Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Turla Updates KAZUAR Backdoor to Target Ukraine's Defense Sector

Date of Publication	Last updated date	Admiralty Code	TA Number
July 21, 2023	November 10, 2023	A1	TA2023309

Summary

First Appearance: 2022
Attack Region: Ukraine and Eastern Europe
Actor Name: 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)
Affected Platform: Windows
Malware: DeliveryCheck (aka CAPIBAR, GAMEDAY), KAZUAR
Targeted Industries: Defense, Government, Military, Aerospace
Attack: Turla's Kazuar variant remains a persistent threat, accompanied by a new .NET-based backdoor, DeliveryCheck, attributed to Russian actor Turla. The attacks target Ukraine's defense sector, utilizing tactics like PowerShell DSC and signaling a dynamic cybersecurity landscape.

Attack Regions

Attack Details

#1 While tracking the evolution of Turla (aka Pensive Ursa, Uroburos), researchers discovered a new variant of Kazuar, an advanced and stealthy .NET backdoor. This variant was found in a campaign targeting the Ukrainian defense sector. Turla, a Russian-based threat group linked to the Russian Federal Security Service (FSB), has been using Kazuar as a second-stage payload since at least 2004.

#2 The new Kazuar variant significantly improves code structure and functionality, offering comprehensive system profiling, credential theft from cloud and sensitive applications, extended command sets, and enhanced automation. The malware emphasizes encryption, obfuscation, and anti-dumping mechanisms to evade detection and analysis.

#3 In addition to the Kazuar discovery, a .NET-based backdoor called DeliveryCheck (also known as CAPIBAR or GAMEDAY) has been targeting the defense sector in Ukraine and Eastern Europe. The attacks have been attributed to a Russian nation-state actor called Turla, which is associated with Russia's Federal Security Service (FSB).

#4 DeliveryCheck is distributed through malicious macros in email attachments and persists via scheduled tasks that download and launch it in memory. It communicates with a command-and-control (C2) server to retrieve tasks, which can include launching arbitrary payloads embedded in XSLT stylesheets.

#5 Notably, DeliveryCheck can breach Microsoft Exchange servers and employs PowerShell Desired State Configuration (DSC) to install a server-side component that turns legitimate servers into malware C2 centers.

#6 The attacks involve the distribution of a known Turla implant called Kazuar, capable of stealing data from web browsers, application configuration files, and event logs. The ultimate goal of these attacks is to exfiltrate messages from the Signal messaging app on Windows systems, enabling the attacker to access sensitive conversations, documents, and images.

#7 Previously, the **Turla Group** distributed KOPILUWAK reconnaissance software and the QUIETCANARY backdoor to victims of ANDROMEDA malware in Ukraine.

#8 This update highlights the evolving tactics of threat actors like Turla and Turla, showcasing the constant development and deployment of sophisticated malware tools in targeted campaigns against critical sectors. Security practitioners are advised to stay vigilant, incorporating the provided insights to enhance their cybersecurity defenses.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious macros.

Endpoint Protection: Deploy reputable endpoint protection software that includes anti-malware and behavior-based detection capabilities to identify and block suspicious activities on endpoints.

Network Segmentation: Implement network segmentation to restrict lateral movement in case of a breach. Isolate critical systems and sensitive data to minimize the potential impact of a security incident.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0040 Impact	TA0043 Reconnaissance
TA0010 Exfiltration	TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1220 XSL Script Processing
T1005 Data from Local System	T1027 Obfuscated Files or Information	T1027.009 Embedded Payloads	T1547 Boot or Logon Autostart Execution
T1567 Exfiltration Over Web Service	T1105 Ingress Tool Transfer	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1090 Proxy	T1104 Multi-Stage Channels	T1055 Process Injection	T1190 Exploit Public-Facing Application

T1546 Event Triggered Execution	T1566.001 Spearphishing Attachment	T1566 Phishing	T1041 Exfiltration Over C2 Channel
T1070 Indicator Removal	T1573 Encrypted Channel	T1056 Input Capture	T1110 Brute Force
T1562 Impair Defenses	T1102 Web Service	T1113 Screen Capture	T1053 Scheduled Task/Job

