE	VALUE
SHA1	93C1C8AD2AF64D0E4C132F067D369ECBEBAE00B7, 8EAA213AE4D482938C5A7EC523C83D2C2E1E8C0E, A1CA41FDB61F03659168050DE3E208F0940F37D8,
File Name	pmsrvd.dll, 3.exe, 1.exe, doc.exe, DJCU.dll, CommonUtilities.dll, CGM.dll, CGD.dll, COL.dll
IPv4	103[.]96[.]128[.]44

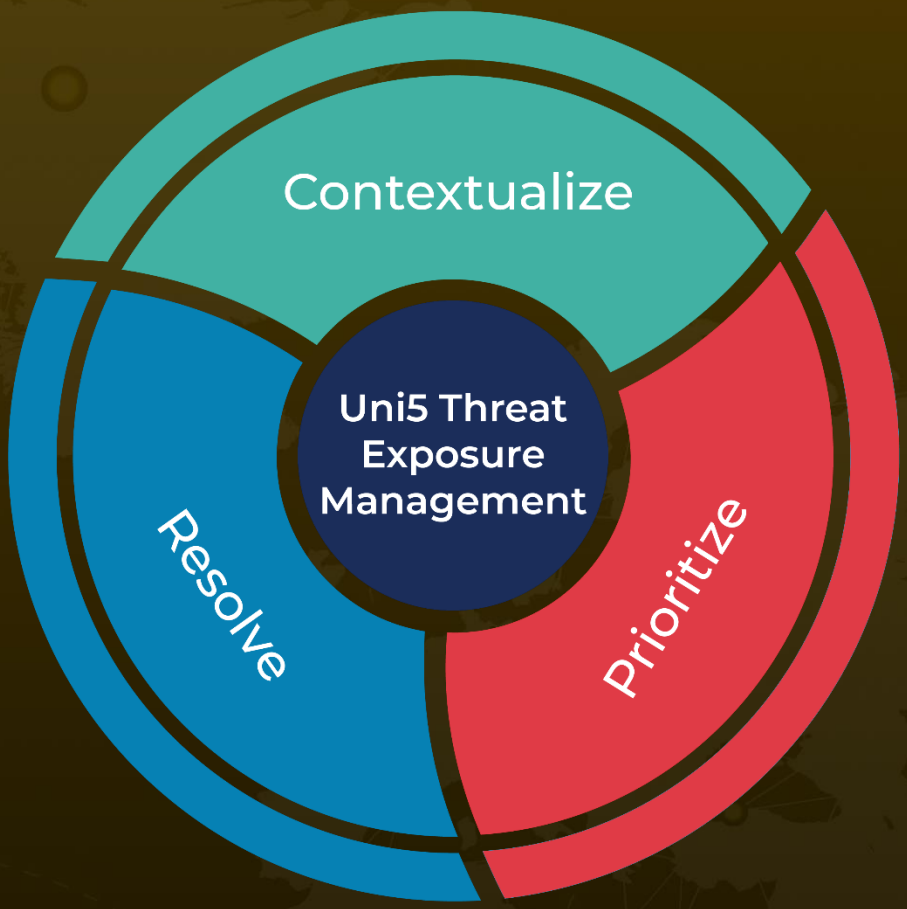
References

https://www.welivesecurity.com/en/eset-research/cloudscout-evasive-panda-scouting-cloud-services/

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

October 30, 2024 • 1:30 AM

More at www.hivepro.com