Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

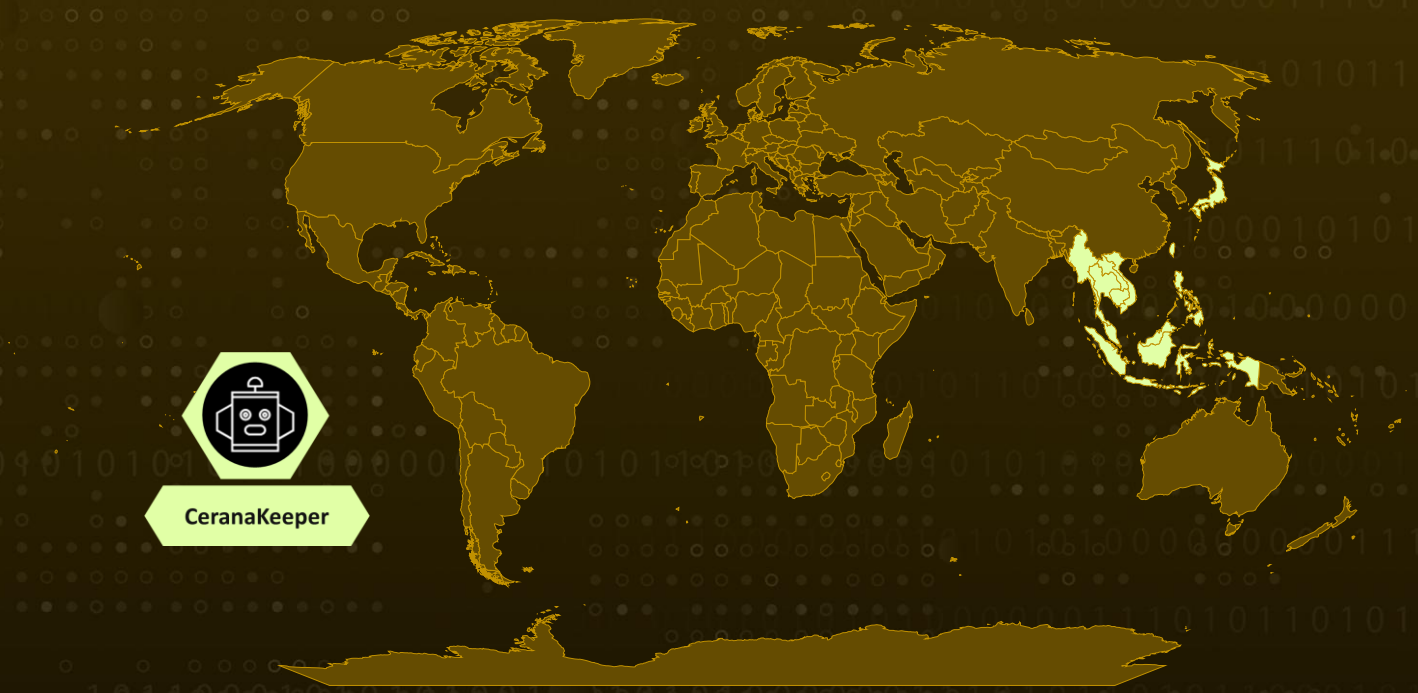
CeranaKeeper: The Hive Mind of Cyber Espionage

Date of Publication	Admiralty Code	TA Number
October 15, 2024	A1	TA2024393

Summary

Active Since: 2022
Threat Actor: CeranaKeeper
Malware: TONESHELL, WavyExfiller, OneDoor, BingoShell
Targeted Countries: Thailand, Myanmar, Philippines, Japan, Taiwan, Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Singapore, Vietnam
Targeted Industry: Government

Actor Map



Actor Details

#1 CeranaKeeper is a China-aligned threat actor engaged in large-scale data exfiltration, particularly targeting governmental institutions across Southeast Asia. Active since 2022, the group has evolved its tactics by repurposing components previously attributed to the APT group Mustang Panda, showcasing a clear adaptation in their methodology.

