Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

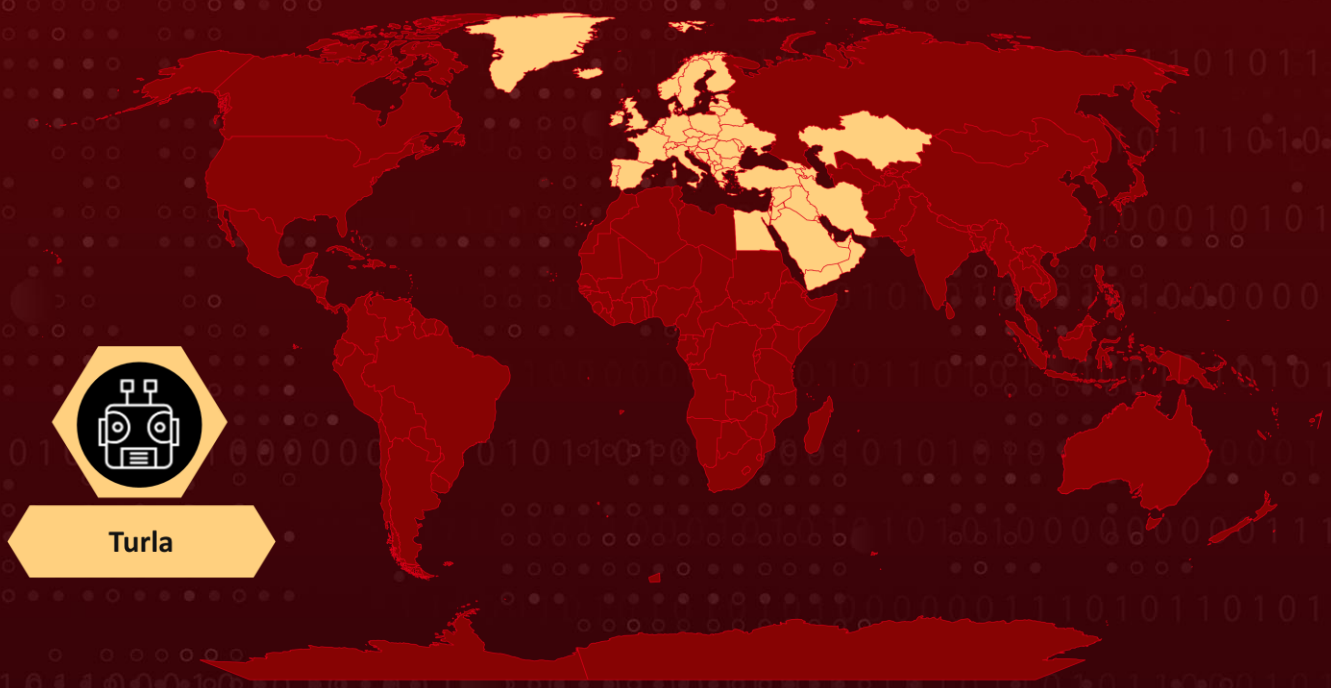
LunarWeb and LunarMail: The Secret Weapons of the Turla APT

Date of Publication	Admiralty Code	TA Number
May 16, 2024	A1	TA2024191

Summary

Attack Commenced: April 2022
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, Blue Python, Snake)
Malware: LunarLoader, LunarWeb, LunarMail
Attack Region: Europe, Middle East
Targeted Industries: Foreign Affairs, Diplomats
Attack: The notorious Turla Advanced Persistent Threat (APT) group, infiltrating a European ministry of foreign affairs and various Middle Eastern entities, skillfully evaded detection by discreetly deploying two previously undisclosed backdoors: LunarWeb and LunarMail.

Attack Regions



Attack Details

#1 The Turla Advanced Persistent Threat (APT) group, which infiltrated a European ministry of foreign affairs and Middle Eastern entities, managed to evade detection and deploy two previously unrecorded backdoors known as LunarWeb and LunarMail.

#2 These sophisticated backdoors share commonalities such as employing a loader that leverages DNS domain names for payload decryption, partially overlapping codebases, and possessing the unique capability of executing Lua scripts. While the precise method of intrusion remains elusive, suspicions point towards a blend of spear-phishing tactics and the exploitation of vulnerabilities within misconfigured Zabbix software.

