Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

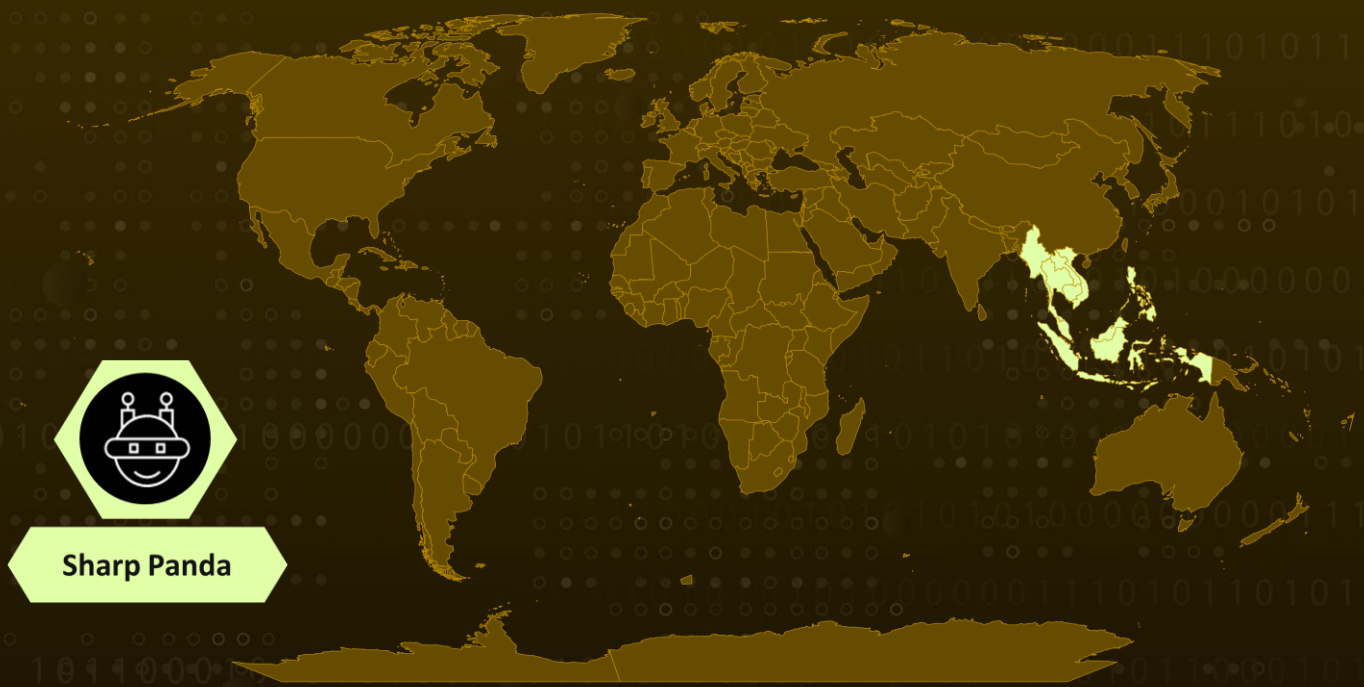
Sharp Panda A Sophisticated Cyber-Espionage Campaign Targeting Governments

Date of Publication	Admiralty Code	TA Number
March 9, 2023	A1	TA2023126

Summary

First Appearance: 2018
Actor Name: Sharp Panda
Target Region: Southeast Asia
Target Sectors: Government

Actor Map



Actor Details

#1

Sharp Panda is engaged in a persistent surveillance operation aimed at Southeast Asian government entities. The attackers initiate the attack through spear-phishing emails, which contain government-themed lures in a Word document. These lures utilize a remote template to download and execute a malicious RTF document, which is weaponized with the notorious RoyalRoad kit.

#2

Upon execution, the malware triggers a sequence of in-memory loaders, consisting of 5.t Downloader, a proprietary DLL downloader, and a second-stage loader responsible for deploying a final backdoor. At the time of Sharp Panda's campaigns, the ultimate payload detected was VictoryDll, a custom and distinct backdoor that enabled remote access and data collection from the compromised device. In addition, a revised edition of the SoulSearcher loader was also utilized, which is responsible for downloading, decrypting, and installing other modules of the Soul modular backdoor into memory..

#3

The primary responsibility of the Soul main module is to establish a link with the C&C server and execute the essential task of accepting and deploying additional modules into the memory. Once the system is thoroughly examined, the backdoor initiates a series of requests to "register" a new connection and authenticate itself against the C&C server. Subsequently, the backdoor enters into an infinite loop, continually communicating with the C&C server. The architecture and capabilities of the threat actors have undergone regular updates and enhancements.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Sharp Panda	China	Southeast Asia	Government
	MOTIVE		
	Information theft and espionage		

