Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Evasive Panda China-Linked Cyberespionage Targeting Tibetans

Date of Publication

March 11, 2024

Admiralty Code

A1

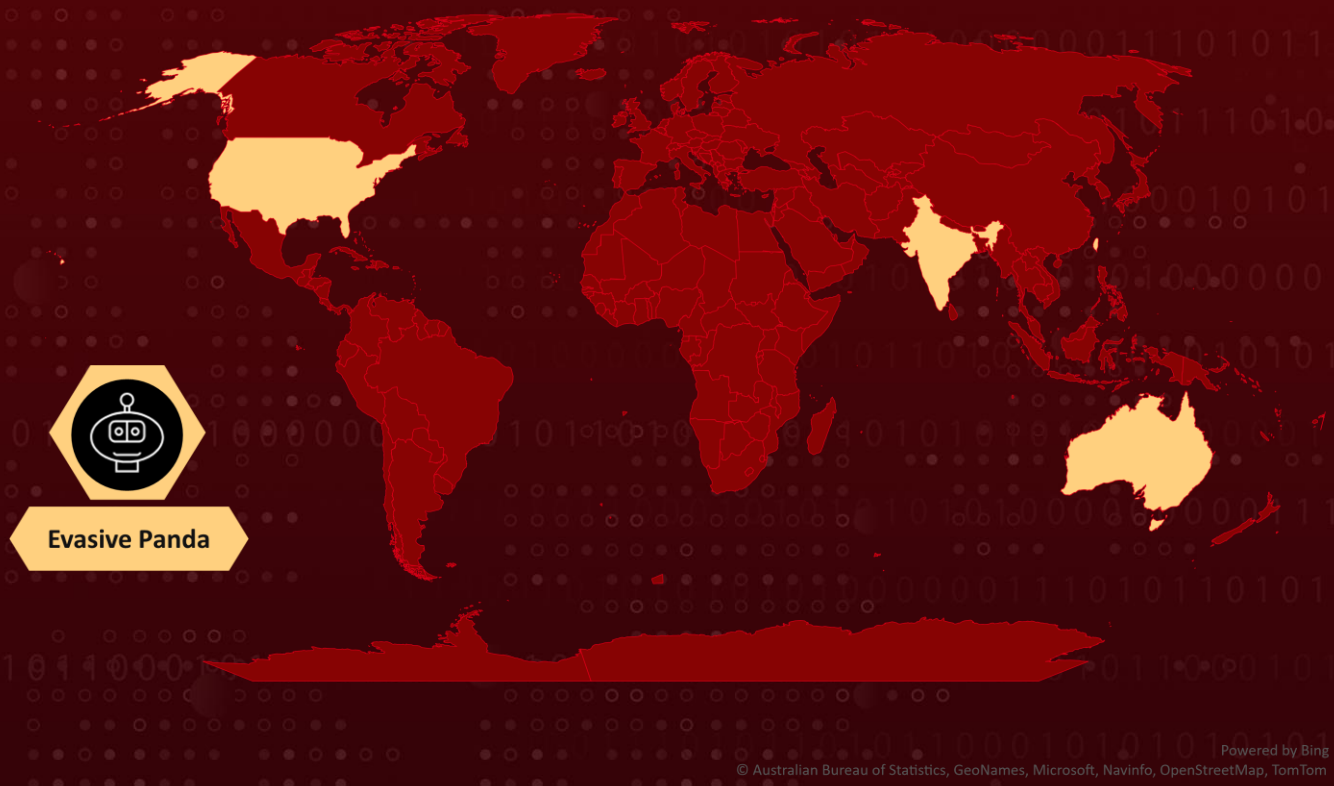
TA Number

TA2024095

Summary

Attack Began: September 2023
Threat Actor: Evasive Panda (aka Daggerfly, Bronze Highland)
Malware: MgBot, Nightdoor
Attack Region: India, Taiwan, Hong Kong, Australia, USA
Attack: Evasive Panda, a threat actor associated with China, has masterminded an intricate cyberespionage campaign targeting Tibetan users since at least September 2023. This operation employs both watering hole and supply chain attacks to achieve its objectives.

Attack Regions



Attack Details

#1 The threat actor associated with China, Evasive Panda (also known as Daggerfly and Bronze Highland), has orchestrated a sophisticated cyberespionage campaign. This operation, which involves both watering hole and supply chain attacks, has been targeting Tibetan users since at least September 2023.

