



THREAT ADVISORY

APT28 CONTINUED TRADECRAFT RESILIENCE

October 28, 2026

TLP:GREEN



UltraViolet Cyber TIDE Team
tide@uvcyber.com



LATEST APT28 OPERATIONS HIGHLIGHT CONTINUED TRADECRAFT RESILIENCE

October 28, 2026

TLP:GREEN

UltraViolet Cyber TIDE Team, tide@uvcyber.com

Executive Snapshot

Recent public reporting has linked APT28 (also known as Fancy Bear, Forest Blizzard, Fighting Ursa, Pawn Storm, and more) to attacks against law enforcement, shipbuilders, and aircraft engine manufacturers in at least two NATO states. In at least one attack, APT28 deployed the HOOKEDGE backdoor to maintain access for at least two months, a short duration by their standards but still ample time for successful espionage operations.

These recently published findings on APT28 operations are undoubtedly interesting and significant on their own. But long-term analysis of the GRU-attributed group highlights a notable pattern in these operations: an exceptionally well-resourced, highly sophisticated actor that is both successful in making mundane techniques work and resistant to sweeping operational change. Given APT28's large, diverse pool of historic target industries, these patterns are important for almost all critical infrastructure and government-related organizations, particularly those based in NATO or NATO-aligned states.

- **Continued abuse of legitimate platforms:** APT28 has abused legitimate platforms such as Mocky, MockBin, InfinityFree, and Webhook to host malicious files and command-and-control traffic since at least early 2023. Recent reporting indicates they are continuing to engage in this technique.
- **Persisting use of macros and maldocs:** APT28 continues to rely on macro-enabled malicious documents (maldocs) for initial access, accounting for roughly one in five of its reported intrusions since 2025, a share well above the broader threat landscape.
- **HEADLACE evolves to HOOKEDGE:** The newly reported HOOKEDGE backdoor shares significant code and behavior with HEADLACE, a malware family APT28 has used since April 2023. This highlights a wider pattern of continued use of the same or similar malware.
- **Why it matters:** APT28 sticks with tools and techniques that are working, doing so for long periods of time and in the face of heavy public reporting. Organizations should expect to keep seeing the same tactics rather than a shift to new ones.



TIDE Team Analysis

ADVERSARY PROFILE

APT28

Fancy Bear, Forest Blizzard, Fighting Ursa

ALSO

Sednit, Strontium, Pawn Storm, GRU Unit 26165, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, FROZENLAKE, and GruesomeLarch

ACTIVE SINCE

2004 (22+ years)

ATTRIBUTION

Russia, General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center, Military Unit 26165

MOTIVES

Espionage, Influence, Disruption

INDUSTRIES

Aerospace, Aviation & Air Transport, Critical Infrastructure (General), Defense & Defense Industrial Base, Diplomatic & Foreign Affairs, Government, International & Multilateral Organizations, Maritime & Sea Transport, Media & Journalism, Military, Politics & Political Organizations, Sports Organizations, and Think Tanks & Policy Organizations.

COUNTRIES

Australia, Canada, Czech Republic, France, Germany, Netherlands, Norway, Poland, Ukraine, United Kingdom, and United States.

NOTABLE TTPs

1. Spearphishing (T1566.001, T1566.002) exploiting CVE-2026-21509 to deploy MiniDoor and PixyNetLoader.
2. Password spraying and forced authentication (T1110.003, T1187) to capture credentials, including NTLM hashes.
3. System firmware implant (T1542.001) for a persistent foothold that survives OS reinstallation.
4. Rootkits, masquerading, and file deletion (T1014, T1036, T1070.004) tied to its Sednit/X-Agent toolset.
5. Infrastructure acquisition and network device compromise (T1583.001, T1584.008) using compromised home/SOHO routers.
6. Command and control over web protocols and proxies (T1071.001, T1090.003, T1102, T1105), via compromised routers.
7. Local, automated, and remote email collection (T1005, T1119, T1114.002), central to its mailbox-theft operations.

Legitimate Sites, Bad Intentions

These recent attacks highlight one of APT28's more intriguing techniques: their longstanding abuse of legitimate sites like Mocky, MockBin, InfinityFree, and Webhook. They have incorporated these sites in their operations since at least early 2023, frequently turning them into maldoc hosting sites or credential harvesting pages, though they have also used them for command and control (C2) and exfiltration. What makes APT28's abuse of these sites tricky for defenders is the legitimate nature of the sites. Unless they lack any reasonable business use case, it's not feasible for organizations to completely block access to these sites. By staging malicious files or C2 traffic on these sites, APT28 can effectively direct targets to legitimate services and blend in with legitimate traffic. Think of it as a maldoc hosted on Google Drive: hosting on a legitimate service as opposed to an unknown website adds a sense of legitimacy for the target users. And given APT28's abuse of these services for over three-and-a-half years, we can infer that the technique has been successful.



Never-Ending Lure Documents

This is where “making mundane techniques work” comes into play. In 2026, threat actors have increasingly moved towards quieter, identity-based initial access techniques. APT28, however, continues to make use of lure documents that rely on malicious macros to progress the infection. This certainly goes against the increasingly popular phrase, “attackers aren’t breaking in, they’re logging in.” And while that is obviously not an all-encompassing sentiment, APT28’s persisting use of this technique is noteworthy, not because they are using it, but because they’ve been using it for years. Their use of this technique spans more than a decade, to at least 2014, and it has continued even after Microsoft began blocking macros by default in 2022.

