Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

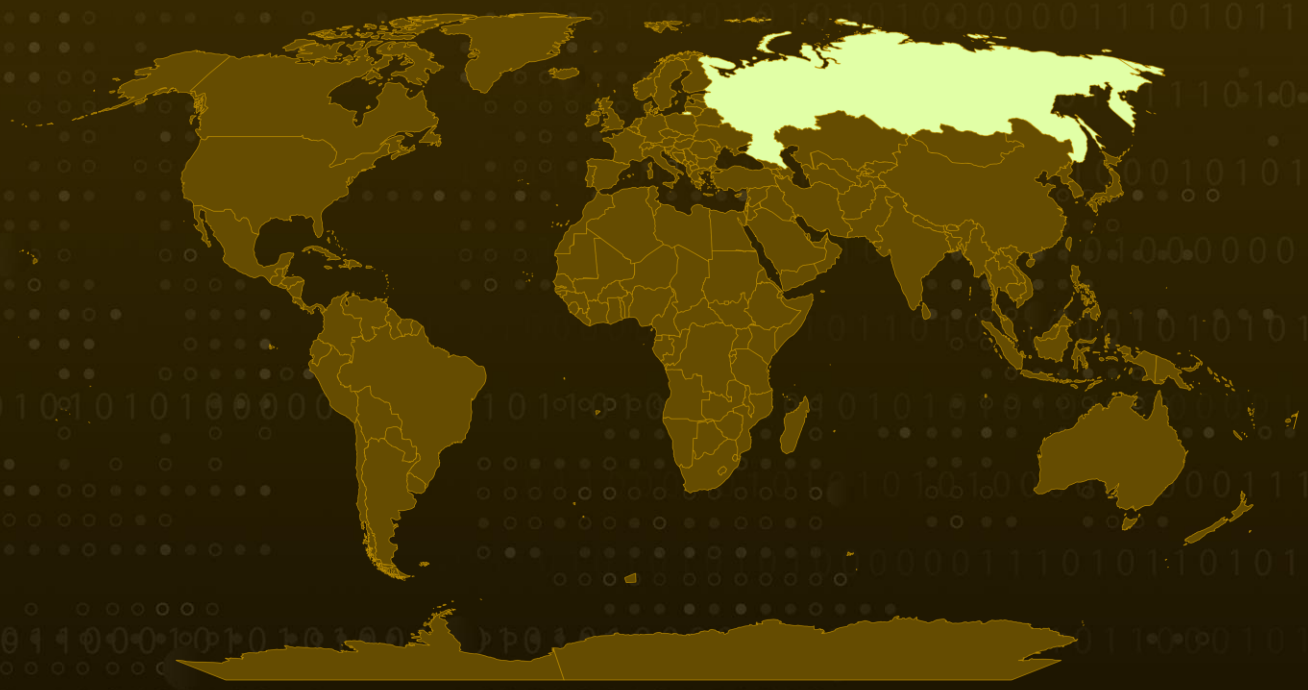
Hackers Infiltrate Russian Government and Industrial Entities

Date of Publication	Admiralty Code	TA Number
October 25, 2023	A1	TA2023431

Summary

Attack Began: June 2023
Malware: Netrunner, Dmcserv
Attack Region: Russia
Targeted Industries: Government and Industrial Organizations
Attack: Numerous governmental and pivotal industrial entities in Russia fell victim to a sophisticated Go-based custom backdoor. This malicious software was specifically crafted for data theft, suggesting its involvement in secretive intelligence operations.

Attack Regions



Attack Details

#1 In June 2023, a targeted campaign struck several government and industrial entities within the Russian Federation, employing a customized Go-based backdoor designed for data exfiltration, strongly implying involvement in covert intelligence activities. By mid-August, a newer iteration of this backdoor emerged, showcasing enhanced evasion tactics, underscoring the campaign's ongoing refinement. The adversaries behind this operation remain unidentified.

#2 The infection chain commenced with a malicious ARJ file attached to an email, containing a ruse PDF document intended to distract the target. An NSIS script within the archive was responsible for retrieving the primary payload from an external URL and executing it. The malevolent software, scripted in Go, meticulously obfuscated its function and variable names.

#3 It's worth noting that the initial phishing wave included two additional backdoors named Netrunner and Dmcserv, distinguished primarily by their command-and-control (C2) server configurations. Upon execution, the malware diligently checked for internet access and whether it was operating within a virtual environment or sandbox.

