Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Turla’s Tiny Backdoor Exploits MSBuild to Evade Detection

Date of Publication	Admiralty Code	TA Number
May 24, 2024	A2	TA2024206

Summary

Attack Began: December 4, 2023
Targeted Countries: Philippines
Malware: Tiny backdoor
Threat Actor: Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23 , Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton , Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard , Pensive Ursa)
Targeted Industries: NGOs
Affected Platform: Windows
Attack: A sophisticated campaign by the Turla APT group, is employing a Tiny backdoor. It uses malicious .LNK files disguised as legitimate documents to target individuals and leverages MSBuild to evade detection.

Attack Regions

Attack Details

#1 A sophisticated campaign likely orchestrated by the Turla APT group, employing malicious .LNK files disguised as PDF documents to deliver a stealthy Tiny backdoor. The campaign primarily targets individuals interested in human rights by using seminar invitations as lures. Upon execution, these .LNK files activate PowerShell scripts that deploy a backdoor through MSBuild, a legitimate Microsoft development tool, thereby avoiding detection.

#2 The infection process involves the .LNK file executing a PowerShell script that creates and opens a lure PDF while simultaneously running an MSBuild project, which decrypts and runs a secondary payload. This payload schedules a task to repeatedly execute another MSBuild project, maintaining a persistent backdoor capable of receiving and executing commands from a command-and-control (C&C) server. The Tiny backdoor enables attackers to hide their activities, execute shell commands, upload and download files, and more.

#3 Analysis links this campaign to the Turla group due to Russian-language comments in the code, the use of specific identifier values in HTTP requests, and the exploitation of compromised web servers for C&C communication. The final payload shares similarities with the TinyTurla backdoor.

Recommendations

Deploy Strong Email Filtering Systems: Implement robust email filtering solutions to detect and prevent the dissemination of harmful attachments, particularly those originating from suspicious or unknown sources. This can significantly reduce the likelihood of initial infection through phishing emails.

Exercise Caution with Email Attachments and Links: Encourage users to exercise caution when interacting with email attachments or links, especially those from unfamiliar senders or containing unexpected content. Verify the sender's identity before opening attachments, and report suspicious emails to the IT security team.

Restrict Access to Development Tools: Limit access to development tools like MSBuild and PowerShell to authorized personnel or specific systems within the organization. By restricting access, you can mitigate the risk of unauthorized usage by threat actors who may leverage these tools for malicious purposes.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0003** Persistence	**TA0011** Command and Control
TA0010 Exfiltration	**T1059.001** PowerShell	**T1059** Command and Scripting Interpreter	**T1204.002** Malicious File
T1204 User Execution	**T1036** Masquerading	**T1140** Deobfuscate/Decode Files or Information	**T1127** Trusted Developer Utilities Proxy Execution
T1127.001 MSBuild	**T1053.005** Scheduled Task	**T1053** Scheduled Task/Job	**T1071** Application Layer Protocol
T1041 Exfiltration Over C2 Channel	**T1027** Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	b4db8e598741193ea9e04c2111d0c15ba79b2fa098efc3680a63ef457e60dbd9, 6829ab9c4c8a9a0212740f46bf93b1cbe5d4256fb4ff66d65a3a6eb6c55758a1, 8c97df4ca1a5995e22c2c4887bea2945269d6f5f158def98d5ebdd5311bb20c4, 76629afb86bd9024c3ea6759eeea197ba6c8c780e0041d1f8182d206cf3bd1b4, c2618fb013135485f9f9aa27983df3371dfdcb7beecde86d02cee0c258d5ed7f, cac4d4364d20fa343bf681f6544b31995a57d8f69ee606c4675db60be5ae8775
URL	hxxps://ies[.]inquirer[.]com[.]ph

References

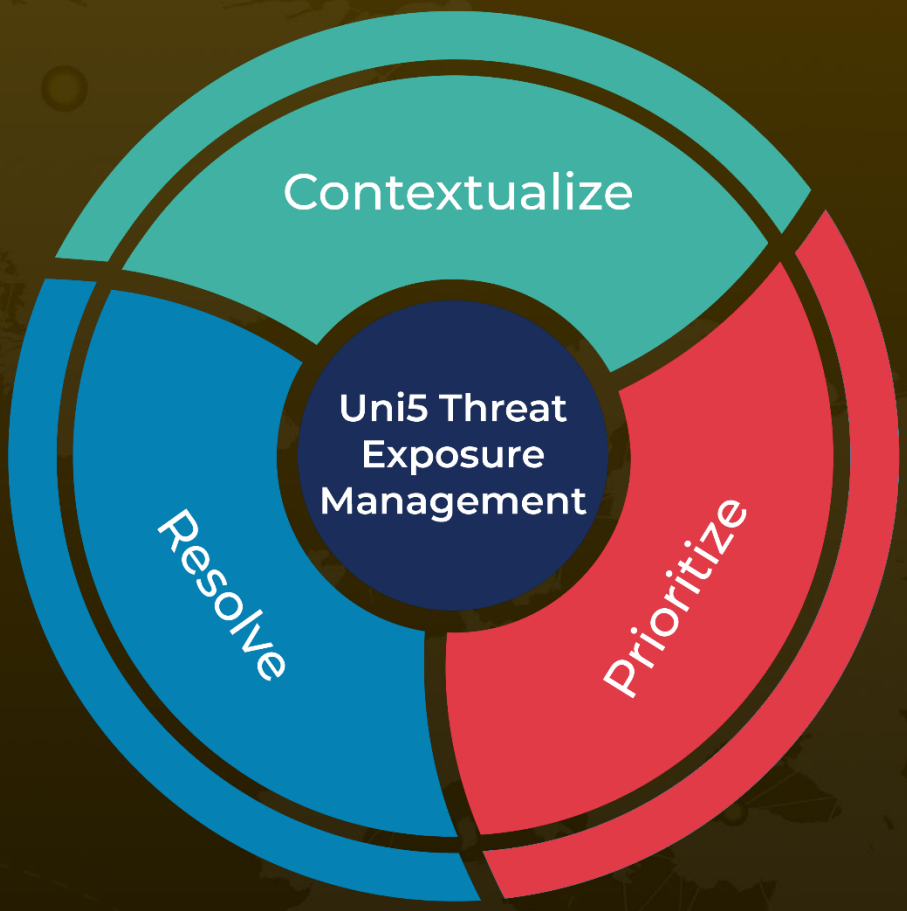
https://cyble.com/blog/tiny-backdoor-goes-undetected-suspected-turla-leveraging-msbuild-to-evade-detection/

https://www.hivepro.com/threat-advisory/turla-expands-their-arsenal-with-next-generation-malwares/

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

May 24, 2024 • 4:30 AM

More at www.hivepro.com