#2 Evasive Panda strategically utilized the annual Kagyu Monlam Festival in India, held in late January and February 2024, to focus on the Tibetan community across various countries and territories. By employing a proprietary malware framework with a modular architecture, the group utilizes its backdoor, **MgBot**, to receive specialized modules for spying on victims and enhancing its capabilities.

#3 The attackers strategically implanted trojanized applications containing a malicious downloader for both Windows and macOS systems. The ultimate objective of these attacks is to disseminate malevolent downloaders for Windows and macOS, facilitating the deployment of a well-known backdoor, MgBot, and an undisclosed Windows implant named Nightdoor.

#4 The attackers incorporated a script into the compromised websites to validate the potential victim's IP address. If within one of the specified targeted address ranges, a deceptive error page is presented, enticing the user to download a seemingly necessary 'fix' labeled as a certificate.

#5 This file serves as a malicious downloader, initiating the subsequent phase in the compromise chain. Subsequently, the downloader or dropper retrieves the payload from the server or drops it, proceeding to execute the malicious content on the victim's machine.

#6 This results in the installation of either Nightdoor or MgBot. The backdoor boasts a range of capabilities, including gathering system information, compiling lists of installed applications and running processes, initiating a reverse shell, conducting file operations, and even uninstalling itself from the compromised system.

Recommendations

Network Segmentation: Implement network segmentation to minimize the lateral movement of attackers within the network, limiting their ability to access critical systems and data.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Zero Trust Architecture: Adopt a Zero Trust security architecture, where trust is never assumed and continuous authentication and authorization mechanisms are implemented, reducing the risk of unauthorized access.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Secure Configuration Management: Enforce secure configurations for servers, network devices, and applications, following industry best practices and security baselines to reduce the attack surface.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1583.004 Server	T1583.006 Web Services	T1584.004 Server

T1585.003 Cloud Accounts	T1587.001 Malware	T1588.003 Code Signing Certificates	T1608.004 Drive-by Target
T1189 Drive-by Compromise	T1195.002 Compromise Software Supply Chain	T1106 Native API	T1053.005 Scheduled Task
T1543.003 Windows Service	T1574.002 DLL Side-Loading	T1140 Deobfuscate/Decode Files or Information	T1562.004 Disable or Modify System Firewall
T1070.004 File Deletion	T1070.009 Clear Persistence	T1036.004 Masquerade Task or Service	T1036.005 Match Legitimate Name or Location
T1027.009 Embedded Payloads	T1055.001 Dynamic-link Library Injection	T1620 Reflective Code Loading	T1087.001 Local Account
T1083 File and Directory Discovery	T1057 Process Discovery	T1012 Query Registry	T1518 Software Discovery
T1033 System Owner/User Discovery	T1082 System Information Discovery	T1049 System Network Connections Discovery	T1560 Archive Collected Data
T1119 Automated Collection	T1005 Data from Local System	T1074.001 Local Data Staging	T1071.001 Web Protocols
T1095 Non-Application Layer Protocol	T1571 Non-Standard Port	T1572 Protocol Tunneling	T1102 Web Service
T1020 Automated Exfiltration	T1567.002 Exfiltration to Cloud Storage		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	188[.]208[.]141[.]204

