SaintBear, Lorec53 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:16:16 UTC

APT group: SaintBear, Lorec53

Names	SaintBear *(ThreatBook)* Ember Bear *(CrowdStrike)* TA471 *(Proofpoint)* UNC2589 *(FireEye)* Lorec53 *(NSFOCUS)* UAC-0056 *(CERT-UA)* Nodaria *(Symantec)* FROZENVISTA *(Google)* Storm-0587 *(Microsoft)* Nascent Ursa *(Palo Alto)* G1003 *(MITRE)*
Country	Russia
Motivation	Information theft and espionage
First seen	2021
Description	(NSFOCUS) In July 2021, several phishing documents created in Georgian were discovered by NSFOCUS Security Labs. In these phishing documents, the attackers used current political hotspots in Georgia to create bait and deliver a secret stealing Trojan to specifically targeted victims aiming to steal various documents from their computers. Correlation analysis shows that this phishing campaign and an earlier phishing attack against the Ukrainian government came from the same unknown threat entity, most likely composed of Russian hackers. From April to July of 2021, the group launched several phishing attacks applying a large number of network resources located in Russia. In order to facilitate ongoing tracking, NSFOCUS Security Labs has tentatively dubbed the hacker group Lorec53 by extracting special names from related Trojans.
Observed	Sectors: Energy, Financial, Government, Media, Transportation. Countries: Georgia, Ukraine, USA.

Tools used	Cobalt Strike, Graphiron, GraphSteel, GrimPlant, OutSteel, SaintBot.	
Operations performed	Feb 2022	Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot <https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/>
	Mar 2022	Ukraine's CERT Warns Threat Actors For Fake AV Updates <https://www.socinvestigation.com/ukraines-cert-warns-russian-threat-actors-for-fake-av-updates/>
	Mar 2022	Cobalt Strikes again: UAC-0056 continues to target Ukraine in its latest campaign <https://blog.malwarebytes.com/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign/>
	Oct 2022	Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer>
Information	<https://nsfocusglobal.com/apt-retrospection-lorec53-an-active-russian-hack-group-launched-phishing-attacks-against-georgian-government/> <https://www.crowdstrike.com/blog/who-is-ember-bear/> <https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G1003/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=nascentursa>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