#4 Subsequently, it launched its core malicious executables discreetly and established persistence by creating a Start Menu link. Any data sent to the C2 server underwent AES encryption to evade detection by network monitoring solutions. In mid-August, a fresh iteration of the backdoor underwent minor adjustments, removing some noisy preliminary checks while introducing new file-stealing capabilities.

#5 Most notably, this version featured a module targeting user passwords stored in 27 web browsers and the Thunderbird email client. Furthermore, the malware refreshed its AES key and incorporated RSA asymmetric encryption to fortify communications between clients and the C2 server.

Recommendations

Browser and Email Client Security: Ensure that web browsers and email clients are securely configured and up to date to mitigate password theft attempts targeting 27 different web browsers and the Thunderbird client.

Zero Trust Architecture: Implement a zero-trust approach to network security, where no entity, whether inside or outside the network, is trusted by default, and strict identity verification is required.

Network Segmentation: Segment your network into isolated zones to limit lateral movement for attackers and reduce the impact of a breach. Deploy network traffic analysis tools to monitor and analyze patterns of communication between endpoints and potential command and control servers

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1059.003 Windows Command Shell	**T1204.002** Malicious File	**T1547.001** Registry Run Keys / Startup Folder	**T1202** Indirect Command Execution
T1070.004 File Deletion	**T1027** Obfuscated Files or Information	**T1087.001** Local Account	**T1083** File and Directory Discovery
T1518.001 Security Software Discovery	**T1082** System Information Discovery	**T1033** System Owner/User Discovery	**T1560.002** Archive via Library
T1005 Data from Local System	**T1071.001** Web Protocols	**T1132.001** Standard Encoding	**T1573.001** Symmetric Cryptography
T1566.001 Spearphishing Attachment	**T1041** Exfiltration Over C2 Channel	**T1497** Virtualization/Sandbox Evasion	**T1560** Archive Collected Data

Indicators of Compromise (IOCs)

TYPE	VALUE
File Names	finansovyy_kontrol_2023_180529.com, detali_dogovora_no_2023_000849.com, Dogovor_No_0339_07_23.com, No_9537_23.com
File Paths	C:\ProgramData\UsrRunVGA, C:\ProgramData\Dmcserv, C:\ProgramData\netrunner, C:\ProgramData\Microsoft\DeviceSync\UsrRunVGA.exe, C:\ProgramData\Mi crosoft\DeviceSync\Dmcserv.exe, C: \ProgramData\Microsoft\DeviceSync\netrunner.exe, %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\StartUp\menu.lnk, C:\Users\{USERPROFILE}\AppData\Local\Temp\homef.dat, C:\Users\{USERPROFILE}\AppData\Local\Temp\ds[AZ]{1}.dat, C:\Users\{USERPROFILE}\AppData\Local\Temp\lg_[A-Za-z]{10} .dat, C:\Users\{USERPROFILE}\AppData\Local\Temp\[0-9]{10}\[A-Za-z]{10}.enc, C:\Users\{USERPROFILE}\AppData\Local \Temp\[0-9]{10}\[A-Za-z]{10}.txt, C:\ProgramData\VirtualDriveModule C:\ProgramData, \UsrNetBrooker C:, \ProgramData\Microsoft\DeviceSync \VirtualDriveModule.exe, C:\ProgramData\Microsoft\DeviceSync\UsrNetBrooker.exe
User-Agent	Mozilla/5.0, Mozilla/5.0 (Windows NT 10.0; Win64; x64), AppleWebKit/537.36 (KHTML, like Gecko), Chrome/91.0.4472.124, Safari/537.36, Edg/91.0.864.5
Domains	fas-gov-ru[.]com, tantsuyushchiykarlik[.]com, skachanye-ru[.]com, mirvovsemire[.]com, vlozhenye24[.]com, megaworstqal[.]com, vlozhenye-ru[.]com, lunnayareka[.]com, fas- otdel-ru[.]com, beshenayasobaka[.]com
MD5	0777dfa3ca844ff59661c261c5b48ba6, 131cb8061a042fc13a640bf783030ded, 16074c7518b2e5a3335ccf5aaa469470, 1ecf7dde0f692e635688b181fe7ae8bb,

