Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

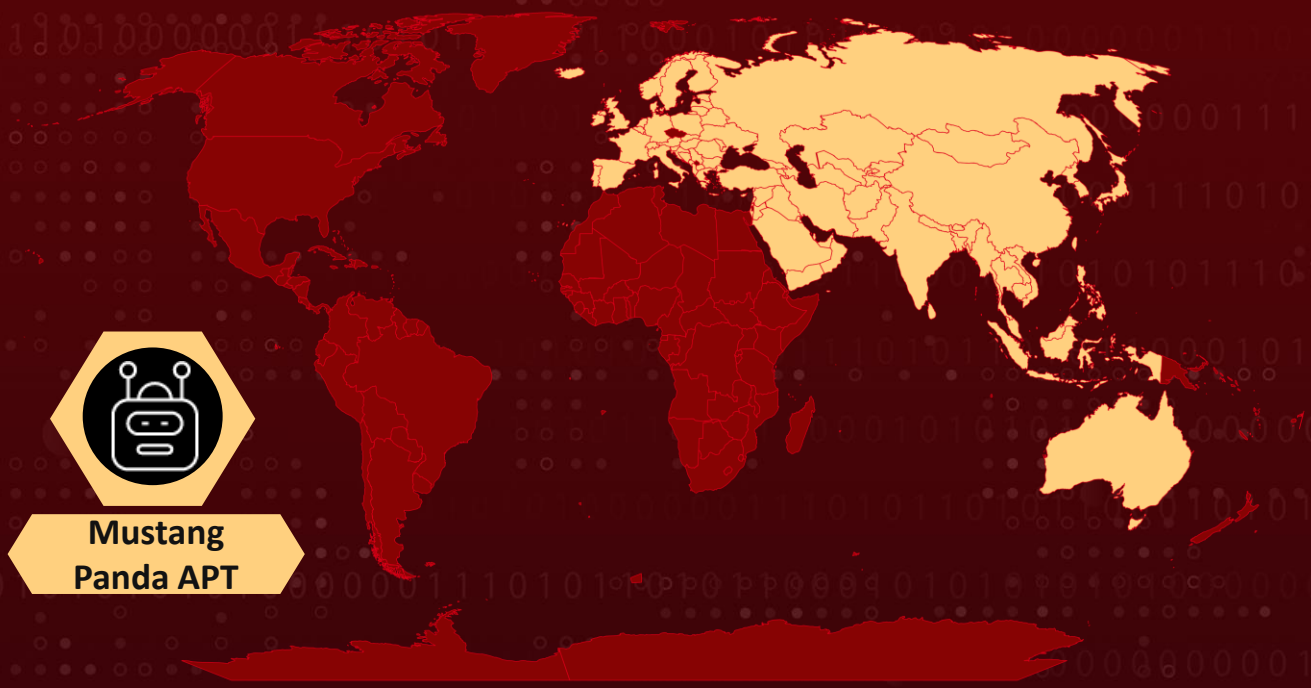
New MQsTTang Backdoor from Mustang Panda Targets Political and Governmental Organizations

Date of Publication	Admiralty Code	TA Number
March 02, 2023	A1	TA2023115

Summary

First Appearance: January 2023
Actor Name: Mustang Panda APT (Bronze President, TEMP.Hex , HoneyMyte, Red Lich, Earth Preta)
Target Region: Taiwan, Australia, Europe, and Asia
Target Sectors: Political and Governmental
Attack: MQsTTang is a custom backdoor attributed to the Mustang Panda APT group. It uses the MQTT protocol for C&C communication and is distributed via spearphishing through RAR archives with names related to diplomacy and passports.

Attack Regions



Attack Details

#1 A new custom backdoor called MQsTTang, which they attribute to the Mustang Panda APT group. This backdoor is part of an ongoing campaign that began in early January 2023, and it appears to be targeting political and governmental organizations in Taiwan, Australia, Europe, and Asia. Unlike most of the group's malware, MQsTTang doesn't seem to be based on existing families or publicly available projects.

#2 MQsTTang is a barebones backdoor that allows the attacker to execute arbitrary commands on a victim's machine and get the output. One of the interesting characteristics of this backdoor is its use of the MQTT protocol for C&C communication. MQTT is typically used for communication between IoT devices and controllers, and the protocol hasn't been used in many publicly documented malware families.