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	11a289347b95aab157aa0efe4a59bf24, 153b713b3c6e642f39993d65ab33c5f0, 17402fc21c7bafae2c1a149035cd0835, 4065e647380358d22926c24a63c26ac4, 420b7dc391f2cb0a9a684c1c48c334e2, 491e462bf1213fede82925dea5df8fff, 5210b3d85fd0026205baee2c77ac0acd, 5c7466a177fcaad2ebab131a54c28fab, 65102299bf8d7f0129ebbcb08a9c2d98, 8c56c22343853d3797037bdac2cec6c7, 9dd2bea4f2df8d3ef51dc10c6db2e07a, 9ececb4acbf692c2a8ea411f2e7dd006, b63c2ec9a631e0217d39c4a43527a0ce, cba1f4c861240223332922d2913d18e5, cdf7fa901701ea1ef642aeb271c70361, D3065b4b1e8f6ecb63685219113ff0b8, 169739e7211295146a61d300c0fef02d
SHA256	01c5778be73c10c167fae6d7970c0be23a29af1873d743419b1803c035d92ef7, 07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57, 19b7ddd3b06794abe593bf533d88319711ca15bb0a08901b4ab7e52aab015452, 1c1bb64e38c3fbe1a8f0dcb94ded96b332296bcbf839de438a4838fb43b20af3, 1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc, 4ef8db0ca305aaab9e2471b198168021c531862cb4319098302026b1cfa89947,

TYPE	VALUE
SHA256	5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e, 5e122ff3066b6ef2a89295df925431c151f1713708c99772687a30c3204064bd, 64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a, 8168dc0baea6a74120fbabea261e83377697cb5f9726a2514f38ed04b46c56c8, 91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233, aaf7642f0cab75240ec65bc052a0a602366740b31754156b3a0c44dccec9bebe, b8ee794b04b69a1ee8687daabfe4f912368a500610a099e3072b03eeb66077f8, ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39, bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76, 01c5778be73c10c167fae6d7970c0be23a29af1873d743419b1803c035d92ef7, 07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57, 19b7ddd3b06794abe593bf533d88319711ca15bb0a08901b4ab7e52aab015452, 1c1bb64e38c3fbe1a8f0dcb94ded96b332296bcbf839de438a4838fb43b20af3, 1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc, 4ef8db0ca305aaab9e2471b198168021c531862cb4319098302026b1cfa89947, 5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e, 5e122ff3066b6ef2a89295df925431c151f1713708c99772687a30c3204064bd, 64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a, 8168dc0baea6a74120fbabea261e83377697cb5f9726a2514f38ed04b46c56c8, 91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233, aaf7642f0cab75240ec65bc052a0a602366740b31754156b3a0c44dccec9bebe, b8ee794b04b69a1ee8687daabfe4f912368a500610a099e3072b03eeb66077f8, ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39, bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76, 91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233, d4d7c12bdb66d40ad58c211dc6dd53a7494e03f9883336fa5464f0947530709f

TYPE	VALUE
Hostname	www[.]pierreagencement[.]fr
URLs	http://aleimportadora[.]net/images/slides_logo/, http://aleimportadora[.]net/images/slides_logo/?page=, http://aleimportadora[.]net/images/slides_logo/fg/message, http://aleimportadora[.]net/images/slides_logo/fg/music, http://aleimportadora[.]net/images/slides_logo/fg/video, http://aleimportadora[.]net/images/slides_logo/index[.]php, http://atomydoc[.]kg/src/open_center/, http://atomydoc[.]kg/src/open_center/?page=ccl, http://atomydoc[.]kg/src/open_center/?page=fst, http://atomydoc[.]kg/src/open_center/?page=snd, http://atomydoc[.]kg/src/open_center/?page=trd, http://mail[.]aet[.]in[.]ua/outlook/api/logoff[.]aspx, http://mail[.]aet[.]in[.]ua/outlook/api/logon[.]aspx, http://mail[.]arlingtonhousing[.]us/outlook/api/logoff[.]aspx, http://mail[.]kzp[.]bg/outlook/api/logoff[.]aspx, http://mail[.]kzp[.]bg/outlook/api/logon[.]aspx, http://mail[.]lebsack[.]de/MICROSOFT[.]EXCHANGE[.]MAILBOXREPLICATIONSERVICE[.]PROXYSERVICE/RPCWITHCERT/SYNC, http://mail[.]lechateaudelatour[.]fr/MICROSOFT[.]EXCHANGE[.]MAILBOXREPLICATIONSERVICE[.]PROXYSERVICE/RPCWITHCERT/SYNC, http://mail[.]numina[.]md/owa/scripts/logon[.]aspx, http://octoberoctopus[.]co[.]za/wp-includes/sitemaps/web/, http://sansaispa[.]com/wp-includes/images/gallery/, http://www[.]adelaida[.]ua/plugins/vmsearch/wp-config-plugins[.]php, http://www[.]adelaida[.]ua/plugins/vmsearch/wp-config-themes[.]php, http://www[.]adelaida[.]ua/plugins/vmsearch/wp-file-script[.]js, http://www[.]pierreagencement[.]fr/wp-content/languages/index[.]php, https://www[.]pierreagencement[.]fr/wp-content/languages/index[.]php, https://octoberoctopus[.]co[.]za/wp-includes/sitemaps/web/, https://sansaispa[.]com/wp-includes/images/gallery/
Domains	aleimportadora[.]net, atomydoc[.]kg, octoberoctopus[.]co[.]za, sansaispa[.]com, mail[.]aet[.]in[.]ua, mail[.]arlingtonhousing[.]us, mail[.]kzp[.]bg, mail[.]lebsack[.]de, mail[.]lechateaudelatour[.]fr, mail[.]numina[.]md, www[.]adelaida[.]ua, www[.]pierreagencement[.]fr, sansaispa[.]com, octoberoctopus[.]co[.]za

