Big Game Hunting: Now in Russia

By Oleg Skulkin, Senior Digital Forensics Analyst at Group-IB

Archived: 2026-05-01 02:39:24 UTC

The email raised no suspicions. An employee of a Russian medical company boldly clicked on the link and downloaded the attached ZIP archive. The message with the subject "*Bill due*" looked like it had been sent by the Finance Department of a large Russian media holding, the RBC Group. After the executable file was run for just twenty seconds, Windows Defender detected and deleted the malware. Yet these twenty seconds were enough for the Trojan to achieve persistence in the infected system. The victim failed to notice anything. Three weeks later, the company's employees arrived at work and were greeted by an alarming message on their computer screens: "*Your files have been encrypted*". All work stopped. The attackers demanded $50,000 in cryptocurrency to decrypt the files. A new cybercriminal group called OldGremlin was behind that attack.

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.

Here is your invoice

In August 2020, Group-IB uncovered the details of the first successful attack conducted by OldGremlin. The victim was a large medical company with a network of regional branches. The initial compromise vector was a phishing email allegedly sent by the media holding company RBC.

Group-IB Threat Intelligence analysts established that, at the initial stage, **the threat actors used a unique custom malware called TinyNode – a backdoor that downloads and launches additional malware.** After gaining remote access to the victim's computer, the cybercriminals could easily perform network reconnaissance, collect valuable data, and propagate across the organization's network. Like many other groups, OldGremlin used the Cobalt Strike framework to ensure that any post-exploitation activity was as effective as possible.

After the attackers conducted reconnaissance and made sure that they were in the domain that interested them, they continued to move laterally across the network, eventually obtaining domain administrator credentials. They even created an additional account with the same privileges in case the main one was blocked.

In this particular case, backing up did not save the victim. A few weeks after the attack began, the cybercriminals wiped the organization's backups. In just a few hours on weekend, they spread their ransomware TinyCryptor across hundreds of computers on the corporate network .

When the employees arrived at work the next day, they were greeted by an alarming message on their computer screens: "*Your files are encrypted. To decrypt them, contact us at…*" The phrase was followed by a mailbox hosted on ProtonMail. Interestingly, the criminals create a new email address for each new campaign. As a result of the attack, the company's regional branches were paralyzed and unable to operate. The attackers demanded **50,000 dollars** in cryptocurrency for decryption.

OldGremlin is the only Russian-speaking ransomware operator that violates the unspoken rule about not working within Russia and post-Soviet countries. They carry out multistage targeted attacks on Russian companies and banks using sophisticated tactics and techniques similar to those employed by APT groups. As with similar groups that target foreign entities, OldGremlin can be classed as part of **Big Game Hunting**, which brings together ransomware operators targeting large corporate networks.

Riding the COVID-19 wave: The first campaigns

Group-IB Threat Intelligence experts first detected OldGremlin's attack between late March and early April 2020. **The criminals took advantage of COVID-19 and sent financial institutions fake recommendations on how to organize a safe working environment during a pandemic**, impersonating the self-regulatory organization Mikrofinansirovaniye i Razvitiye (SRO MiR). It was the first time that the threat actors used TinyPosh, a custom Trojan they developed themselves. The second attack occurred on April 24. The scheme was more or less the same, but this time the hackers impersonated Novadent, a dental clinic.

Two weeks later, Old Gremlin changed tactics. They prepared a fake email allegedly sent by a Russian RBC journalist who invited recipients to take part in the "*Nationwide survey of the banking and financial sectors during the coronavirus pandemic*." Unlike with emails used in earlier incidents, the message from the "RBC reporter" was meticulously drafted in correct Russian and accurately imitated the media holding's style.

The "journalist" offered the potential victim (a bank employee) a 30-minute interview and promised to schedule the meeting through Calendly. For the attack, the hackers created a calendar using this software, in which they made an appointment for the victim.

The criminals then sent the victim a second email in which the "journalist" explained that she had "*uploaded the questions to the cloud*" and was awaiting answers. The email was designed to spark the victim's interest and encourage them to click on the link. To make the email look more convincing, each message contained the name of a major foreign cybersecurity vendor that had allegedly verified it.

As in the first campaigns, **opening the link in the email resulted in the TinyPosh Trojan being downloaded to the victim's computer.** The malware achieved persistence in the system, obtained privileges of the account from which the Trojan was launched, and could download and launch the Cobalt Strike Beacon upon command. To hide the real C&C address, the hackers used the Cloudflare Workers server.