TYPE	VALUE
MD5	24e5a0d1f0bc19d36aee67a715b0b573, 25eb1b4534a91524e6a293b459d71a19, 2cd36bcc238b797c5dd224a6aa80cef4, 2e8a4a6d19cac2653279dab822d69bf5, 35b192d30a6e495d36c0eb0fde06409e, 44cfdac04e1cb3e813bb8f0c3d695f56, 45de46b40e80cf37c8125a7dbfe60fae, 45f824b00d2ad14181803ae5c63bebd3, 509901d73fe39a5f46fdb2bfc9c7de9f, 51b6c1454fc79179c66ca4f949d201e9, 5ee1e79b341510858d609b67648da6bb, 6086673a65b85b3463b551ba611ee6e6, 64865d6f2e8fe256d2a8de6c97c3c661, 678dbd5294150f0dedd125eed41e7728, 67b388477cedd7aaa1054fefa4f20db0, 67e38a5bd8d14ba507124894fa988342, 6b944c0e8c2d76a2dc2477c720e82f14, 6ce34d82d23b6a73b54e957c9cba7fc0, 787ec689241c2b01954045879be30ed2, 88219b612564d0821f86c4f3dc1ff5f5, 9722e3e0db3774ebdceef142d8143956, 9da5e7c549b30f5f8507dc6aadb3cf9d, a383f9f87218897ae3fbcfa8f3617aa9, ab2f197a1ed2d418e9bb717aaa057cf2, af39ff63a49f170d70736d4e9c619012, b5b796db5331655b6c7f44f5dcfb60e7, b994b476a45d76173f048cbb247013f4, b9f91e09b24f0d249147e5ecec8ed6b8, bab4065f4e9f569f0658ea9e33459ef2, c842b05b4315cc6ca1b015812b31e3fb, c87ba9afe2cb05f286f909eb4db79726, e57e91eb891e4cb98fa16fc2e740b39d, e9253667a17f36ba12622f5170a59d40, ebaaef4d739001f49a0e4d05a10284bf, f7664bf2e56403d1e235dc302bf807f1, fe3887c853846c7fd8bb7aa8f87d6a18

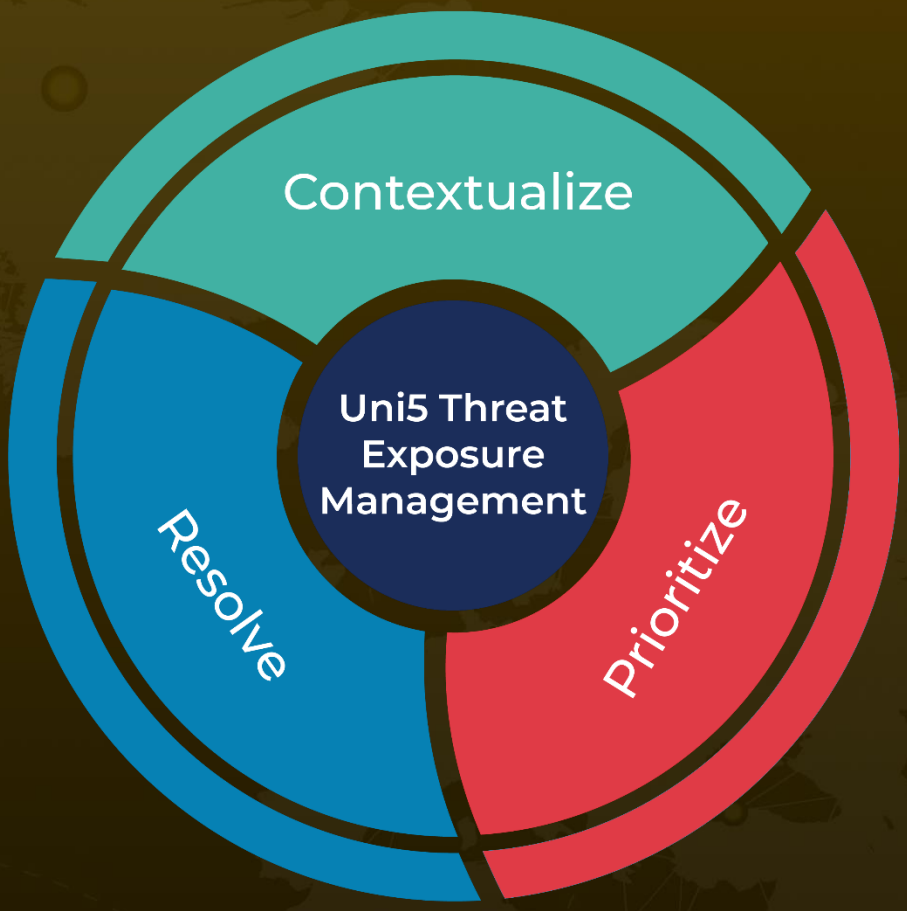
References

https://web.archive.org/web/20231024145301/https://securelist.ru/ataki-na-industrialnyj-i-gosudarstvennyj-sektory-rf/108229/

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

October 25, 2023 • 4:30 AM

More at www.hivepro.com