Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

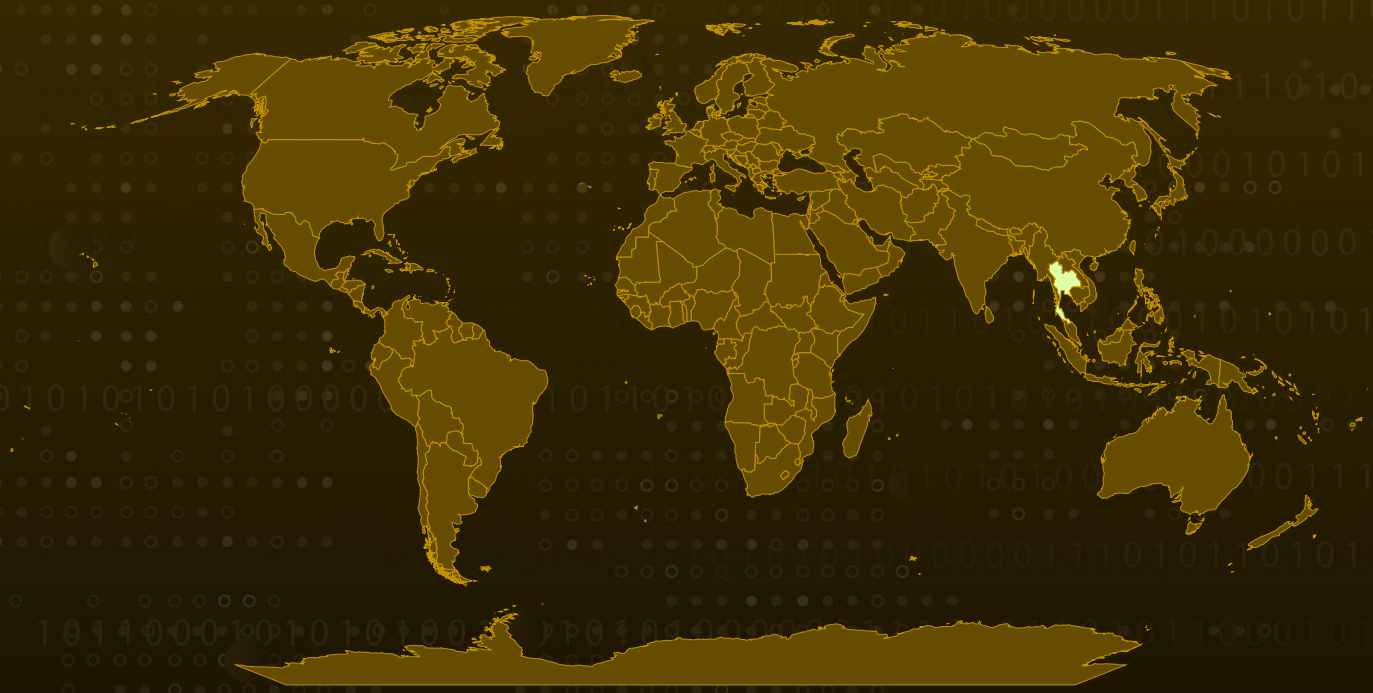
Yokai A New Backdoor Stalks Thai Officials

Date of Publication	Admiralty Code	TA Number
December 18, 2024	A1	TA2024465

Summary

Malware: Yokai Backdoor
Targeted Country: Thailand
Targeted Industries: Government
Attack: Thai government officials are being targeted in a sophisticated cyberattack that leverages DLL side-loading to deploy Yokai, a newly discovered backdoor. The attack involves executing decoy documents while covertly deploying malicious payloads and gathering key system data, which is encrypted and transmitted to maintain control. This underscores the evolving threats facing government entities.

Attack Regions



Attack Details

#1 Thai government officials are being targeted in a sophisticated cyber campaign that leverages DLL side-loading to deploy a newly discovered backdoor called Yokai. At the core of this attack is a RAR archive containing two Windows shortcut files. Although the exact method used to deliver this archive remains unknown, executing the shortcuts opens decoy files a PDF and a Microsoft Word document while simultaneously deploying a malicious payload in the background.

#2 This payload is engineered to drop three components onto the compromised system: a legitimate binary from the iTop Data Recovery application, a malicious DLL, and a DATA file with information obtained from an attacker-controlled server.

#3 Yokai operates by establishing persistence on the targeted system and communicating with a command-and-control (C2) server. This connection enables it to receive instructions, such as spawning and executing shell commands using cmd.exe.

#4 In addition to executing commands, the backdoor collects key system information, including the hostname, username, and a malware version string. This data is encrypted, formatted into a structured block, and transmitted to the C2 server, facilitating sustained communication and control.

Recommendations

Secure Software Sources: Download software only from trusted sources, such as vendor websites or verified app stores. Avoid using unofficial or third-party repositories for updates or installations.

Code and System Hardening: Harden systems and networks and deploy code to minimize vulnerabilities. Use code analysis and penetration testing tools to identify and address any weak points in software or websites.

