# Big Game Hunting comes to Big Country: Group-IB detects series of ransomware attacks by OldGremlin

September 23, 2020 · 6 min to read

Managed XDR | OldGremlin | Oleg Skulkin | Threat Intelligence

Group-IB, a global threat hunting and intelligence company headquartered in Singapore, has detected a successful attack by a ransomware gang, codenamed OldGremlin. The Russian-speaking threat actors are relatively new to the Big Game Hunting. Since March, the attackers have been trying to conduct multistage attacks on large corporate networks of medical labs, banks, manufacturers, and software developers in Russia. The operators use a suite of custom tools with the ultimate goal of encrypting files in the infected system and holding it for a ransom of about $50,000.

The first successful attack of OldGremlin, known to Group-IB team, has been detected in August. Group-IB Threat Intelligence team has also collected evidence of earlier campaigns dating back to the spring of this year. The group has targeted only Russian companies so far, which was typical for many Russian-speaking adversaries, such as Silence and Cobalt, at the beginning of their criminal path. Using Russia as a testing ground, these groups then switched to other geographies to distance themselves from vicious actions of the victim country's police and decrease the chances of ending behind the bars.

# Unsought invoice

As the initial vector of their attacks, OldGremlin use spearphishing emails, to which the group adopted creative approach. They, in particular, utilized the names of actually existing senders and, in one instance, sent out emails in several stages, making the victims think that they are arranging an interview with a journalist of a popular Russian business newspaper. In other instances, the gang exploited the COVID-19 theme and anti-government rallies in Belarus in their phishing emails.

The most recent successful attack, known to Group-IB Threat Intelligence team, took place in August when OldGremlin targeted a clinical diagnostics laboratory operating throughout the country. The analysis of the incident revealed that the ransomware attack started with a phishing email sent on behalf of Russia's major media holding company, with the «Invoice» subject. In their email, OldGremlin informed the recipient of their inability to contact the victim's colleague highlighting the urgency to pay the bill, the link to which was included in the text body. By clicking the link, the victim downloaded a ZIP-archive that contained a unique custom backdoor, dubbed TinyNode. The backdoor downloads and installs additional malware on the infected machine.

The cybercriminals then used the remote access to the victim's computer, obtained with the help of TinyNode, as a foothold for network reconnaissance, gathering data and lateral movement in the victim's network. As part of post-exploitation activities, OldGremlin used Cobalt Strike to move laterally and obtain authentication data of domain administrator.

Several weeks after the attack's launch, the cybercriminals deleted server backups before encrypting the victim's network with the help of TinyCryptor ransomware (aka decr1pt), which is also OldGremlin's brainchild. When the work of the company's regional branches had been paralyzed, they demanded about $50,000 in cryptocurrency. As a contact email, the threat actors gave an email registered with ProtonMail.



# Up-to-date phishing

Group-IB Threat Intelligence experts have also detected other phishing campaigns carried out by the group, with the first of them having occurred in late March — early April. Back then, the group sent out emails to financial organizations from an email that mimicked that of a Russian microfinance organization, providing the recipients with the guidelines on how to organize safe remote work during the COVID-19. It was the first time when OldGremlin used their other custom

backdoor — TinyPosh, which allows the attackers to download additional modules form their C2. To hide their C&C server, OldGremlin resorted to Cloudflare Workers server.

Two weeks after the above-mentioned malicious mailing, OldGremlin, keeping up with the urgent agenda, sent out emails with the subject «All-Russian study of the banking and financial sectors during the pandemic» purported to be from a real-life journalist with a major Russian media holding. The sender then asked for an online interview and schedule it with the Calendly and informed them that the questions for the interview had been uploaded to a cloud platform. As it was the case with their first campaigns, the link downloaded a custom TinyPosh Trojan.



Fig. 1 Phishing email sent on behalf of a Belarusian plant

Another round of phishing emails by OldGremlin was detected by CERT-GIB on August 19, when the group sent out messages exploiting the issue of protests in Belarus. The email that claimed to be from the CEO of the Minsk Tractor Works plant informed its partners of the fact that the enterprise was being probed by the country's prosecutor's office due to its participation in the anti-government protests and asked them to send missing documents. The list of the necessary documents was reportedly attached to the email, an attempt to download it, however, let TinyPosh into the user's computer. Between May and August, Group-IB detected nine campaigns conducted by the group.

