Hive Pro

Threat Level
Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

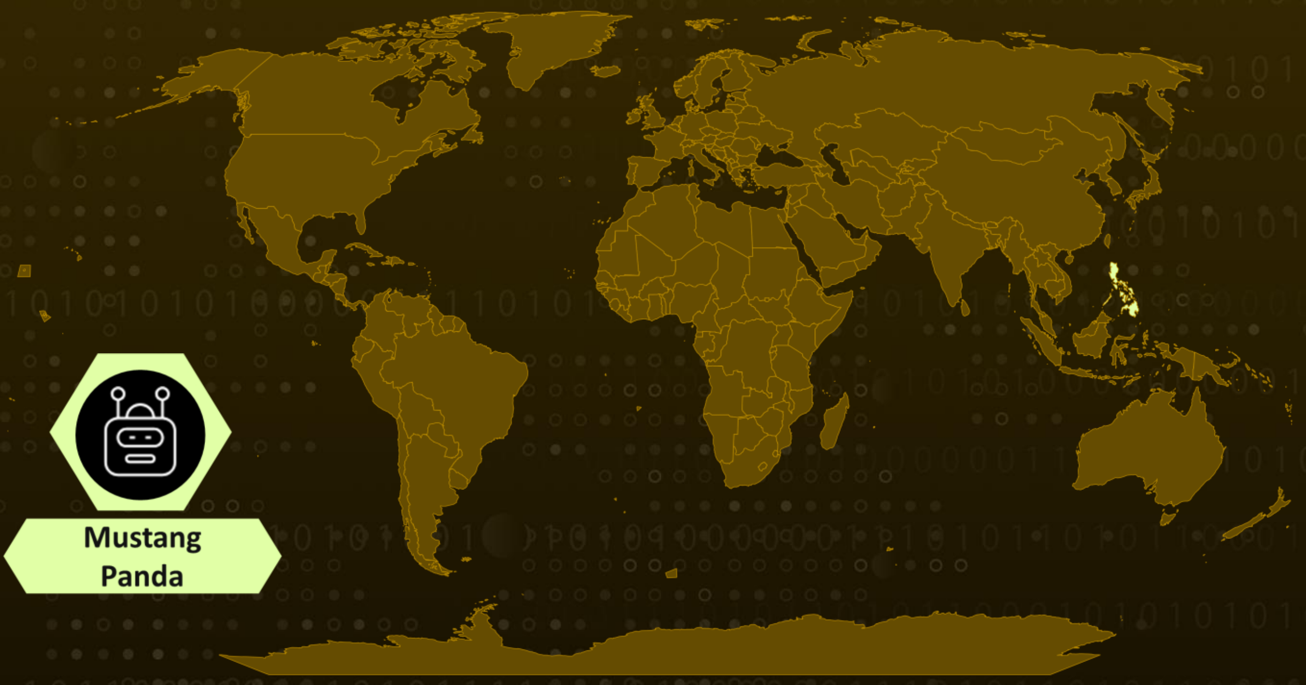
Mustang Panda Targets Philippines Government Using Legitimate Software

Date of Publication	Admiralty Code	TA Number
November 22, 2023	A1	TA2023471

Summary

Attack Discovered: August 2023
Attack Region: Philippines
Targeted Industries: Government entity
Actor: Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, Stately Taurus)
Attack: Mustang Panda, a threat actor associated with China, has been implicated in a cyber attack targeting a government entity in the Philippines. The attackers employed a strategy of using legitimate software, such as Solid PDF Creator and SmadavProtect (an antivirus solution based in Indonesia), to load malicious files. Additionally, the malware was configured to imitate authentic Microsoft traffic, enabling the threat actors to establish command and control connections without detection.

Attack Regions



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

Attack Details

#1 In August, three distinct campaigns associated with Mustang Panda, a Chinese APT, were identified. These campaigns targeted a government entity in the Philippines. The attackers utilized legitimate software, such as Solid PDF Creator and SmadavProtect (an antivirus solution based in Indonesia), to load malicious files. The threat actors employed creative configurations to make the malware mimic genuine Microsoft traffic, facilitating undetected C2 connections.

#2 On August 1, 2023, a Mustang Panda malware package was detected on Google Drive. Disguised as a ZIP file, it presented users with what seemed to be a legitimate application featuring a PDF icon. The folder contained a hidden file named "SolidPDFCreator.dll." When users attempted to execute the software, the malicious DLL would be sideloaded, establishing a connection with a remote server for C2 purposes.

#3 On August 3, 2023, a second campaign featured a ZIP file named "NUG's Foreign Policy Strategy.zip." The malware within this package included a legitimate copy of Solid PDF Creator software and a concealed SolidPDFCreator.dll file. The threat involved sideloading SolidPDFCreator.dll, copying files errordetails, SmadavProtect32.exe and Smadhook32c.dll to the victim's home directory, and establishing a registry key to invoke SmadavProtect32.exe upon user logon.