Use Application Whitelisting: Implement application whitelisting to prevent unauthorized or malicious software from running on your systems, allowing only trusted applications to execute.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1053 Scheduled Task/Job	**T1559** Inter-Process Communication	**T1564** Hide Artifacts	**T1564.004** NTFS File Attributes
T1036 Masquerading	**T1574.002** DLL Side-Loading	**T1574** Hijack Execution Flow	**T1480.002** Mutual Exclusion
T1480 Execution Guardrails	**T1071.001** Web Protocols	**T1071** Application Layer Protocol	**T1573.001** Symmetric Cryptography
T1573 Encrypted Channel	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell
T1027 Obfuscated Files or Information	**T1082** System Information Discovery	**T1041** Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a944e263baef43c482e33b7eaff84a4f, 025e03797d3ccfc548accded09a1f93d, c3886f5904c0ff21d49433fd1fa05655, 4b1e6b39e13bf7c665e4ed51f4e49411, 596645fd383ee909024f9e742bc71bf5, 70c79d162bc8d094f721c430b7a768b2, 47a2679a34763a2fc22dd3b55628fc91, f36371db03d12b389c74b3f92a3e4af8
SHA1	a472eded72eabc52792a51187062ee021c32b3c9, 4da70f14a0e0ea6054a42eb7d43f6cd59f09a72e, 6065c56dcf34de1568cec41450c798fe32395f31, 2b58537f6039444ca4920245a2854f4368c9ded5, 94e8e815315dcd439395c718658fc87f750be2aa, 47b1a8b12e46af207fc67ea8ca4f5ed7847ee7bf, ac050f6c8924fc3094145d77e40596e5f34a7b6f, 57d28f7f4859853a9fc42bdcfc2b0d2d7341443a
SHA256	248c50331f375e7e73f010e4158ec2db8835a4373da2687ab75e8a73fde795f0, c74f67bb13a79ae8c111095f18b57a10e63d9f8bfbffec8859c61360083ce43e, 24509eb64a11f7e21feeb667b1d70520b1b1db8345d0e6502b657d416ef81a4d, c7746e0031fba26ca6a8ecc3cee9e3dd50507fe2c1136356f852e068e1f943d0, 90f4364705f19929d5cc0dafc44946768e39e81338715503dbc923b75c6edfd5, f361f5ec213b861dc4a76eb2835d70e6739321539ad216ea5dc416c1dc026528, 452be2f9018f1ef2d74c935eac391ecdceff9a12cb950441f4f4e26b2b050fa1, eaae6d5dbf40239fb5abfa2918286f4039a3a0fcd28276a41281957f6d850456, 3e5cfe768817da9a78b63efad9e60d2d300727a97476edf87be088fb26f06500, 1626ce79f2b96c126cbdb00195dd8509353e8754b1a0ce88d359fa890acd6676, 2852223eb40cf0dae4111be28ce37ce9af23e5332fb78b47c8f5568d497d2611

TYPE	VALUE
URLs	122[.]155[.]28[.]155[:]80/page/index[.]php, 154[.]90[.]47[.]77[:]80/, 191[.]police[.]go[.]th[:]443/api/index[.]php, 191[.]police[.]go[.]th[:]443/Assessment/Report/PDF/default[.]php, m-society[.]dpis[.]go[.]th[:]443/default[.]php, 49[.]231[.]18[.]150[:]80/research/files/index[.]php
IPv4	154[.]90[.]47[.]77

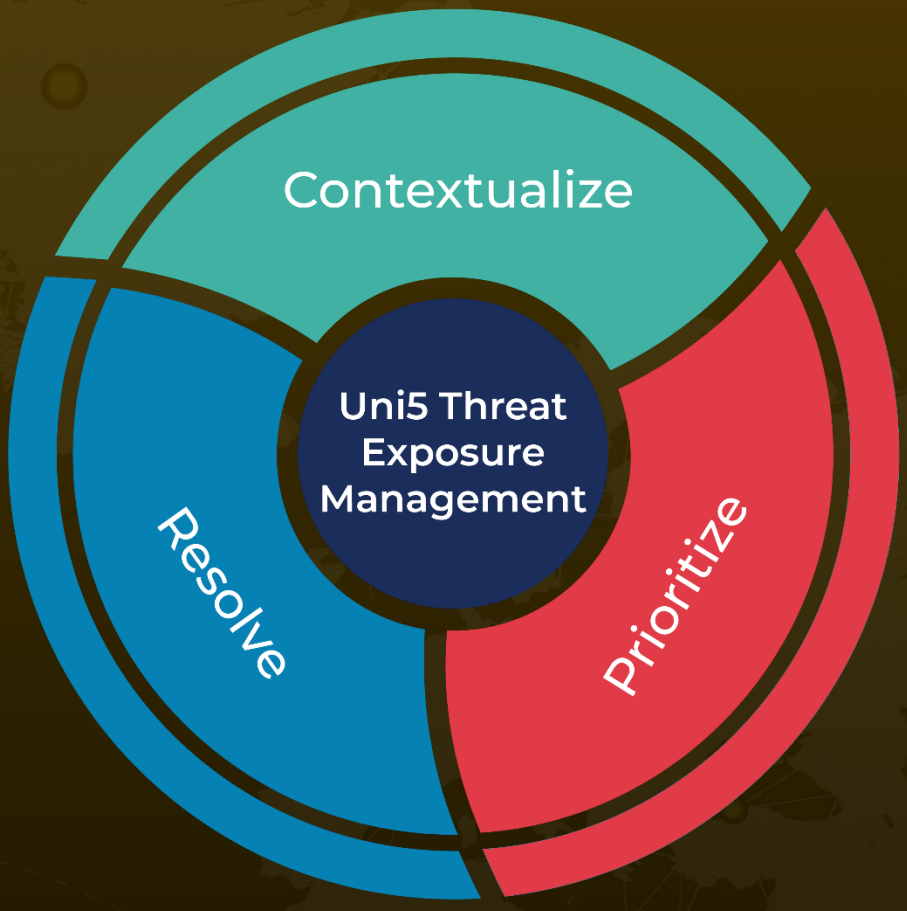
References

https://www.netskope.com/blog/new-yokai-side-loaded-backdoor-targets-thai-officials

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

December 18, 2024 • 7:30 AM

More at www.hivepro.com