**Oleg Skulkin**

Senior Digital Forensics analyst

**What distinguishes OldGremlin from other Russian-speaking threat actors is their fearlessness to work in Russia. This indicates that the attackers are either fine-tuning their techniques benefiting from home advantage before going global, as it was the case with Silence and Cobalt, or they are representatives of some of Russia's neighbors who have a strong command of Russian. Amid global tensions, cybercriminals have learned to navigate the**

**political agenda, which gives us grounds to suggest that the attackers might come from some of the post-Soviet countries Russia has controversy or weak ties with.**

Despite the vim, showed by ransomware operators recently, there is still a number of measures that can be taken to fight off ransomware attacks. They include, among others, using multifactor authentication, complex passwords for the accounts used for access via RDP and changing them regularly, restricting the list of IP addresses that can be used to make external RDP connections, and etc. Relevant threat intelligence and proactive approach to threat hunting are paramount in building resilient infrastructure. Implementing Group-IB Managed Extended Detection and Response (MXDR) allows to hunt for advanced on both network and host levels.



## Share article

# About Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its technological capabilities to defend businesses, citizens, and support law enforcement operations.

Group-IB's Digital Crime Resistance Centers (DCRCs) are located in the Middle East, Europe, Central Asia, and Asia-Pacific to help critically analyze and promptly mitigate regional and country-specific threats. These mission-critical units help Group-IB strengthen its contribution to global cybercrime prevention and continually expand its threat-hunting capabilities.

Group-IB's decentralized and autonomous operational structure helps it offer tailored, comprehensive support services with a high level of expertise. We map and mitigate adversaries' tactics in each region, delivering customized cybersecurity solutions tailored to risk profiles and requirements of various industries, including retail, healthcare, gambling, financial services, manufacturing, crypto, and more.

The company's global security leaders work in synergy with some of the industry's most advanced technologies to offer detection and response capabilities that eliminate cyber disruptions agilely.

**Group-IB's Unified Risk Platform (URP)** underpins its conviction to build a secure and trusted cyber environment by utilizing intelligence-driven technology and agile expertise that completely detects and defends against all nuances of digital crime. The platform proactively protects organizations' critical infrastructure from sophisticated attacks while continuously analyzing potentially dangerous behavior all over their network.

The comprehensive suite includes the world's most trusted Threat Intelligence, The most complete Fraud Protection, AI-powered Digital Risk Protection, Multi-layered protection with Managed Extended Detection and Response (XDR), All-infrastructure Business Email Protection, and External Attack Surface Management.

Furthermore, Group-IB's full-cycle incident response and investigation capabilities have consistently elevated industry standards. This includes the 77,000+ hours of cybersecurity incident response completed by our sector-leading DFIR Laboratory, more than 1,400 successful investigations completed by the High-Tech Crime Investigations Department, and round-the-clock efforts of CERT-GIB.

Time and again, its solutions and services have been revered by leading advisory and analyst agencies such as Aite Novarica, Gartner®, Forrester, Frost & Sullivan, KuppingerCole Analysts AG, and more.

Being an active partner in global investigations, Group-IB collaborates with international law enforcement organizations such as INTERPOL, EUROPOL and AFRIPOL to create a safer

cyberspace. Group-IB is also a member of the Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, which was created to foster closer cooperation between Europol and its leading non-law enforcement partners.

# Read next

March 19, 2026

**Group-IB Partners with Copy Cat Group to Strengthen Intelligence-Led Cybersecurity Across East Africa**

March 13, 2026

**Group-IB Supports INTERPOL's Operation Synergia III, Contributing Intelligence to Global Cybercrime Takedown**

March 12, 2026

**Group-IB Expands into the Americas with Launch of Digital Crime Resistance Center in Chile**

March 3, 2026

**Group-IB and Nebrija University Strengthen Cybersecurity Education Through MOU and Threat Intelligence Integration**

February 26, 2026

**Group-IB Partners with Savex Technologies to Advance Predictive Threat Intelligence and Cyber Fraud Protection Across India and SAARC**

February 16, 2026

**National Polytechnic University of Armenia and Group-IB sign strategic partnership to strengthen cybersecurity education and research in Armenia**

Go to all Press Releases →

MSSP and MDR Partner Program
Technology Partners
Partner Locator

Team
CERT-GIB
Careers
Internship
Academic Aliance
Sustainability
Media Center
Contact

**Subscription plans**

**Services**

**Resource Center**

## Contact

APAC: +65 3159 3798
EU & NA: +31 20 226 90 90
MEA: +971 4 568 1785

info@group-ib.com

## Subscribe to stay up to date with the latest cyber threat trends