#2 While their exact initial access methods remain unknown, CeranaKeeper exploits compromised systems to move laterally across networks. They have also demonstrated innovation by converting compromised machines into update servers and using GitHub's pull request and issue comment features to establish a stealthy reverse shell.

#3 Additionally, they deploy single-use tools designed to harvest entire file trees from victim systems. CeranaKeeper's arsenal includes both custom-built tools and publicly available software. Key components such as TONEINS, TONESHELL, and PUBLOAD remain central to their operations. However, in 2023, the group introduced several new tools that leveraged popular cloud and file-sharing platforms like Pastebin, Dropbox, OneDrive, and GitHub to execute commands and exfiltrate sensitive data.

#4 Among these tools is WavyExfiller, a Python-based tool designed to collect data from connected devices like USB drives and hard drives, using Dropbox and PixelDrain for exfiltration. Another tool, DropboxFlop, is a Python variant of the DropFlop reverse shell, which enables file uploads and downloads using Dropbox as a command-and-control (C2) server.

#5 CeranaKeeper also employs OneDoor, a C++ backdoor that exploits Microsoft OneDrive's REST API to receive commands and exfiltrate files, and BingoShell, a Python backdoor that takes advantage of GitHub's pull request and issue comment features to create a covert reverse shell.

#6 Although CeranaKeeper and Mustang Panda share similarities in some tools, they operate independently, each utilizing its own distinct set of capabilities. CeranaKeeper's focus on exfiltrating large volumes of data is evident in their extensive use of wildcard expressions to traverse entire drives, underscoring their aim for massive data theft.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRY
CeranaKeeper	China **MOTIVE** Information theft and Espionage	Thailand, Myanmar, Philippines, Japan, Taiwan, Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Singapore, Vietnam	Government

Recommendations

Network Segmentation: Consider network segmentation to limit lateral movement within the network. By isolating critical systems, organizations can reduce the risk of widespread data exfiltration in the event of a breach.

User Education and Training: Conduct regular cybersecurity awareness training for all employees, emphasizing the risks associated with phishing attacks and social engineering tactics. Employees should be informed about the signs of cyber threats and how to report suspicious activity.

Enhanced Monitoring and Detection: Implement advanced monitoring solutions to detect anomalous activities related to data exfiltration. Tools that analyze network traffic patterns can help identify unusual communication with cloud and file-sharing services like Dropbox, OneDrive, and GitHub.

Review and Harden Cloud Configurations: Regularly audit and harden the configurations of cloud services and file-sharing platforms to ensure they comply with security best practices. Disable unnecessary features and services to reduce the attack surface.

Incident Simulation and Drills: Conduct regular tabletop exercises and simulations to test the effectiveness of incident response plans. This helps identify weaknesses in processes and improve team readiness against potential attacks from groups like CeranaKeeper.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	T1583 Acquire Infrastructure
T1583.001 Domains	T1583.003 Virtual Private Server	T1587 Develop Capabilities	T1587.001 Malware
T1585 Establish Accounts	T1585.003 Cloud Accounts	T1072 Software Deployment Tools	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1140 Deobfuscate/Decode Files or Information
T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1560 Archive Collected Data	T1560.001 Archive via Utility
T1005 Data from Local System	T1039 Data from Network Shared Drive	T1074 Data Staged	T1074.001 Local Data Staging
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1132 Data Encoding	T1132.002 Non-Standard Encoding
T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1573.002 Asymmetric Cryptography	T1090 Proxy
T1090.001 Internal Proxy	T1102 Web Service	T1102.002 Bidirectional Communication	T1567 Exfiltration Over Web Service
T1567.002 Exfiltration to Cloud Storage	T1588.002 Tool	T1588 Obtain Capabilities	T1105 Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e7b6164b6ec7b7552c93713403507b531f625a8c64d36b60d660d66e82646696, 451ee465675e674cebe3c42ed41356ae2c972703e1dc7800a187426a6b34efdc, dafad19900fff383c2790e017c958a1e92e84f7bb159a2a7136923b715a4c94f, 3f81d1e70d9ee39c83b582ac3bcc1cdfe038f5da31331cdbcd4ff1a2d15bb7c8, 24e12b8b1255df4e6619ed1a6ae1c75b17341eef7418450e661b74b144570017, b25c79ba507a256c9ca12a9bd34def6a33f9c087578c03d083d7863c708eca21, e6ab24b826c034a6d9e152673b91159201577a3a9d626776f95222f01b7c21db, 6655c5686b9b0292cf5121fc6346341bb888704b421a85a15011456a9a2c192a, b15ba83681c4d2c2716602615288b7e64a1d4a9f4805779cebdf5e6c2399afb5
File Name	EACore.dll, SearchApp.exe, OneDrive.exe, dropbox.exe, Update.exe, oneDrive.exe, MsOcrRes.orp, avk.dll, TurboActivate.dll
IPv4	104[.]21[.]81[.]233, 172[.]67[.]165[.]197, 103[.]245[.]165[.]237, 103[.]27[.]202[.]185, 103[.]27[.]202[.]185
Domains	www[.]toptipvideo[.]com, dljmp2p[.]com, inly5sf[.]com, www[.]dl6yfsl[.]com, www[.]uvfr4ep[.]com

