Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

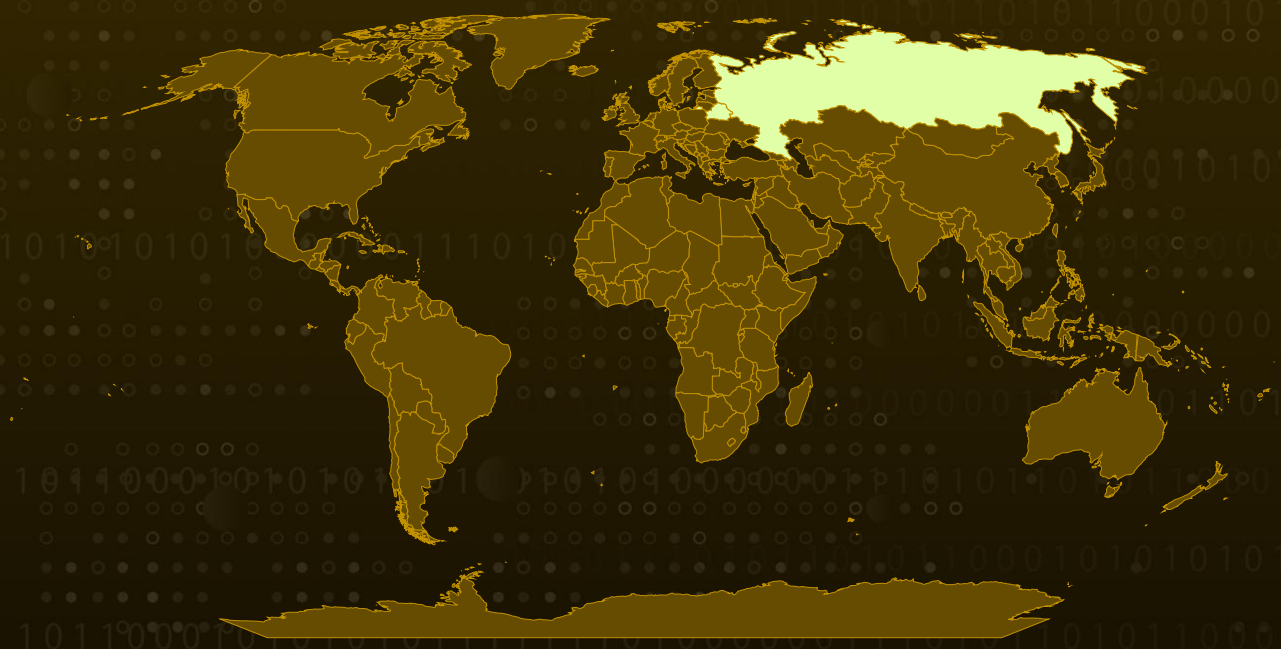
Operation SkyCloak: Covert Cyber Strikes on Russian and Belarusian Military Personnel

Date of Publication	Admiralty Code	TA Number
November 4, 2025	A1	TA2025335

Summary

Attack Discovered: 2025
Targeted Countries: Russia and Belarus
Targeted Industry: Defence
Campaign: Operation SkyCloak
Affected Platform: Windows
Attack: A stealthy cyber campaign, Operation SkyCloak, has surfaced targeting Russian and Belarusian military personnel, using phishing lures disguised as official military letters to deploy PowerShell scripts, Tor bridges, and hidden OpenSSH servers for covert access. The attackers built a complex infection chain that hides communication through obfs4 Tor bridges, executes decoy-laced payloads, and maintains persistence via scheduled tasks and custom onion services. The campaign's precision and use of anonymizing infrastructure suggest a calculated effort to infiltrate defense networks while staying hidden under the radar.

Attack Regions



Attack Details

#1 A focused cyber campaign, Operation SkyCloak, has been observed targeting military personnel in Russia and Belarus, notably elements of the Russian Airborne and Belarusian special operations community. The intrusion chain favors stealth: initial lures and PowerShell-based stagers, covert command-and-control over Tor using obfs4 bridges, and an embedded OpenSSH server deployed inside user profiles to enable discreet remote administration.

#2 Two separate military-themed letters are included in the dataset and help contextualize potential targeting. Several archived files from Belarus were weaponized in late September 2025 and contain a classic phishing artifact: a ZIP archive with a double-extension LNK shortcut. The shortcuts, associated with machine IDs desktop-V7i6LHO and desktop-u4a2HgZ, trigger PowerShell commands that unpack a staged archive. A secondary archive is recovered from a FOUND.000 folder and drops payloads, a text file, then executes a hidden PowerShell script. The packages include multiple EXEs, text files, a decoy PDF, a DLL, and XML configuration files, together supporting a multi-stage deployment that culminates in script execution.

#3 The PowerShell stager performs environmental reconnaissance and anti-sandbox checks, enforces single-instance execution via a mutex, parses XML for configuration, and installs scheduled tasks to survive reboots. It constructs an onion address and waits for a local Tor process to be ready before issuing an identification beacon over Tor, implemented with curl tunneled through a Tor SOCKS listener and robust retry logic to maximize reliability. These behaviors point to an operator preference for resilience and low observability rather than brute-force persistence.

