Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

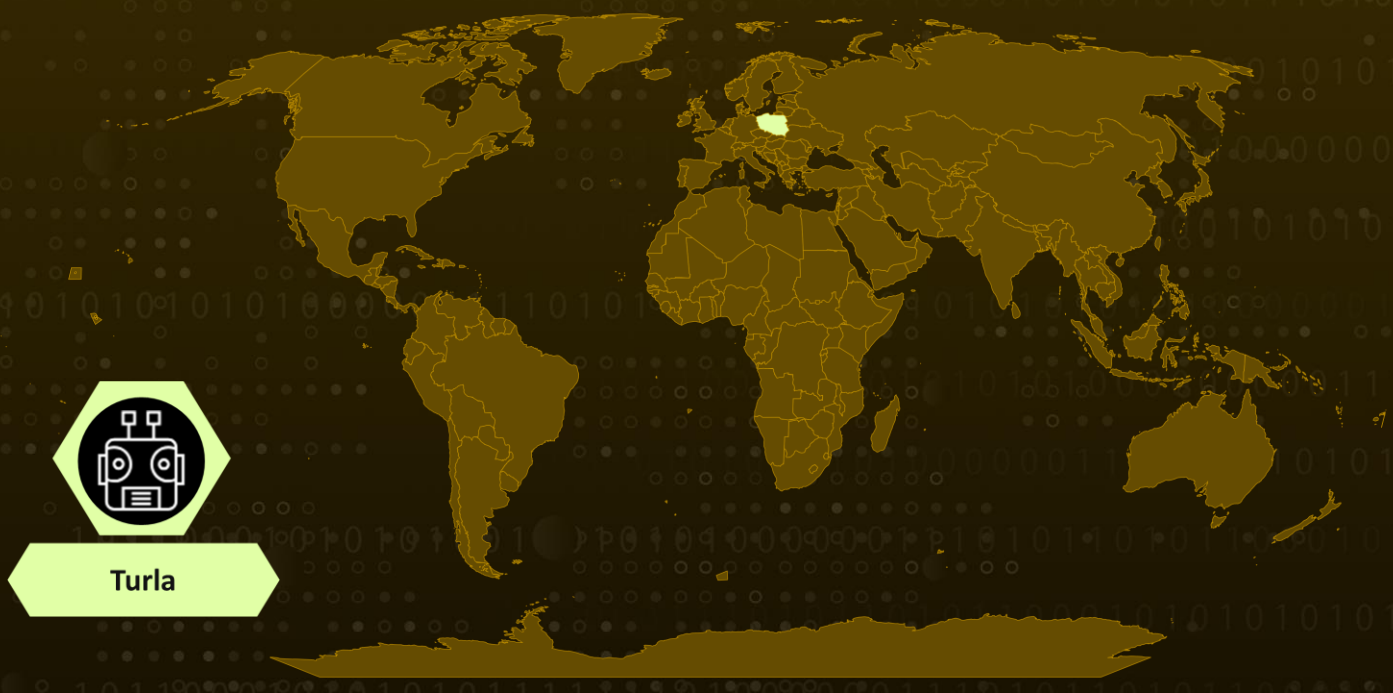
Turla Expands Their Arsenal with Next-Generation Malwares

Date of Publication	Last Update Date	Admiralty Code	TA Number
February 16, 2024	February 23, 2024	A1	TA2024061

Summary

Attack Discovered: December 2023
Attack Region: Poland
Malware: TinyTurla-NG (TTNG), TurlaPower-NG
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)
Attack: In December 2023, a new backdoor dubbed TinyTurla-NG was deployed by the Russia-affiliated threat actor Turla as part of a three-month campaign targeting Polish non-governmental organizations (NGOs). The threat actor utilized malicious PowerShell scripts hosted on various websites, exploiting vulnerable versions of WordPress for their C2 operations.

Attack Regions



Attack Details

#1 In December 2023, the Russian hacker group Turla employed new malware, named TinyTurla-NG and TurlaPower-NG, to gather sensitive data and maintain access to a targeted network. The threat actor utilized malicious PowerShell scripts and took advantage of several websites running vulnerable versions of WordPress for their C2 operations.

#2 Turla, a cyber espionage group active since 2004, has been associated with the Russian intelligence agency Federal Security Service (FSB). Expanding its target scope to include non-governmental organizations, Turla has introduced the TinyTurla-NG and TurlaPower-NG malware families to its toolkit.

#3 In its recent campaign targeting Polish non-governmental organizations, the Turla threat group utilized compromised WordPress websites as the C2 endpoints for its TTNG backdoor. The group leveraged vulnerable versions of WordPress on several websites to host PHP files with C2 code. Multiple C2 servers were employed to host PowerShell scripts and execute arbitrary commands on the target computers throughout the three-month campaign.

#4 The malware invokes distinct threads for various features and leverages windows events for synchronization. The malware responds to various commands and provide functionalities such as initiating sleep, changing shells, executing commands, exfiltrating files from the victim's system, and generating a BAT file with a specific name.

