Gremlins' prey, secrets, and dirty tricks: the ransomware gang OldGremlin set new records

Media Center → Press Releases

October 20, 2022 · 4 min to read

OldGremlin Phishing Ransomware Scam

Group-IB, one of the global leaders in cybersecurity, headquartered in Singapore, released a first threat report detailing the operations of a Russian-speaking ransomware group **OldGremlin**: **"OldGremlin Ransomware. Never ever feed them after the Locknight"**. According to Group-IB, in just two years and a half, the "Gremlins" carried out 16 malicious campaigns. OldGremlin remains one of the very few ransomware gangs targeting Russian companies. However, their growing ambitions can push them to explore new geographies in the future. For the second year in a row, OldGremlin demanded the highest ransom from Russian organizations: in 2021 their largest ransom demand amounted to $4.2 million, while in 2022 it soared to $16.9 million.

As usual, Group-IB's report provides access to a set of data and detailed information about the current tactics, techniques, and procedures (TTPs) used by the attackers, which are described using MITRE ATT&CK®. The information provided will benefit organizations that fight cybercrime, and especially heads of information security teams, SOC analysts, incident responders, and potential victims who can use the information to protect their infrastructure from OldGremlin.

Do not feed the Gremlins

Compared to other world regions, the post-Soviet space remained a harbor safe from ransomware groups primarily focusing on North America, Europe, Asia Pacific, and other locations. But this paradigm began to shift. According to Group-IB, last year, the number of ransomware attacks on Russian businesses increased by more than 200%. Among the most notorious ransomware gangs targeting this region was a group called OldGremlin.

OldGremlin (also known as TinyScouts) was uncovered by **Group-IB Threat Intelligence** team in March 2020 and was described in detail in September 2020 in the blog post "OldGremlin: secrets, and dirty tricks". According to Group-IB, in two and a half years OldGremlin carried out a total of 16 malicious email campaigns.

OldGremlin was most active in 2020. That year, the gang carried out ten campaigns, with emails purporting to be from microfinance companies, a metals and mining company, a tractor manufacturer, and a business media holding. In 2021, the group carried out a single but highly successful campaign: the threat actor impersonating an association of online retailers. In 2022, OldGremlin carried out five campaigns masquerading as tax and legal services companies, a payment system, an IT company, and more.

The group's victim list includes banks, logistics, and manufacturing companies, insurance firms, retailers, real estate developers, and software companies. In 2020, the group even targeted an arms manufacturer.

According to Group-IB, the average ransom demanded by OldGremlin amounts to $1.7 million, and the highest ransom to date reached $16.9 million. Unlike other ransomware operators involved in Big Game Hunting, OldGremlin tend to take long breaks after successful attacks

The craft of phishing

Like most ransomware groups, OldGremlin used phishing emails to gain initial access. The use of trending news topics (Covid-19, remote work, sanctions) together with well-crafted prepared emails presented masked as interview requests, commercial proposals, and financial documents helped the threat actors to trick the recipients into clicking on links and downloading malicious files. Due to the

massive scale of their email campaigns, the gang was able to compromise several working stations at once, which facilitated lateral movement within the victim's network.

Although OldGremlin mainly targets corporate **Windows**-based networks, the group's most recent attacks show that their arsenal includes dedicated ransomware for **Linux**. The threat actor is up to date on the latest trends in cybersecurity and successfully combines new methods with tried-and-tested tools such as Cobalt Strike and open-source frameworks (e.g., PowerSploit). One of the privilege escalation methods identified by Group-IB was the exploitation of Cisco AnyConnect vulnerabilities. To facilitate attacks, OldGremlin developed an entire Tiny framework and then improved it with each new campaign.

On average, the attackers spend **49 days** in the victim's network before deploying ransomware, which means that in addition to reactive methods of detecting traces of OldGremlin, proactive methods that help prevent the network from being infected by ransomware through email and other channels are also relevant.

The new report takes a deep dive into all 16 campaigns carried out by the group and includes the first description of OldGremlin's entire kill chain, from gaining initial access to encrypting data and demanding ransoms.

"OldGremlin has debunked the myth that ransomware groups are indifferent to Russian companies. According to our data, the gang's track record includes almost twenty attacks with multi-million ransom demands, with large companies becoming their preferred targets more often," says Ivan Pisarev, Head of Dynamic Malware Analysis Team at Group-IB. *"Despite the fact that OldGremlin has been focusing on Russia so far, they should not be underestimated elsewhere. Many Russian-speaking gangs started off by targeting companies in post-Soviet space and then switched to other geographies. By publishing the first threat report about OldGremlin we want to help security professionals better track OldGremlin and eliminate the risks of incidents involving the gang."*

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