GHOST WRITER

[/ ˈgoʊstˌraɪ.tər /]

Ghostwriter is a Belarus-aligned, Russia-linked APT active since 2016, conducting high-risk cyber-espionage and disinformation campaigns. It targets government, military, media, NGOs, and election infrastructure in Eastern Europe, NATO, and EU states, blending influence operations with credential theft and phishing.

IDENTITY

Attribution	: Belarus-aligned APT with strong ties to Russia; widely linked to the Belarusian military intelligence agency (GSSD).
Active Since	: At least 2016, with a sharp increase in operations from 2020 onward.
Aliases	: TA445, DEV-0257, Storm-0257, UNC1151, UAC-0057, PUSHCHA.
Motivation	: Political and military influence operations - blending disinformation, cyber-espionage, and credential theft to advance Belarusian and Russian strategic interests.

TTPs

Initial Access	: Spear-phishing campaigns delivering malicious attachments or credential-harvesting links; exploitation of website CMS vulnerabilities.
Persistence	: Use of compromised email accounts, fake personas on social media, and long-term access via stolen credentials.
Command & Control (C2)	: Relies on compromised infrastructure and hijacked websites for C2 traffic.
Malware & Tools	: Credential harvesters, backdoors, infostealers; use of publicly available tools alongside custom scripts.
Techniques	: Coordinated influence operations (fake news sites, social media manipulation) combined with espionage (credential theft, lateral movement).

TARGET PROFILE

Target Sectors	: Government, military, media, NGOs, and election infrastructure.
Geographies Targeted	: Primarily Eastern Europe - Ukraine, Poland, and the Baltic states - with expanded campaigns targeting NATO and EU institutions.

THREAT ASSESSMENT

Risk Level	: High – Ghostwriter's combination of influence operations and espionage makes it a dual-threat actor.
Most Recent Activity	: Active through 2024–2025, running phishing campaigns and information operations in support of Russian activities in Ukraine.
Evolution	: Initially focused on disinformation (fake news, propaganda), Ghostwriter has evolved into a hybrid actor combining influence with direct cyber-espionage.

NOTABLE OPERATIONS

- **2016–2019:** Early influence campaigns using fake news websites targeting NATO's credibility in Eastern Europe.
- **2020:** High-profile phishing and disinformation targeting Polish officials, NATO forces, and the Baltic states.
- **2021:** Combined credential theft and disinformation operations against journalists and government institutions in Eastern Europe.
- **2022:** Increased operational tempo during Russia's invasion of Ukraine, supporting pro-Russian narratives and targeting Ukrainian and NATO-linked entities.
- **2023:** Expanded targeting of European election infrastructure and political organizations with phishing and propaganda campaigns.
- **2024–2025:** Ongoing hybrid campaigns - credential theft against NATO officials, disinformation in EU states, and coordinated narratives to weaken Western support for Ukraine.