TYPE	VALUE
Domains	tibetpost[.]net, www.monlamit[.]com, update.devicebug[.]com
SHA1	0a88c3b4709287f70ca2549a29353a804681ca78, 1c7df9b0023fb97000b71c7917556036a48657c5, f0f8f60429e3316c463f397e8e29e1cb2d925fc2, 7a3fc280f79578414d71d70609fbdb49ec6ad648, 70b743e60f952a1238a469f529e89b0eb71b5ef7, fa44028115912c95b5efb43218f3c7237d5c349f, 5273b45c5eabe64edbd0b79f5d1b31e2e8582324, 5e5274c7d931c1165aa592cdc3bfceb4649f1ff7, 59aa9be378371183ed419a0b24c019ccf3da97ec, 8591a7ee00fb1bb7cc5b0417479681290a51996e, 82b99ad976429d0a6c545b64c520be4880e1e4b8, 3eee78ede82f6319d094787f45afd9bfb600e971, 2a96338bacce3bb687bdc274daad120f32668cf4,
SHA1	8a389afe1f85f83e340ca9dfc0005d904799d44c, 944b69b5e225c7712604efc289e153210124505c, a942099338c946fc196c62e87942217bf07fc5b3, 52fe3fd399ed15077106bae9ea475052fc8b4acc, 57fd698ccb5cb4f90c014efc6754599e5b0fbe54, c0575af04850eb1911b000bf56e8d5e9362a61e4, 7c3fd8ee5d660bbf43e423818c6a8c3231b03817, fa78e89ab95a0b49bc0663f7ab33aaf1a924c560, 5748e11c87aeab3c19d13db899d3e2008be928ad
Filename	autorun.exe, default_ico.exe, default_ico.exe, default_ico.exe, UjGnsPwFaEtl.exe, RPHost.dll, certificate.pkg, certificate.exe, default_ico_1.exe, memmgrset.dll, pidgin.dll Monlam_Grand_Tibetan_Dictionary_2018.zip, jquery.js, Monlam Bodyig 3.1.exe, deutsch-tibetisches_w__rterbuch_installer_windows.zip, monlam-bodyig3.zip, Monlam-Grand-Tibetan-Dictionary-for-mac-OS-X.zip, monlam-bodyig-mac-os.zip,

TYPE	VALUE
Filename	Security~.x64, Security~.arm64, Security.fat, Monlam_Grand_Dictionary export file
URLs	hxxps[://]tibetpost[.]net/templates/protostar/html/layouts/joomla/system/default_fields[.]php hxxp[://]188.208.141[.]204:5040/a62b94e4dcd54243bf75802f0cbd71f3[.]exe

References

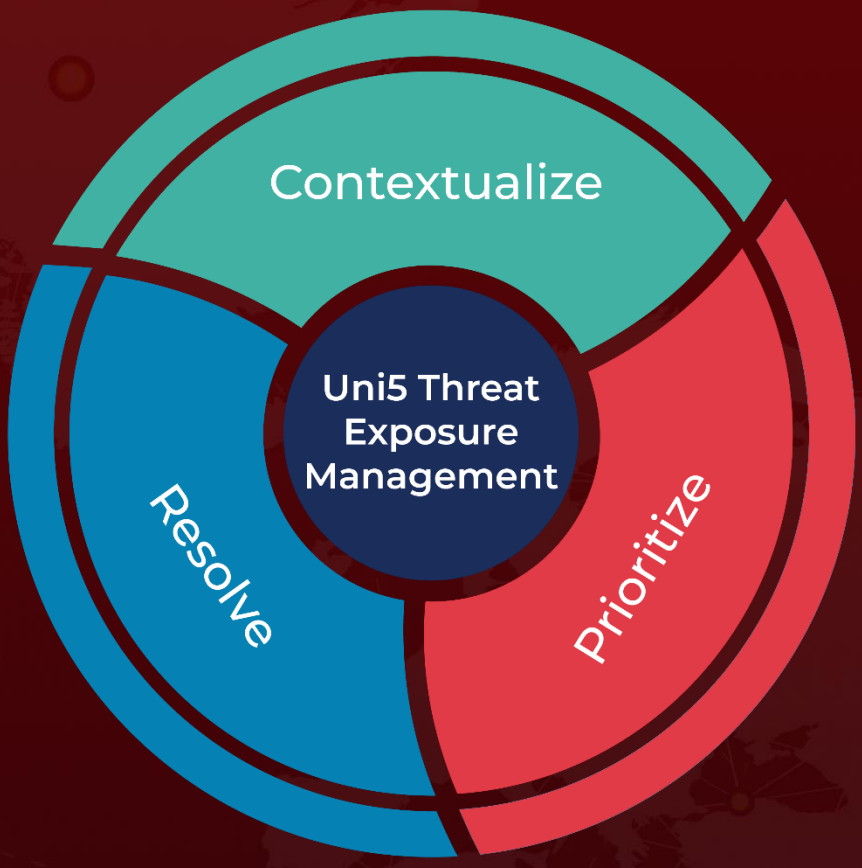
https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/

https://www.hivepro.com/threat-advisory/daggerfly-apt-deploys-mgbot-to-target-african-telecoms-organization/

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

March 11, 2024 • 4:00 AM

More at www.hivepro.com