Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:02:50 UTC

APT group: OldGremlin

Names	OldGremlin *(Group-IB)*	
Country	Russia	
Motivation	Financial crime, Financial gain	
First seen	2020	
Description	(Group-IB) Group-IB Threat Intelligence team recently tracked a successful attack conducted on a Russian medical company by OldGremlin, a new criminal group. The threat actor encrypted the company's entire corporate network and demanded a $50,000 ransom. It is common knowledge that Russian hackers have an unspoken rule about not working within Russia and post-Soviet countries. Yet OldGremlin, made up of Russian speakers, is actively attacking Russian companies: banks, industrial enterprises, medical organizations, software developers… According to Group-IB expert estimations, since the spring OldGremlin has conducted at least seven phishing campaigns. The hackers have impersonated the self-regulatory organization Mikrofinansirovaniye i Razvitiye (SRO MiR); a Russian metallurgical holding company; the Belarusian plant Minsk Tractor Works; a dental clinic; and the media holding company RBC.	
Observed	Sectors: Financial, Healthcare, Media. Countries: Russia.	
Tools used	Cobalt Strike, TinyCryptor, TinyNode, TinyPosh.	
Operations performed	Feb 2021	Old Gremlins, new methods <https://blog.group-ib.com/oldgremlin_comeback>
Information	<https://www.group-ib.com/blog/oldgremlin> <https://www.group-ib.com/media-center/press-releases/oldgremlin-2022/>	

Last change to this card: 18 November 2022

Download this actor card in PDF or JSON format