TURLA

[/ ˈtʊər.lə /]

Turla is one of the most enduring Russia-linked APT groups, attributed to the FSB and active since the early 2000s. Specializing in long-term, stealthy espionage, it targets governments, military bodies, and diplomatic missions across Europe and NATO member states. Over two decades, the group has evolved from simple rootkits into a sophisticated modular framework — and remains actively operational through 2024–2025.

IDENTITY

Attribution	: Russia-linked APT group, associated with Russian intelligence services (FSB).
Active Since	: Early 2000s.
Aliases	: Snake, Uroburos, ATK13, Group 88, Waterbug, IRON HUNTER, Secret Blizzard, UNC4210, ITG12, TAG_0530, VENOMOUS Bear, UAC-0003, UAC-0024, UAC-0144, Pacifier APT, G0010, Blue Python, Hippo Team, KRYPTON, MAKERSMARK, Pfinet, Popeye, SIG23, SUMMIT, WRAITH.
Motivation	: State-aligned espionage, cyber operations supporting Russian geopolitical and military goals.

TTPs

Initial Access	: Spear-phishing campaigns, watering-hole attacks, supply chain intrusions, exploitation of VPN and server vulnerabilities.
Persistence	: Custom rootkits (Snake/Uroburos), registry modifications, scheduled tasks, long-lived implants.
Command & Control (C2)	: Satellite-based C2 channels, multi-hop proxy chains, compromised infrastructure, encrypted HTTPS communication.
Tools & Malware	- Snake/Uroburos rootkit – flagship modular backdoor with stealth and persistence - Carbon – modular espionage framework - Kazuar – backdoor with .NET components - Epic Turla – first-stage reconnaissance toolkit - Gazer/Pfinet – second-stage malware for espionage
Techniques	- Living-off-the-land binaries (LOLbins) for stealth - Credential theft and privilege escalation - Long-term persistence through rootkits and stealthy backdoors - Supply chain and watering-hole compromises to reach sensitive targets

TARGET PROFILE

Target Sectors	: Government ministries, military and defense contractors, diplomatic missions, critical infrastructure, technology & research institutions.
Geographies Targeted	: Primarily Europe and NATO countries; also Middle East, Central Asia, North America.

THREAT ASSESSMENT

Risk Level	: Very High – highly sophisticated, stealthy, and enduring APT actor.
Most Recent Activity	: 2024–2025 campaigns deploying updated Snake malware against European ministries and NATO-related organizations.
Evolution	: From early custom rootkits and backdoors (Uroburos, Carbon, Epic Turla) to highly modular espionage frameworks with satellite-based C2 and advanced evasion.

NOTABLE OPERATIONS

- **2008–2014:** Deployment of Snake/Uroburos against European government targets; development of satellite-based C2.
- **2015–2017:** Epic Turla and Carbon used in espionage against diplomatic and military organizations in Europe.
- **2018–2020:** Targeted Middle Eastern and Central Asian governments; Kazuar backdoor linked to SolarWinds-related activity.
- **2021–2023:** Expanded campaigns against NATO, Eastern European defense, and diplomatic targets.
- **2024–2025:** Upgraded Snake and Kazuar variants deployed in Europe, exploiting VPN vulnerabilities and using sophisticated proxy chains.