Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:30:41 UTC

APT group: NB65

Names	NB65 *(self given)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2022	
Description	(BleepingComputer) A hacking group used the Conti's (Wizard Spider, Gold Blackburn) leaked ransomware source code to create their own ransomware to use in cyberattacks against Russian organizations. While it is common to hear of ransomware attacks targeting companies and encrypting data, we rarely hear about Russian organizations getting attacked similarly. This lack of attacks is due to the general belief by Russian hackers that if they do not attack Russian interests, then the country's law enforcement would turn a blind eye toward attacks on other countries. However, the tables have now turned, with a hacking group known as NB65 now targeting Russian organizations with ransomware attacks.	
Observed	Countries: Russia.	
Tools used	NB65.	
Operations performed	Apr 2022	The Russian entities claimed to have been attacked by the hacking group include document management operator Tensor, Russian space agency Roscosmos, and VGTRK, the state-owned Russian Television and Radio broadcaster <https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/>
Information	<https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/>	

Last change to this card: 30 June 2025

Download this actor card in PDF or JSON format