OldGremlin spreads across Russia

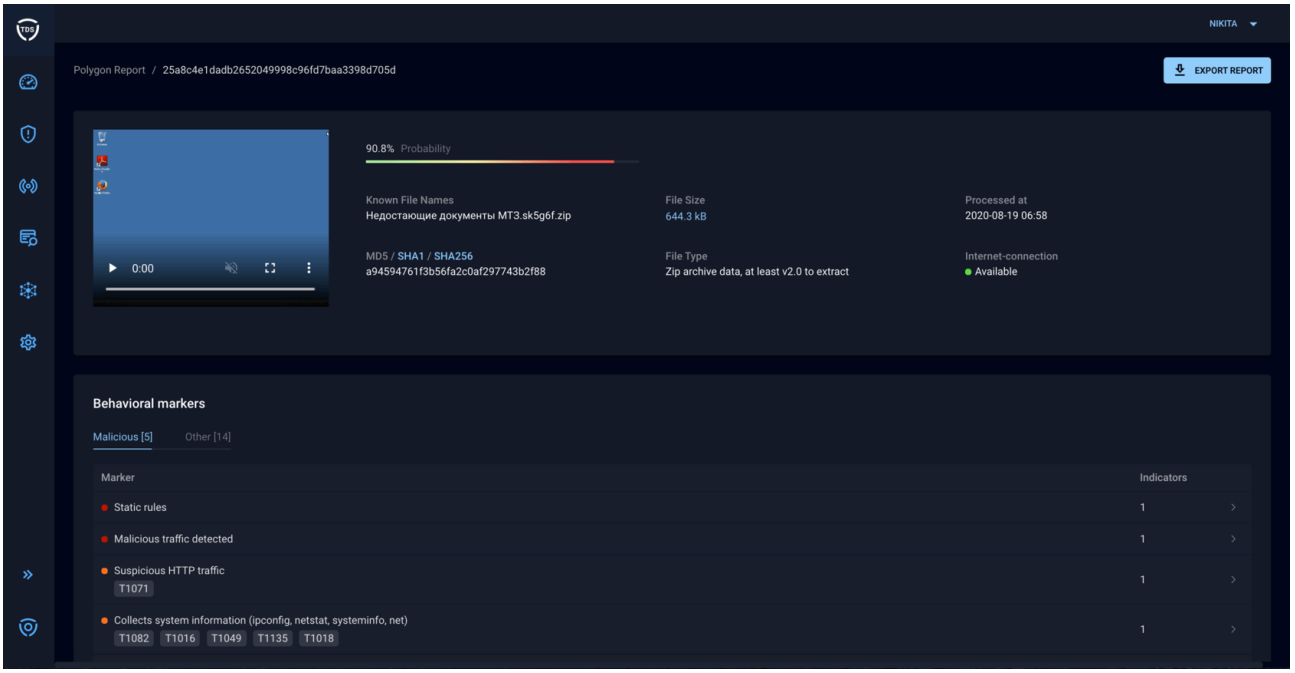
After a short "vacation", the group resumed its activity. On August 13 and 14, 2020, CERT-GIB (Group-IB's Computer Emergency Response Team) tracked two large-scale malicious campaigns as part of which the hackers impersonated RBC (Russian media holding company) and a mining and metallurgical company. Within two days, **the criminals sent around 250 malicious emails targeting Russian companies in the financial and industrial sectors**. Unlike the case with the "journalist" (the name used was the same as an actual RBC reporter's), the senders impersonated non-existent employees.

Within a few days, the cybercriminals edited the decoy email to take advantage of the key topic in Russian-language media: the protests in Belarus. On the morning of August 19, CERT-GIB team detected malicious campaigns targeting Russian financial organizations. The emails were allegedly from Minsk Tractor Works (MTZ). In total, more than 50 malicious emails were identified and blocked by Group-IB Threat Detection System (TDS).

The email's sender was "Alesya Vladimirovna" (or "A.V. Volokhina" in some cases), allegedly MTZ's CEO, although the company is in fact headed by a different person: Vitaly Vovk. The cybercriminals used the protests and strikes in Belarus as a theme for their emails: "*Unfortunately, about a week ago the prosecutor's office inspected MTZ. It is clear that this happened because of a strike we organized to protest against Lukashenko*." Further down, the recipients were asked to follow a link, download an archive, and send the missing documents

for verification. In fact, CERT-GIB analysts established that after victims opened the attachment, the TinyPosh backdoor was downloaded and installed on their computer.