#4 The configuration artifacts reveal two distinct SSHD deployments. One bundle listens on a nonstandard port (20321) with password authentication disabled and public-key only access, implying a hardened, stealth SSH instance. A second setup runs under tor.exe and exposes multiple services through an onion service, using an obfs4 pluggable transport implemented by binaries presented as confluence.exe or rider.exe (acting as obfs4proxy) and connecting to defined bridge endpoints by IP, port, fingerprint, and certificate. Netflow shows bridge traffic originating from Russia and neighboring countries; the IPs are classified variously as Tor nodes or residential hosts with little activity on targeted ports.

#5 In sum, this is a multi-chain, stealth-focused intrusion that leverages PowerShell, OpenSSH, and Tor bridges to enable covert remote access and lateral movement against defense and government-adjacent targets in Eastern Europe.

Recommendations

- **Update and Patch Regularly:** Make sure all operating systems and software, especially PowerShell, Tor, and OpenSSH, are fully updated. Attackers often exploit unpatched systems to gain a foothold.
- **Disable PowerShell Where Unnecessary:** If PowerShell isn't required for daily operations, disable or restrict its use through group policies. This helps block malicious scripts used for initial infection and persistence.
- **Inspect Scheduled Tasks and Startup Entries:** Review Windows Task Scheduler for any unexpected or hidden tasks. Attackers often create these to maintain access even after reboots.
- **Check for Suspicious Files and Directories:** Look for strange folders like dynamicUpdatingHashingScalingContext, logicpro, or reaper under %APPDATA%. Their presence could indicate malware components or staging areas.
- **Educate Users About Phishing:** Be cautious with email attachments, especially ZIP or LNK files with double extensions. Encourage them to report anything suspicious immediately.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**T1583** Acquire Infrastructure	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1204** User Execution	**T1204.002** Malicious File	**T1059** Command and Scripting Interpreter

T1059.001 PowerShell	**T1106** Native API	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task
T1547 Boot or Logon Autostart Execution	**T1027** Obfuscated Files or Information	**T1036** Masquerading	**T1497** Virtualization/Sandbox Evasion
T1083 File and Directory Discovery	**T1046** Network Service Discovery	**T1033** System Owner/User Discovery	**T1021** Remote Services
T1119 Automated Collection	**T1071** Application Layer Protocol	**T1090** Proxy	**T1571** Non-Standard Port
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	952f86861feeaf9821685cc203d67004, d246dfa9e274c644c5a9862350641bac, 8716989448bc88ba125aead800021db0, ae4f82f9733e0f71bb2a566a74eb055c, 32bdbf5c26e691cbbd451545bca52b56, 2731b3e8524e523a84dc7374ae29ac23, 39937e199b2377d1f212510f1f2f7653, 9242b49e9581fa7f2100bd9ad4385e8c, b61a80800a1021e9d0b1f5e8524c5708, b52dfb562c1093a87b78ffb6bfc78e07, 45b16a0b22c56e1b99649cca1045f500, dcdf4bb3b1e8ddb24ac4e7071abd1f65, e1a8daea05f25686c359db8fa3941e1d, b3382b6a44dc2cefdf242dc9f9bc9d84, 229afc52dccd655ec1a69a73369446dd, f6837c62aa71f044366ac53c60765739, 2599d1b1d6fe13002cb75b438d9b80c4, b7ae44ac55ba8acb527b984150c376e2, 0f6aaa52b05ab76020900a28afff9fff, 219e7d3b6ff68a36c8b03b116b405237,

TYPE	VALUE
MD5	dfc78fe2c31613939b570ced5f38472c, 77bb74dd879914eea7817d252dbab1dc, f6c0304671c4485c04d4a1c7c8c8ed94, cdd065c52b96614dc880273f2872619f, 37e83a8fc0e4e6ea5dab38b0b20f953b, 6eafae19d2db29f70fa24a95cf71a19d, 664f09734b07659a6f75bca3866ae5e8, 6eafae19d2db29f70fa24a95cf71a19d, 23ad48b33d5a6a8252ed5cd38148dcb7, c8c41b7e02fc1d98a88f66c3451a081b
SHA256	30a5df544f4a838f9c7ce34377ed2668e0ba22cc39d1e26b303781153808a2c4, a939d1edcc422772124a373be68b7cb38110639db8b1f4b5dca0b7e94b8399e3, e555083bdb62cf9df6aa7101908d9dbb89f55788ddab2e3288d57e48d43abd35, f8dc5e9747ca7ea00c88817472d273c570fec6899134f419cd1ae98235db1830, 99ec6437f74eec19e33c1a0b4ac8826bcc44848f87cd1a1c2b379fae9df62de9, f44fa352c430d5f34462143daa726660be9d1bd0666ab2f3672df47adde55986, 7269b4bc6b3036e5a2f8c2a7908a439202cee9c8b9e50b67c786c39f2500df8f, 0b9df542755298cd0b087681efbfaf91d35209966ff3bd8368ba65bcc0536a59, fdbb5d65ee611b35ccca6dd00ee0f9288dbaef8be9d8a247b067c8de3826759f, a250eb4fa9e270006defb04f5cc8eaa56bb016697f4e97739ca49d7d8ff3c11f, 949bc47d0cbbca0eeb73e18722fe2aa45c7681344bfa0e3bc9a7f9a4a8a88341, 51f02908ff27e270999ce9b796d92ec866d397aaf42af8b3eb2654463e1c53fd, 2f1a2fc130eeef678c44d2f1a43be64283b13db001b6facd9c1e7135672d88f5, 21ce085622d3ce447f36552290f2c22bc4bda5e176620a5683bc3ed995d10344, a68a72f845931408740870dbd3f0eac3b7acdbae3fdc8ea86aa8dfe48d351ce6, 0ff79b5a5af723654a6a6b8ce879a0aed2b009cee93dc9a8452b7dc7608f7aae, 710e8c96875d6a3c1b4f08f4b2094c800658551065b20ef3fd450b210dcc7b9a,

