Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

# APT28 Targets Government Agencies with BEARDSHELL and COVENANT

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| June 25, 2025 | A1 | TA2025198 |

# Summary

**Attack Commenced:** March 2024
**Targeted Country:** Ukraine
**Malware:** BeardShell, Covenant, and SlimAgent
**Threat Actor:** APT28 (aka Sednit group, Sofacy, Fancy Bear, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Forest Blizzard, GruesomeLarch, BlueDelta, TA422, Fighting Ursa, Blue Athena, UAC-0063, TAG-110)
**Targeted Platforms:** Windows
**Targeted Industry:** Government
**Attack:** APT28 (UAC-0001), a Russian state-linked group, targeted government agencies with a sophisticated cyberattack using spear-phishing emails to deliver malicious documents via Signal. The attack deployed BEARDSHELL and COVENANT malware, enabling remote access and data exfiltration through trusted cloud services. By leveraging fileless techniques and legitimate platforms, the attackers evaded detection and maintained persistent control over compromised systems. This campaign highlights the evolving tactics of APT28 in targeting critical government infrastructure.

## Attack Regions

# Attack Details

**#1**

A recent cyberattack campaign attributed to the Russian state-sponsored group APT28 (also known as UAC-0001 or Fancy Bear) has targeted government agencies using sophisticated malware tools, including BEARDSHELL and COVENANT. The attackers initiated the operation via spear-phishing, distributing malicious Microsoft Word documents through the encrypted messaging app Signal. These documents contained macros which, once enabled, triggered a multi-stage, fileless infection chain designed for stealth and persistence.

**#2**

Upon execution, the macros dropped malicious DLLs and registry entries to hijack COM objects, specifically exploiting explorer.exe to stealthily launch shellcode hidden in image files. This shellcode loaded the COVENANT framework—a .NET-based command-and-control tool—directly into memory. By leveraging legitimate services like Koofr for C2 communications, the attackers obscured their traffic and evaded detection.

**#3**

COVENANT facilitated the delivery of further payloads, most notably BEARDSHELL, a custom backdoor written in C++ that decrypted and executed PowerShell scripts retrieved via the Icedrive API. BEARDSHELL used ChaCha20-Poly1305 encryption for its payloads and included features for full remote access. Another tool, SLIMAGENT, was used to capture and encrypt screenshots for exfiltration.

**#4**

The campaign's notable use of trusted platforms, Signal, Koofr, and Icedrive, enabled the attackers to blend malicious activity with legitimate traffic. Combined with in-memory execution and COM hijacking, this significantly hindered detection efforts. Ukrainian authorities have underscored this as part of a broader strategy wherein Russian APTs, particularly APT28, pilot advanced cyberespionage techniques against Ukraine before potentially applying them elsewhere.

# Recommendations

**Restrict Macro Execution:** Disable or limit the use of Office macros, especially in documents from external sources. Use Group Policy or Office Trust Center settings to block macro-enabled documents by default.

**Monitor for COM Hijacking:** Audit registry keys commonly used for COM object hijacking (e.g., HKCU\Software\Classes\CLSID). Watch for DLLs loaded via non-standard COM paths, particularly under user-specific registry hives.

**Enable Endpoint Protection and EDR/XDR Tools:** Deploy modern Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions. Ensure they are configured to detect script-based threats, registry modifications, privilege escalation, and persistence mechanisms.

**Detect Abuse of Legitimate Cloud Services:** Monitor outbound traffic to cloud platforms like Koofr and Icedrive, especially from systems that do not routinely use them. Use proxy or firewall rules to block access to unnecessary cloud storage services.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0003<br>Persistence | TA0001<br>Initial Access | TA0002<br>Execution | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0010<br>Exfiltration | TA0011<br>Command and Control | TA0040<br>Impact |
| TA0007<br>Discovery | T1546<br>Event Triggered Execution | T1564<br>Hide Artifacts | T1059.005<br>Visual Basic |
| T1567.002<br>Exfiltration to Cloud Storage | T1567<br>Exfiltration Over Web Service | T1041<br>Exfiltration Over C2 Channel | T1546.015<br>Component Object Model Hijacking |

| | | | |
|---|---|---|---|
| T1566.003<br>Spearphishing via Service | T1566<br>Phishing | T1204<br>User Execution | T1059.001<br>PowerShell |
| T1059<br>Command and Scripting Interpreter | T1574.001<br>DLL | T1204.002<br>Malicious File | T1574<br>Hijack Execution Flow |
| T1053.005<br>Scheduled Task | T1218<br>System Binary Proxy Execution | T1562<br>Impair Defenses | T1053<br>Scheduled Task/Job |
| T1071.001<br>Web Protocols | T1071<br>Application Layer Protocol | T1573<br>Encrypted Channel | T1027<br>Obfuscated Files or Information |
| T1021<br>Remote Services | T1003<br>OS Credential Dumping | T1036<br>Masquerading | T1102<br>Web Service |
| T1082<br>System Information Discovery | T1113<br>Screen Capture | | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | 915179579ab7dc358c41ea99e4fcab52, 2cae8dc37baf5216a3e7342aac755894, b52c71318815836126f1257a180a74e7, 5171e84d59fd2bbef9235dfa6459ad8a, 99f2fd309b88b8ec3a9c9c50dddb08b5, bd76f54d26bf00686da42f3664e3f2ae, b859f38bfa8bba05d7c0eb4207b95037, b6e3894c17fb05db754a61ac9a0e5925, d802290cb9e5c3fed1ba1a8daf827882, 8e0143a6fd791c859d79445768af44d1, 5d938b4316421a2caf7e2e0121b36459, 889b83d375a0fb00670af5276816080e |