An analysis of open-source intelligence suggests APT28 has relied on the maldoc technique in about 20 percent of reported intrusions since 2025, including this newly reported activity. They have made some adaptations to align with the new macro landscape (for example, the macros are often minimized to serve as a simple launch point while evading sandboxes and EDR agents), but they continue to leverage maldocs nonetheless. This is significantly more than the wider threat landscape: maldocs with embedded macros appear to have accounted for less than 5% of reported initial access attempts during the same timeframe. Similar to their continued use of legitimate sites, this implies continued success in achieving initial access and progressing in to subsequent stages of infections while using this technique.

The Same Malware...For Years

Per recent reporting, APT28 has deployed the HOOKEDGE backdoor in support of their recent operations. HOOKEDGE is a novel malware that was first reported in August 2026 as part of the uncovering of an espionage campaign that ran from September 2025 through April 2026. Interestingly, HOOKEDGE is reported to share significant code and behavioral overlap with HEADLACE, an infamous backdoor that APT28 first debuted in April 2023. This is an important note, as HEADLACE was one of the longest tenured malware families in APT28’s arsenal. Their pivot to a modularly similar malware is indicative of small tweaks to enhance and modernize the tool rather than a hard turn away from it.

Malware is perhaps the riskiest element to resist change to, as recurring public analysis, in theory, makes life easier for defenders and defense tools alike. Yet APT28 continues to favor some malware families for years and only make minor tweaks to them, as evidenced by the HEADLACE to HOOKEDGE evolution. Similar to the previous two points, this is another long-term pattern in APT28 operations: they will continue to deploy the same malware family for long periods of time, sometimes years, if their operations continue to succeed.

Why It Matters

The repeating nature of these trends suggests a few things. First, these techniques have been successful for APT28, or at least successful enough to persist in their arsenal for the last several years. And second, and perhaps more importantly for the long-term outlook, that APT28 will stick with tradecraft and malware, even in the face of heavy reporting and analysis, so long as it continues to bring them success. This goes against what we would typically expect to see from threat actors, as many are known to pivot malware and, with time, techniques following heavy public analysis. There are a few exceptions, of course, but most threat actors, particularly state-sponsored espionage actors who are very well-resourced, will rotate malware with some degree of regularity to help mask attribution and analysis.



The latter point also tells us that APT28 prioritizes operational success a substantial degree more than they prioritize avoiding attribution. This may come across as a little brazen, and possibly counterintuitive for an espionage-centric group, but the approach seems to be working. Minimal changes to their tools and techniques over a multi-year time period would most likely be an indicator of one of two things: a lack of resources (which is almost certainly not an issue for the GRU), or significant success with their tradecraft. And while the frequent reporting on APT28 tells us that they are regularly being identified, it also tells us that their operational tempo is extremely high.

Separately, although not to be overlooked, this activity also highlights APT28's continued targeting of maritime and maritime-adjacent organizations. A May 2025 Joint Cybersecurity Advisory implicated the group in espionage attacks against maritime, shipping, and transportation organizations with the purpose of acquiring schedules and manifests related to Ukraine-bound shipments. Their more recent attacks included at least one similar victim in a naval shipbuilding organization. While maritime and maritime-related organizations have not historically been thought of as primary targets for APT28 activity, this continuing activity suggests this mentality is outdated. With this in mind, maritime organizations (particularly those in NATO and NATO-aligned states) should take extra precautions and preventative measures, some of which are outlined below, to harden their environments, identify APT28 intrusions, and respond effectively.

Looking ahead, this pattern points to specific expectations rather than generic risk. In the near term, APT28 will most likely continue reusing its current playbook, including maldocs, legitimate-site abuse, and the HOOKEDGE backdoor, against the same industries and the broader population of NATO and NATO-aligned logistics, defense, and government targets tied to continued support for Ukraine. Long-term, expect APT28 to keep relying on the same core playbook and incrementally updated malware like HOOKEDGE for the foreseeable future. It's worth noting that this applies to their activity across the board, not just the trends brought to light in these recent attacks. Nothing in their track record suggests public exposure alone is enough to force a change, and the group has absorbed years of reporting on each of these techniques without abandoning them.

How to Respond

- ☐ Disable Office macros from internet-sourced documents wherever business operations allow it, and avoid carving out broad exceptions for legacy workflows that reintroduce the exposure Microsoft's default blocking was designed to close.
- ☐ If possible, restrict access to webhook-relay and request-inspection services such as webhook.site, Mocky, MockBin, and InfinityFree to known developer or business use cases rather than permitting them organization-wide, since APT28 relies on their legitimate reputation to blend in with normal traffic.
- ☐ Watch for browsers launched in headless or hidden-window modes that are communicating with external infrastructure, and for scheduled tasks that execute scripts from user-writable folders such as %userprofile% or %appdata%, particularly when the filenames are randomized.
- ☐ Disable NTLM authentication where feasible, enforce SMB signing, and monitor for forced-authentication attempts that coerce internal systems into connecting to attacker-controlled resources.
- ☐ Treat routers and other network edge devices connected to the corporate environment as part of the attack surface. Keep their firmware current, verify its integrity where tooling allows, and replace end-of-life hardware that can no longer receive security updates.



- ☐ Apply security patches for Microsoft Office and other frequently targeted software as soon as they are available, and track vendor advisories for actively exploited vulnerabilities rather than waiting for a scheduled patch cycle.
- ☐ Perform annual tech refresh reviews to gain a holistic understanding of your infrastructure. Speak with your UltraViolet Cyber TAM Representative to schedule a [Red Team](#) or [Purple Team](#) engagement to gain insight into the vulnerabilities in your environment.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity. UltraViolet is also maximizing detection coverage proactively through [Equinox](#).
- Tracking the latest threat actor intelligence, as well as the corresponding impact on industries around the world, through TIDE's Adversary Intelligence platform.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | [in](#) UltraViolet Cyber | [X](#) @uv_cyber