TYPE	VALUE
SHA256	7946a2275c1c232eebed6ead95ea4723285950175586db1f95354b910b0a3cce, a0eed0e1ef8fc4129f630e6f68c29c357c717df0fe352961e92e7f8c93e5371b, feae0baf291ff54a1366f0cd628665d2b1c9fe279ce2544d4f84c7aa46064f3c, 08db5bb9812f49f9394fd724b9196c7dc2f61b5ba1644da65db95ab6e430c92b, feae0baf291ff54a1366f0cd628665d2b1c9fe279ce2544d4f84c7aa46064f3c, 5d3a6340691840d1a87bfab543faec77b4a9d457991dd938834de820a99685f7, f889e06affd416bbbb49361639ab67e61ea9c5e989f87d5eeefd4fba5491c77a
IPv4:Port	77[.]20[.]116[.]133[:]8080, 156[.]67[.]24[.]239[:]33333, 146[.]59[.]116[.]226[:]50845, 142[.]189[.]114[.]119[:]443
Tor Address	yuknkap4im65njr3tlprnpqwj4h7aal4hrn2tdieg75rpp6fx25hqbyd[.]onion

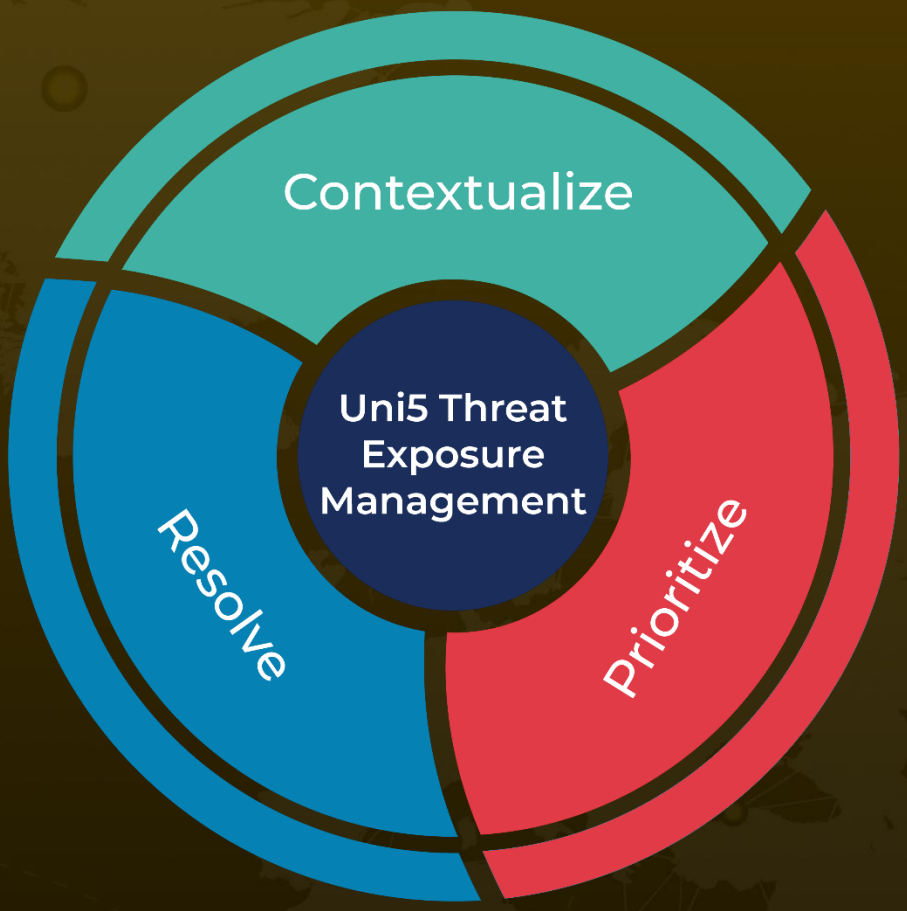
References

https://www.seqrite.com/blog/operation-skycloak-tor-campaign-targets-military-of-russia-belarus/

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

November 4, 2025 • 9:00 AM

More at www.hivepro.com