| TYPE | VALUE |
| --- | --- |
| SHA256 | c49d4acad68955692c32d5fa924eb5bb3f95a192d2c70ff6b0b2ce63c6afe985, be588c14f7ed3252e36c7db623c09cde8e01fa850c5431d9d621ac942695804d, 0a0fefb509a85c069539003c03c4f9c292d415fb27d18aef750446b63533b432, 84e9eb9615f16316adac6c261fe427905bf1a3d36161e2e4f7658cd177a2c460, 296b294a5fed830c2ff1fac9cb361a2d665b70f2f37188b593b5d1401cd6ca28, 225b7abe861375141f6cfebde4981f615cb2aa4d913faf85172666fa4b4b320b, d1deeaf0f1807720b11d0f235e3c134a1384054e4c3700eabab26b3a39d2c19a, 20987f7163c8fe466930ece075cd051273530dfcbe8893600fd21fcfb58b5b08, 88e28107fbf171fdbcf4abbc0c731295549923e82ce19d5b6f6fefa3c9f497c9, 39c1f38d0bdc70e50588964ccf3e63dabb871dca83392305a0c64144c7860155, 2eabe990f91bfc480c09db02a4de43116b40da2d6eaad00a034adf4214dac4d1, 9faeb1c8a4b9827f025a63c086d87c409a369825428634b2b01314460a332c6c |
| File Name | tcpiphlpsvc.dll, eapphost.dll, Act.doc, ctec.dll, windows.png, ksmqsyck.dx4.exe, PlaySndSrv.dll, sample-03.wav, BeardShell.dll, tmsnrb41da2y867.tmp, cache_ertf5gw56jikh5dwe, WordIllustration.png |
| File Path | %APPDATA%\microsoft\protect\ctec.dll, %LOCALAPPDATA%\Packages\PlaySndSrv.dll, %LOCALAPPDATA%\windows.png, %TEMP%\cache_d3qf5gw56jikh5tb6, %TEMP%\io1snrb41da2gn5.tmp, %USERPROFILE%\Music\Samples\sample-03.wav, %TEMP%\cache_ertf5gw56jikh5dwe, %PUBLIC%\Pictures\WordIllustration.png, |

| TYPE | VALUE |
| --- | --- |
| File Path | HKEY_CURRENT_USER\Software\Classes\CLSID\{2227A280-3AEA-1069-A2DE-08002B30309D}\InProcServer32, HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InProcServer32, Microsoft\Windows\Multimedia\SystemSoundsService, C:\Windows\System32\tcpiphlpsvc.dll, C:\Windows\System32\wbem\eapphost.dll |
| Host Name | Api[.]icedrive[.]net, App[.]koofr[.]net |
| Domains | icedrive[.]net, koofr[.]net |
| URLs | hxxps[://]api.icedrive[.]net, hxxps[://]app.koofr[.]net |

# References

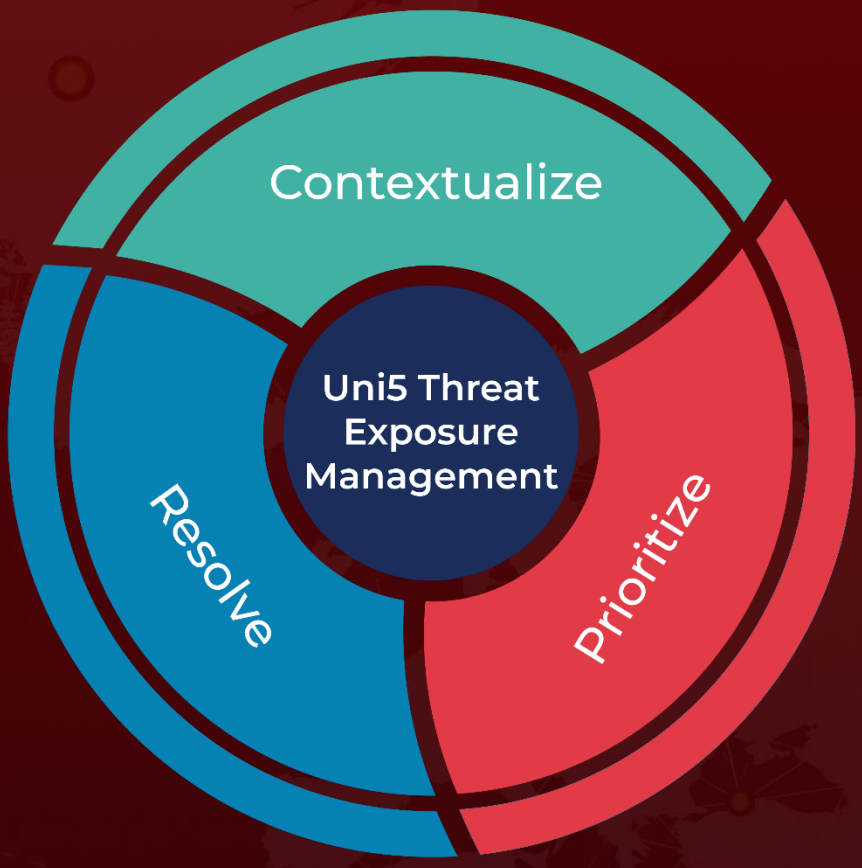

https://cert.gov.ua/article/6284080

https://hivepro.com/threat-advisory/operation-roundpress-apt28s-webmail-espionage-exposed/

# 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

**June 25, 2025 • 11:30 PM**



More at www.hivepro.com