#3 The initial phase of the attack chain unfolds with the utilization of a compiled version of an ASP.NET web page serving as a conduit for decoding two embedded blobs. These embedded binaries comprise LunarLoader, the designated loader, and the LunarWeb backdoor. Turla, also recognized as Snake, boasts a history possibly extending back to the late 1990s, with alleged affiliations to the Russian Federal Security Service (FSB), rendering it a formidable APT.

#4 LunarWeb, operational on servers, communicates with its command and control (C&C) infrastructure via HTTP(S), camouflaging its activities amidst legitimate requests. Conversely, LunarMail, entrenched within workstations, adopts the guise of an Outlook add-in and communicates with its C&C infrastructure via email messages. Both backdoors employ steganography, concealing commands within images to evade detection.

Recommendations

Implement File Integrity Monitoring (FIM): Deploy FIM solutions to monitor critical system files and configurations for unauthorized changes or modifications, detecting potential indicators of compromise and unauthorized access attempts by threat actors like the Turla APT group.

Adopt Zero Trust Architecture: Embrace a Zero Trust security model that verifies and validates every access attempt, regardless of whether it originates from inside or outside the network perimeter, reducing the attack surface and thwarting unauthorized access attempts by sophisticated adversaries.

Implement Network Monitoring: Deploy robust network monitoring tools to detect unusual or malicious activities, such as communication with unknown command and control servers or attempts to execute Lua scripts, indicative of potential cyber threats like those posed by the Turla APT group.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0042 Resource Development
TA0043 Reconnaissance	T1591 Gather Victim Org Information	T1583.002 DNS Server	T1583.003 Virtual Private Server
T1584.003 Virtual Private Server	T1586.002 Email Accounts	T1587.001 Malware	T1047 Windows Management Instrumentation
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.005 Visual Basic
T1106 Native API	T1204.002 Malicious File	T1137.006 Add-ins	T1547 Boot or Logon Autostart Execution
T1574 Hijack Execution Flow	T1027 Obfuscated Files or Information	T1027.003 Steganography	T1027.007 Dynamic API Resolution
T1027.009 Embedded Payloads	T1036.005 Match Legitimate Name or Location	T1070.004 File Deletion	T1070.008 Clear Mailbox Data
T1140 Deobfuscate/Decode Files or Information	T1480.001 Environmental Keying	T1620 Reflective Code Loading	T1007 System Service Discovery
T1016 System Network Configuration Discovery	T1057 Process Discovery	T1082 System Information Discovery	T1518.001 Security Software Discovery

T1005 Data from Local System	**T1074.001** Local Data Staging	**T1113** Screen Capture	**T1114.001** Local Email Collection
T1560.002 Archive via Library	**T1001.002** Steganography	**T1001.003** Protocol Impersonation	**T1071.001** Web Protocols
T1071.003 Mail Protocols	**T1090.001** Internal Proxy	**T1095** Non-Application Layer Protocol	**T1132.001** Standard Encoding
T1573.001 Symmetric Cryptography	**T1573.002** Asymmetric Cryptography	**T1020** Automated Exfiltration	**T1030** Data Transfer Size Limits
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
Registry Key	HKCU\SOFTWARE\Classes\CLSID\{3115036B-547E-4673-8479-EE54CD001B9D}\
Domain	thedarktower[.]av[.]master[.]dns-cloud[.]net
SHA1	00006b30806f915911349d82beeb1aeb9025adb4, 19d86cf2ed82eae23e019706fae8dafc60552e85, 2ed792e39f7d56de52bdf4aed96afc898478bfdf, 4c84110f1b10df5fdd612759e210e44b0f0505ef, 512e4fa7d6119270ff44a3b2a2359ee8825392ef, 5d3975e57bdcb630a00febe5d405eefb6d119d86, 5ef771afc96c24371d367448627609cfacb34a57, 67c6aec8d129e610378ef52f8bf934886587932f, 754fb657156643fd09a68ec9fc124528578cab0c, 795c4127d42fe8dfaf4510b406b52ba5bede8d3a, 94a4ce9c75bc847e7be59b96c4133d677d909414, 9cec3972fa35c88de87bd66950e18b3e0a6df77c, de83c2c3fe68cb1bf96173e9ee3ea6161dcfb24a, f09e36553e48ebd42e60d9b25a390c0f57ff8de0, fcae66f6d95c78dc829688cc0f4c39bb5a57828b