References

https://twitter.com/MsftSecIntel/status/1681695399084539908

https://cert.gov.ua/article/5213167

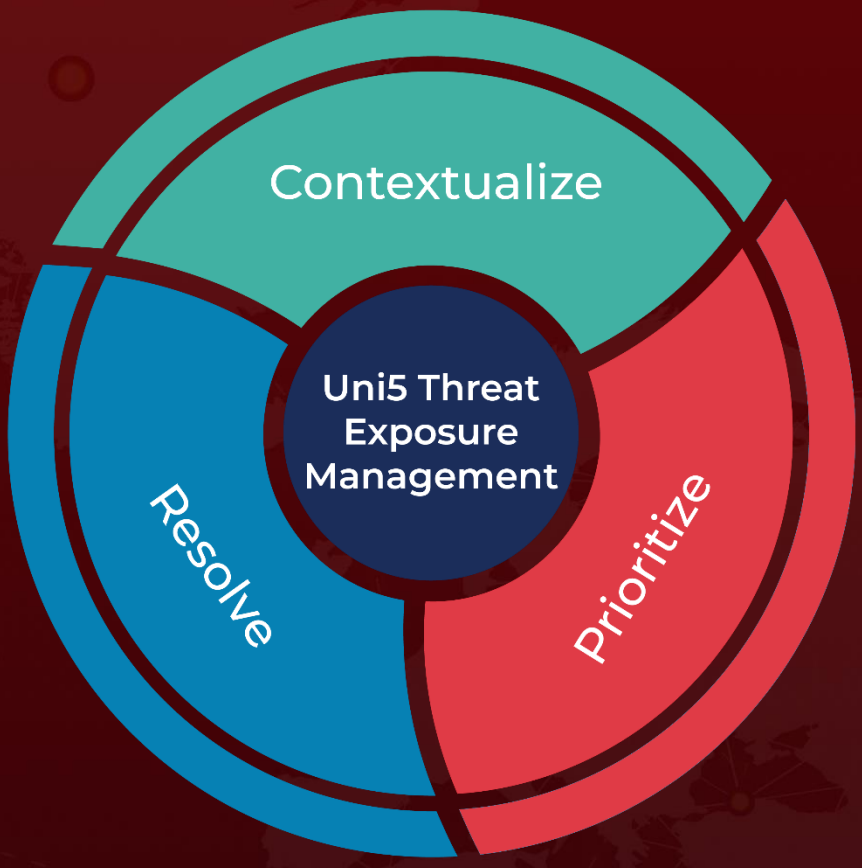
https://www.hivepro.com/turla-apt-used-andromeda-malware-to-infiltrate-a-variety-of-industries/

https://unit42.paloaltonetworks.com/pensive-ursa-uses-upgraded-kazuar-backdoor/

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

July 21, 2023 • 6:30 AM

More at www.hivepro.com