VOODOO BEAR | Threat Actor Profile | CrowdStrike

By AdamM

Archived: 2026-04-05 22:22:14 UTC

For the past several years, CrowdStrike® has published a yearly calendar that includes international holidays, working days of the most prevalent threat actors, and significant geopolitical events. Every month features the rendering of a threat actor, based on dossiers compiled by CrowdStrike Falcon® Intelligence™ analysts about each actor's behaviors and targets. This year we are going to be releasing a monthly blog post introducing the "Threat Actor of the Month," complete with detailed background information on that actor. January 2018 features a Russia-based actor we call VOODOO BEAR. This actor is **also known as Sandworm Team, and BlackEnergy APT Group**.

Voodoo Bear's Methods

VOODOO BEAR is a highly advanced adversary with a suspected nexus to the Russian Federation. This adversary has been identified **leveraging custom-developed plugins for versions 2 and 3 of the commodity malware *Black Energy* to target entities associated with energy, industrial control systems and SCADA, government, and media for espionage and destructive purposes, since at least 2011.** Some tools used by this actor — specifically BlackEnergy and GCat — have been adapted from commodity malware. Destructive malware used by VOODOO BEAR includes a wiper called PassKillDisk. A commonly observed element of implants from VOODOO BEAR — at least until this information was made public in late 2014

— were references in the malware to the 1965 science fiction novel *Dune*, by Frank Herbert.

Voodoo Bear's Targets

This adversary displays a particular focus on **targeting entities in the Ukraine** and is believed to be behind the Ukrainian energy sector attacks that caused widespread power outages in late 2015. The use of zero-day exploits, custom-developed plugins for the Black Energy implant, and the propensity to target entities involved in energy and critical infrastructure for espionage and destructive purposes — these characteristics all highlight the likelihood that VOODOO BEAR operates in alignment with Russian state interests. VOODOO BEAR appears to be integrated into an organization that also operates or tasks multiple pro-Russian hacktivist entities. VOODOO BEAR's known operations are consistent with an entity operating in support of Russian economic and national objectives through targeted espionage and sabotage operations.

Other Known Russia-Based Adversaries

- Fancy Bear
- Cozy Bear
- Venomous Bear

Curious about other nation-state adversaries? *Visit our [threat actor center] to learn about the new adversaries that the CrowdStrike team discovers.*

Learn More

- To learn more about how to incorporate intelligence on threat actors like VOODOO BEAR please visit the Falcon Intelligence product page.
- **Want the insights on the latest adversary tactics, techniques, and procedures (TTPs)?** Download the *CrowdStrike 2020 Global Threat Report*