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

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1053 Scheduled Task/Job	T1203 Exploitation for Client Execution
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1036 Masquerading	T1012 Query Registry
T1018 Remote System Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery
T1001 Data Obfuscation	T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer
T1573 Encrypted Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	45.76.190[.]210 45.197.132[.]68 45.197.133[.]23 103.78.242[.]11 103.159.132[.]96 103.173.154[.]168 103.213.247[.]48 139.180.137[.]73 139.180.138[.]49 152.32.243[.]17
Domain	office.oiqezet[.]com
SHA256	32a0f6276fea9fe5ee2ffda461494a24a5b1f163a300bc8edd3b33c9c6cc2d17 ca7f297dc04acad2fab04d5dc2de9475aed4186805f6c237c10b8f56b384cf30 341dee709285286bc5ba94d14d1bce8a6416cb93a054bd183b501552a17ef314 9d628750295f5cde72f16da02c430b5476f6f47360d008911891fdb5b14a1a01 811a020b0f0bb31494f7fbe21893594cd44d90f77fcd1f257925c4ac5fabed43 b023e2b398d552aacb2233a6e08b4734c205ab6abf5382ec31e6d5aa7c71c1cb 81d9e75d279a953789cbbe9ae62ce0ed625b61d123fef8ffe49323a04fecdb3f 12c1a4c6406ff378e8673a20784c21fb997180cd333f4ef96ed4873530baa8d3 f2779c63373e33fdbd001f336df36b01b0360cd6787c1cd29a6524cc7bcf1ffb 7a7e519f82af8091b9ddd14e765357e8900522d422606aefda949270b9bf1a04 4747e6a62fee668593ceebf62f441032f7999e00a0dfd758ea5105c1feb72225 3541f3d15698711d022541fb222a157196b5c21be4f01c5645c6a161813e85be 0f9f85d41da21781933e33dddcc5f516c5ec07cc5b4cff53ba388467bc6ac3fd 17f4a21e0e8c0ce958baf34e45a8b9481819b9b739f3e48c6ba9a6633cf85b0e f8622a502209c18055a308022629432d82f823dd449abd9b17c61e363a890828

TYPE	VALUE
SHA256	1a15a35065ec7c2217ca6a4354877e6a1de6108613111749842 32ba5ff749114 065d399f6e84560e9c82831f9f2a2a43a7d853a27e922cc81d3b c5fcd1adfc56 1e18314390302cd7181b710a03a456de821ad85334acfb55f53 5d311dd6b3d65 c4500ad141c595d83f8dba52fa7a1456959fb0bc2ee6b0d0f687 336f51e1c14e 390e6820b2cc173cfd07bcebd67197c595f4705cda7489f4bc44 c933ddcf8de6 d1a6c383de655f96e53812ee1dec87dd51992c4be28471e44d7 dd558585312e0 df5fe7ec6ecca27d3affc901cb06b27dc63de9ea8c97b87bc899a 79eca951d60

References

https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/#single-post

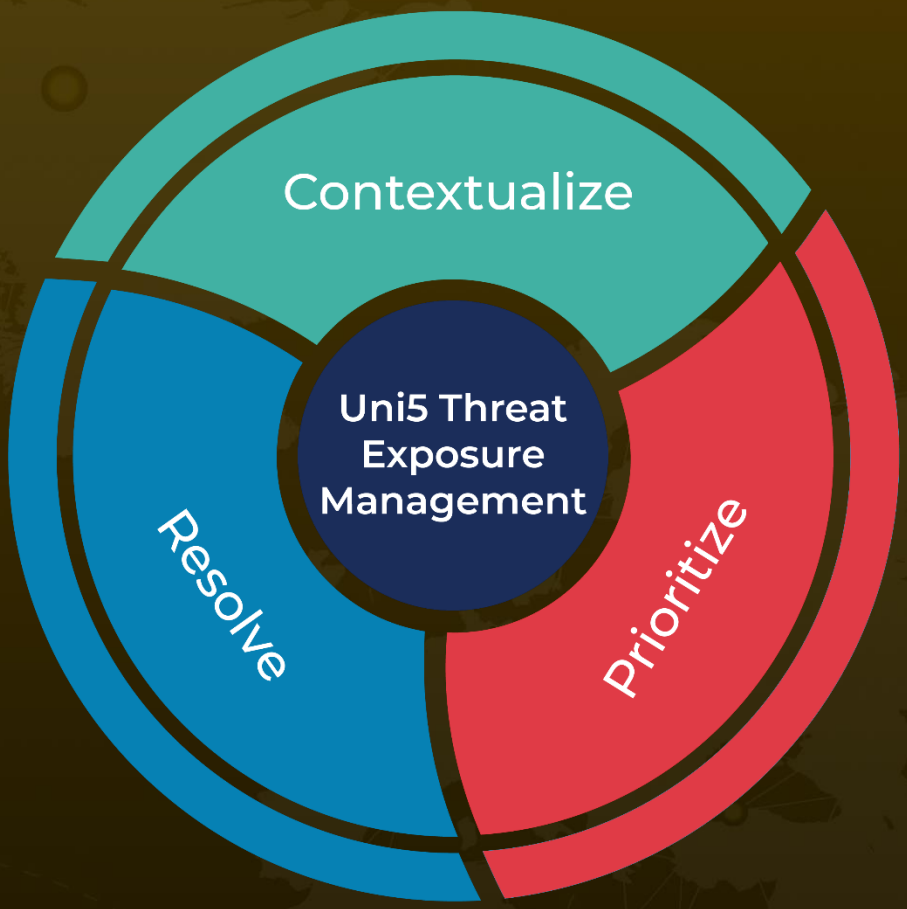
https://thehackernews.com/2023/03/sharp-panda-using-new-soul-framework.html

https://www.hivepro.com/the-intricate-evolution-of-soulsearcher-loader-for-multi-stage-malware-execution/

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 9, 2023 • 3:17 AM

More at www.hivepro.com