#5 TinyTurla-NG serves as a vehicle for deploying TurlaPower-NG PowerShell scripts, which have the specific purpose of extracting key material from password databases commonly found in popular password management software. The threat actors focus on extracting key material from password databases and related files associated with password management software, all of which are then included in the archive. Following this process, the script exfiltrates the archive via HTTP/S POST requests.

#6 Additionally, TinyTurla-NG introduces a tunneling tool named Chisel to establish a reverse SOCKS proxy connection. This tool is bundled into a single UPX-compressed file. TinyTurla-NG functions as a "last resort" backdoor, similar to TinyTurla; it is used in situations where all other attempts to gain unauthorised access or detection have failed or have been discovered on compromised systems. The development of new NG-malwares and the recent Turla campaign implies the group's desire to expand its malware arsenal and target base.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Always ensure to download software from trusted and reputable sources to minimize the risk of inadvertently installing malware or malicious programs on your system.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
T1070 Indicator Removal	T1566 Phishing	T1102 Web Service	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1083 File and Directory Discovery	T1056 Input Capture
T1560 Archive Collected Data	T1041 Exfiltration Over C2 Channel	T1071 Application Layer Protocol	T1071.001 Web Protocols

T1105 Ingress Tool Transfer	**T1552** Unsecured Credentials	**T1552.004** Private Keys	**T1555** Credentials from Password Stores
T1555.005 Password Managers	**T1555.003** Credentials from Web Browsers	**T1036** Masquerading	**T1027** Obfuscated Files or Information
T1027.002 Software Packing			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b, d6ac21a409f35a80ba9ccfe58ae1ae32883e44ecc724e4ae8289e7465ab2cf40, ad4d196b3d85d982343f32d52bffc6ebfeec7bf30553fa441fd7c3ae495075fc, 13c017cb706ef869c061078048e550dba1613c0f2e8f2e409d97a1c0d9949346, b376a3a6bae73840e70b2fa3df99d881def9250b42b6b8b0458d0445ddfbc044
Domains	hanagram[.]jp, thefinetreats[.]com, caduff-sa[.]ch, jeepcarlease[.]com, buy-new-car[.]com, carleasingguru[.]com
IP	91[.]193[.]18[.]120

References

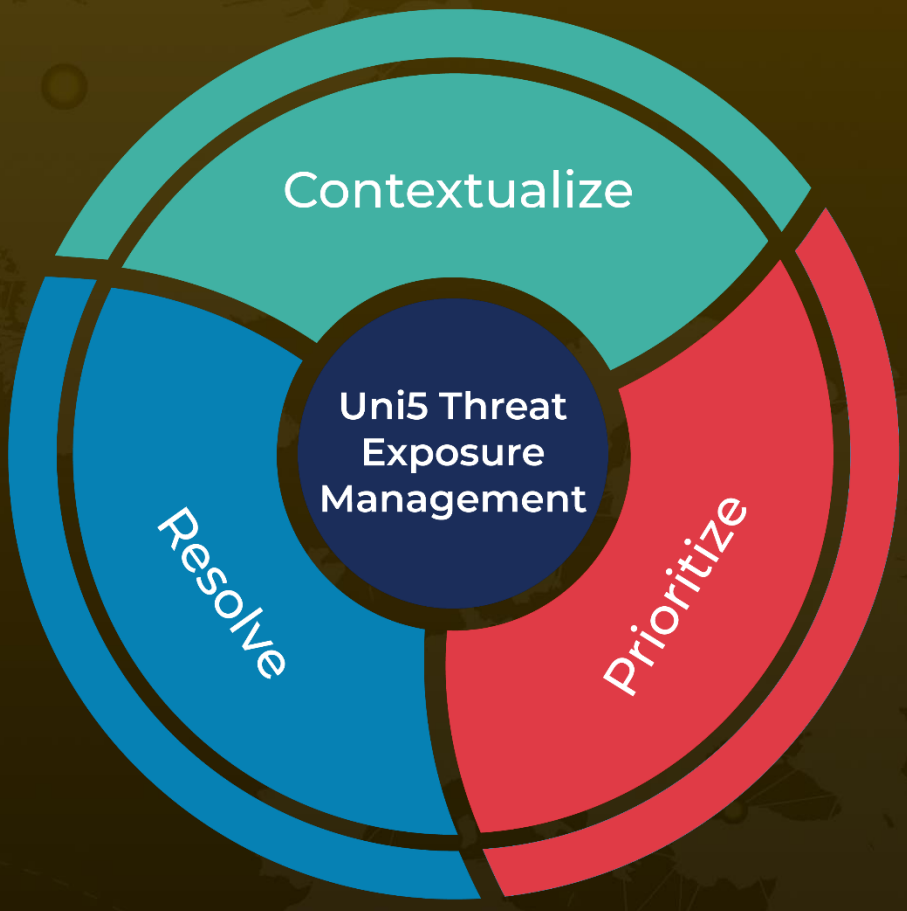
https://blog.talosintelligence.com/tinyturla-next-generation/

https://blog.talosintelligence.com/tinyturla-ng-tooling-and-c2/

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

February 16, 2024 • 4:45 AM

More at www.hivepro.com