#3 MQsTTang is distributed in RAR archives, which only contain a single executable. These executables usually have names related to Diplomacy and passports. These archives are hosted on a web server with no associated domain name. This fact and filenames lead researchers to believe that the malware is spread via spearphishing.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	**TA0002** Execution	**TA0043** Reconnaissance	**TA0004** Privilege Escalation
TA0011 Command and Control	**TA0010** Exfiltration	**TA0005** Defense Evasion	**TA0042** Resource Development
TA0001 Initial Access	**T1583.003** Acquire Infrastructure: Virtual Private Server	**T1583.004** Acquire Infrastructure: Server	**T1587.001** Develop Capabilities: Malware
T1588.002 Obtain Capabilities: Tool	**T1608.001** Stage Capabilities: Upload Malware	**T1608.002** Stage Capabilities: Upload Tool	**T1566.002** Phishing: Spearphishing Link
T1106 Native API	**T1204.002** User Execution: Malicious File	**T1547.001** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	**T1036.004** Masquerading: Masquerade Task or Service
T1036.005 Masquerading: Match Legitimate Name or Location	**T1480** Execution Guardrails	**T1622** Debugger Evasion	**T1071** Application Layer Protocol
T1102.002 Web Service: Bidirectional Communication	**T1132.001** Data Encoding: Standard Encoding	**T1573.001** Encrypted Channel: Symmetric Cryptography	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	3.228.54[.]173 80.85.156[.]151 80.85.157[.]3 185.144.31[.]86

TYPE	VALUE
SHA1	A1C660D31518C8AFAA6973714DE30F3D576B68FC 430C2EF474C7710345B410F49DF853BDEAFBDD78 F1A8BF83A410B99EF0E7FDF7BA02B543B9F0E66C 02D95E0C369B08248BFFAAC8607BBA119D83B95B 0EA5D10399524C189A197A847B8108AA8070F1B1 982CCAF1CB84F6E44E9296C7A1DDE2CE6A09D7BB 740C8492DDA786E2231A46BFC422A2720DB0279A AB01E099872A094DC779890171A11764DE8B4360 61A2D34625706F17221C1110D36A435438BC0665 30277F3284BCEEF0ADC5E9D45B66897FA8828BFD BEE0B741142A9C392E05E0443AAE1FA41EF512D6 F6F3343F64536BF98DE7E287A7419352BF94EB93 F848C4F3B9D7F3FE1DB3847370F8EEFAA9BF60F1

References

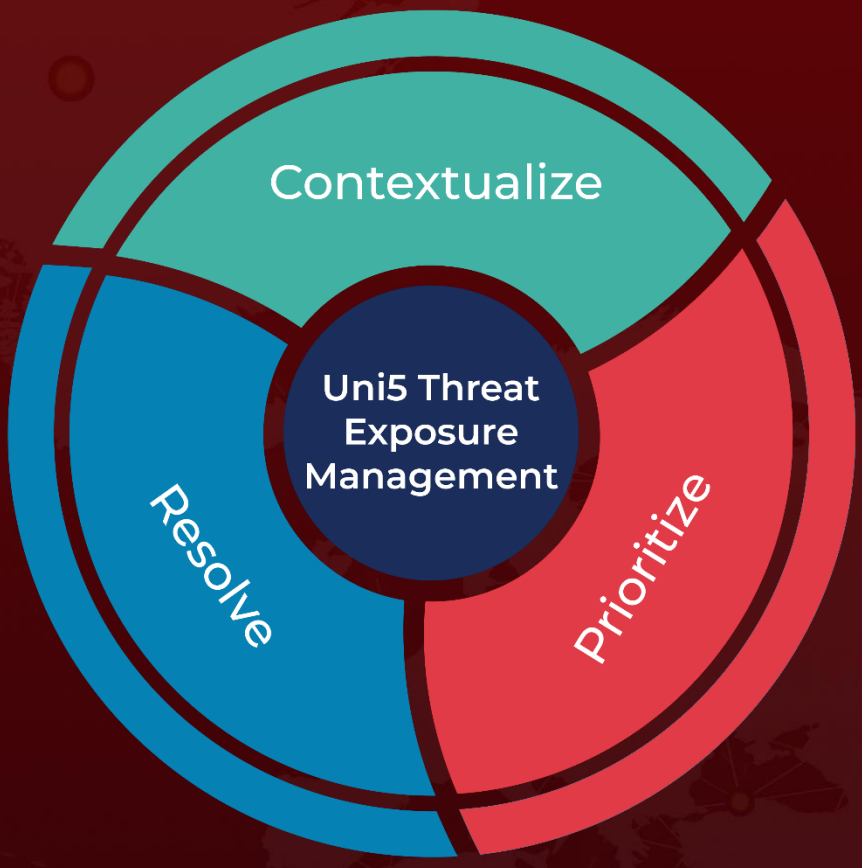
https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/

https://www.hivepro.com/mustang-panda-apt-targets-europe-with-customized-plugx-malware/

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 02, 2023 • 11:30 PM

More at www.hivepro.com