References

https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/

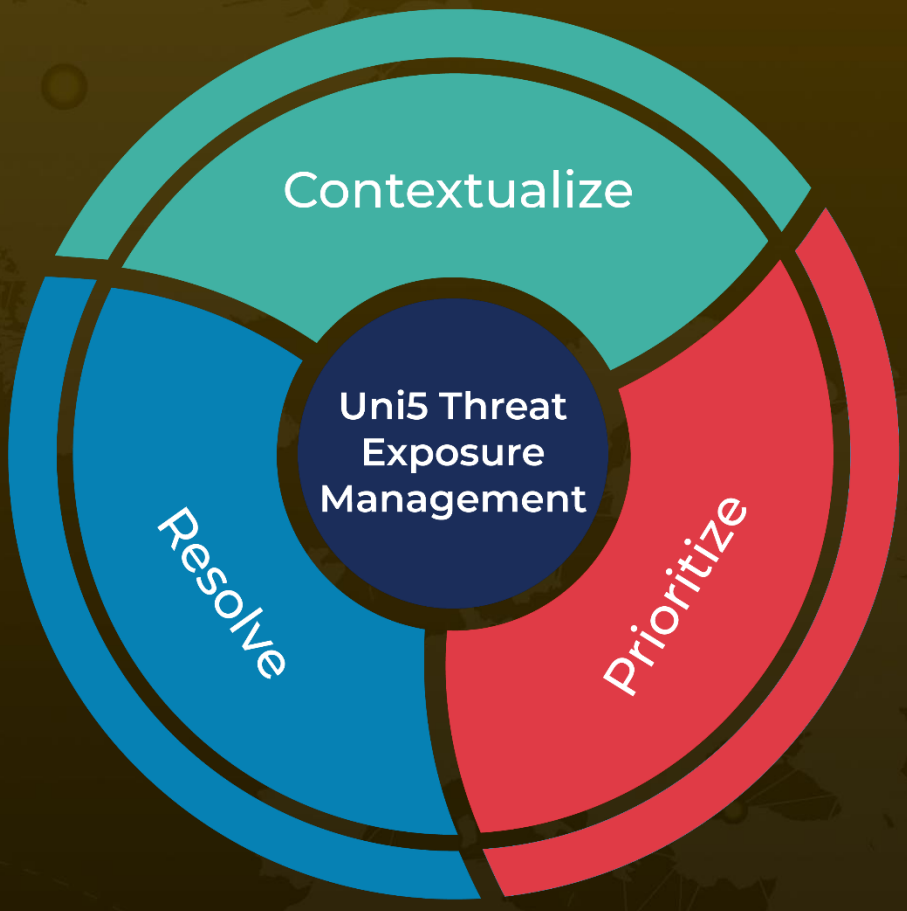
https://web-assets.esetstatic.com/wls/en/papers/white-papers/ceranakeeper.pdf

https://hivepro.com/threat-advisory/chinese-apt-earth-preta-runs-spearphishing-campaigns/

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 15, 2024 • 5:00 AM

More at www.hivepro.com