#4 The third campaign, initiated on August 16, 2023, mirrored the first campaign but employed the file name "Labour Statement.zip." Victims encountered two files: "Labour Statement.exe," a seemingly benign copy of Solid PDF Creator software, and "SolidPDFCreator.dll," a malicious DLL. Mustang Panda consistently demonstrates its capability to engage in ongoing cyber espionage operations directed at a diverse array of international organizations, strategically aligning with geopolitical issues of interest to the Chinese government.

Recommendations

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.

Monitor Network Traffic: Utilize network monitoring tools to scrutinize incoming and outgoing traffic, identifying potential Port Knocking attempts or irregular communication patterns. This can help detect and thwart attackers attempting to establish connections with their command-and-control servers.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Remain vigilant: 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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0011 Command and Control	T1566 Phishing	T1204 User Execution	T1204.002 Malicious File
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1036 Masquerading	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	bebde82e636e27aa91e2e60c6768f30beb590871ea3a3e8fb6aedbd9f5c154c5, 24c6449a9e234b07772db8fdb944457a23eecbd6fbb95bc0b1398399de798584, ba7c456f229adc4bd75bfb876814b4deaf6768ffe95a03021aead03e55e92c7c, 969b4b9c889fbec39fae365ff4d7e5b1064dad94030a691e5b9c8479fc63289c, 3597563aebb80b4bf183947e658768d279a77f24b661b05267c51d02cb32f1c9, d57304415240d7c08b2fbada718a5c0597c3ef67c765e1daf4516ee4b4bdc768, 54be4a5e76bdca2012db45b1c5a8d1a9345839b91cc2984ca80ae2377ca48f51, 2b05a04cd97d7547c8c1ac0c39810d00b18ba3375b8feac78a82a2f9a314a596
IP	45.121.146[.]113
URL	hxxps://drive.google[.]com/uc?id=1QLIQXP-s42TtZsONsKLAAtOr4Pdxljcu

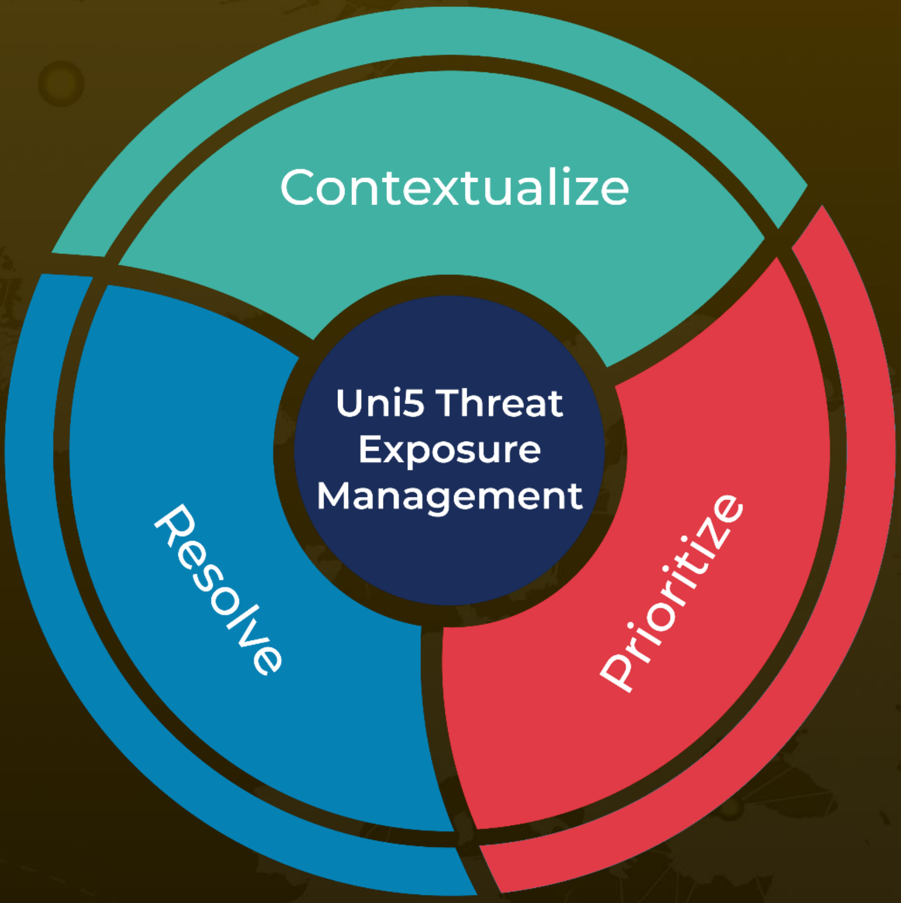
References

https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/

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

November 22, 2023 • 3:45 AM

More at www.hivepro.com