Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Ghostwriter

Names	Operation Ghostwriter *(FireEye)* UNC1151 *(FireEye)* TA445 *(Proofpoint)* UAC-0051 *(CERT-UA)* UAC-0057 *(CERT-UA)* PUSHCHA *(Google)* DEV-0257 *(Microsoft)* Storm-0257 *(Microsoft)* White Lynx *(Palo Alto)*
Country	Belarus
Sponsor	State-sponsored
Motivation	Information theft and espionage, Sabotage and destruction
First seen	2017
Description	(FireEye) Mandiant Threat Intelligence has tied together several information operations that we assess with moderate confidence comprise part of a broader influence campaign—ongoing since at least March 2017—aligned with Russian security interests. The operations have primarily targeted audiences in Lithuania, Latvia, and Poland with narratives critical of the North Atlantic Treaty Organization's (NATO) presence in Eastern Europe, occasionally leveraging other themes such as anti-U.S. and COVID-19-related narratives as part of this broader anti-NATO agenda. We have dubbed this campaign "Ghostwriter." Many, though not all of the incidents we suspect to be part of the Ghostwriter campaign, appear to have leveraged website compromises or spoofed email accounts to disseminate fabricated content, including falsified news articles, quotes, correspondence and other documents designed to appear as coming from military officials and political figures in the target countries.
Observed	Sectors: Defense, Education, Government, Media. Countries: Belarus, Colombia, Estonia, France, Germany, Ireland, Kuwait, Latvia,

	Lithuania, Poland, Switzerland, Ukraine.	
Tools used	Cobalt Strike, HALFSHELL, Impacket, RADIOSTAR, VIDEOKILLER.	
Operations performed	2021	Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity <https://content.fireeye.com/web-assets/rpt-unc1151-ghostwriter-update>
	Mar 2021	German Parliament targeted again by Russian state hackers <https://www.bleepingcomputer.com/news/security/german-parliament-targeted-again-by-russian-state-hackers/>
	Jan 2022	Ukraine suspects group linked to Belarus intelligence over cyberattack <https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/>
	Feb 2022	Ukraine links Belarusian hackers to phishing targeting its military <https://www.bleepingcomputer.com/news/security/ukraine-links-belarusian-hackers-to-phishing-targeting-its-military/>
	Feb 2022	In the past several days, we've seen increased targeting of people in Ukraine, including Ukrainian military and public figures <https://about.fb.com/news/2022/02/security-updates-ukraine/>
	Feb 2022	Operation "Asylum Ambuscade" State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement <https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails> <https://www.welivesecurity.com/2023/06/08/asylum-ambuscade-crimeware-or-cyberespionage/>
	Feb 2022	Ghostwriter/UNC1151, a Belarusian threat actor, has conducted credential phishing campaigns over the past week against Polish and Ukrainian government and military organizations. <https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/>
	Mar 2022	GhostWriter APT targets state entities of Ukraine with Cobalt Strike Beacon <https://securityaffairs.co/wordpress/129527/apt/ghostwriter-apt-targets-state-entities-of-ukraine-with-cobalt-strike-beacon.html>

	Mar 2022	Ghostwriter, a Belarusian threat actor, recently introduced a new capability into their credential phishing campaigns. In mid-March, a security researcher released a blog post detailing a 'Browser in the Browser' phishing technique. <https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/>
	Apr 2022	Ghostwriter, a Belarusian threat actor, has remained active during the course of the war and recently resumed targeting of Gmail accounts via credential phishing. <https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/>
	Apr 2022	Malicious campaigns target government, military and civilian entities in Ukraine, Poland <https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/>
	Apr 2024	UNC1151 Strikes Again: Unveiling Their Tactics Against Ukraine’s Ministry of Defence <https://cyble.com/blog/unc1151-strikes-again-unveiling-their-tactics-against-ukraines-ministry-of-defence/>
	Jan 2025	Ghostwriter | New Campaign Targets Ukrainian Government and Belarusian Opposition <https://www.sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/>
Counter operations	Early 2022	We’ve seen a further spike in compromise attempts aimed at members of the Ukrainian military by Ghostwriter, a threat actor tracked by the security community. <https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf>
Information	<https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf> <https://www.prevailion.com/diving-deep-into-unc1151s-infrastructure-ghostwriter-and-beyond/> <https://www.mandiant.com/resources/unc1151-linked-to-belarus-government> <https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf> <https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/>	

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format