TYPE	VALUE
IPv4	45[.]33[.]24[.]145, 45[.]79[.]93[.]87, 82[.]165[.]158[.]86, 82[.]223[.]55[.]220, 139[.]162[.]23[.]113, 161[.]97[.]74[.]237, 176[.]57[.]150[.]252, 212[.]57[.]35[.]174, 212[.]57[.]35[.]176, 74[.]50[.]80[.]35, 158[.]220[.]102[.]80, 65[.]109[.]179[.]67
File Path	C:\Windows\System32\DynamicAuth.bin, C:\Program Files\LAPS\CSE\admpwd.cache, C:\ProgramData\Microsoft\WinThumb\adcache.clb, C:\Windows\System32\perfcache.dat, %USERPROFILE%\Gpg4win\tempkeys.dat, C:\ProgramData\Microsoft\Windows\Templates\content.tpl, C:\ProgramData\Microsoft\WinThumb\thumb.clb, C:\ProgramData\Microsoft\WinThumb\cfcache.clb, C:\Windows\System32\perfconfm.dat, %LOCALAPPDATA%\Microsoft\Outlook\outlk.share
File Name	admpwd.dll, App_Web_0bm4blbr.dll, gpgol.dll

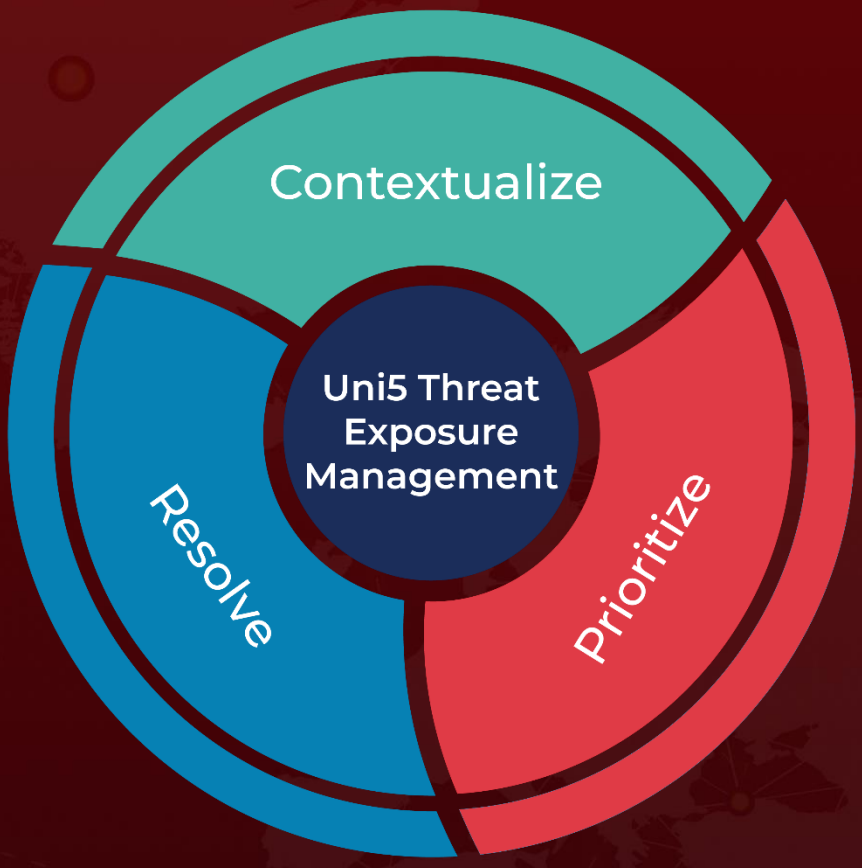
References

https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

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 16, 2024 • 9:00 PM

More at www.hivepro.com