OldGremlin adopted creative approach to their spearphishing emails. On August 19, Group-IB Managed XDR detected and blocked emails, containing links to malicious ZIP-files. These well-crafted emails exploited current news as a lure. The cybercriminals also used public URL shortening service (e.g. bit.ly) to mask the links to malicious files. OldGremlin's campaigns were successfully detected and their emails were blocked at the companies equipped with Group-IB Managed XDR.



Managed Extended Detection and Response Polygon is designed to conduct behavior analysis of files extracted from emails, network traffic, file storage systems, personal computers, and automated systems, as well as manually uploaded files and those extracted through API integration.

The lack of a strong channel of communication between organizations that counter cybercrime and the context of political instability have led to the emergence of new criminal groups who think that they can get away with their crimes. Another factor that help cybercriminals make money on ransoms include businesses underestimating threats and the lack of security controls that identify and block ransomware on time.

Rustam Mirkasymov, Head of Dynamic Malware Analysis Department at Group-IB

MITRE ATT&CK Mapping

Tactic	Technique	Procedure
Initial Access	Phishing: Spearphishing Link	OldGremlin used spearphishing links to archives with malicious LNK files or SFX-archives.

Tactic	Technique	Procedure
Execution	User Execution: Malicious File	A user must run a malicious file to start code execution.
	Command and Scripting Interpreter: PowerShell	OldGremlin used obfuscated PowerShell scripts.
	Command and Scripting Interpreter: JavaScript/JScript	OldGremlin used obfuscated JS-scripts.
Persistence	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	OldGremlin used Software\Microsoft\Windows\CurrentVersion\Run for TinyPosh and TinyNode persistence.
Defense Evasion	Signed Binary Proxy Execution: Mshta	OldGremlin used mshta.exe to run obfuscated JS-scripts.
	Signed Binary Proxy Execution: Rundll32	OldGremlin used rundll32.exe to open a decoy document.
	Process Injection: Asynchronous Procedure Call	OldGremlin injected Cobalt Strike into legitimate processes (e.g., svchost.exe and rundll32.exe) via asynchronous procedure call (APC) queue.
	Obfuscated Files or Information	OldGremlin obfuscated scripts and commands they used during the attack lifecycle.
Credential Access	Credentials from Password Stores: Credentials from Web Browsers	OldGremlin extracted passwords from web-browsers via NirSoft WebBrowserPassView.
	Unsecured Credentials: Credentials In Files	OldGremlin extracted email passwords via NirSoft Mail PassView.
Discovery	Software Discovery	OldGremlin collected information about programs installed on the compromised host.
	Remote System Discovery	OldGremlin collected information about the hosts in the network to move laterally and deploy TinyCryptor.
Lateral Movement	Lateral Tool Transfer	OldGremlin moved laterally with help of Cobalt Strike Beacon.
	Remote Services: Remote Desktop Protocol	OldGremlin used RDP for lateral movement.

Tactic	Technique	Procedure
	Remote Services: SMB/Windows Admin Shares	OldGremlin deployed TinyCryptor with PsExec module of Cobalt Strike.
Collection	Screen Capture	OldGremlin created screenshots from the compromised host.
Command and Control	Proxy: Multi-hop Proxy	OldGremlin used Tor to communicate with the compromised host.
	Encrypted Channel: Symmetric Cryptography	OldGremlin used RC4 to encrypt transmitted data.
Impact	Data Encrypted for Impact	OldGremlin encrypted data on computers in the network with help of TinyCryptor ransomware.

Indicators of compromise

MD5

arrow_drop_down

e47a296bac49284371ac396a053a8488

2c6a9a38ace198ab62e50ab69920bf42

306978669ead832f1355468574df1680

94293275fcc53ad5aca5392f3a5ff87b

1e54c8bc19dab21e4bd9cfb01a4f5aa5

fc30e902d1098b7efd85bd2651b2293f

e0fe009b0b1ae72ba7a5d2127285d086

f30e4d741018ef81da580ed971048707

ac27db95366f4e7a7cf77f2988e119c2

30fdbf2335a9565186689c12090ea2cf

e1692cc732f52450879a86cb7dcfbccd

Registry paths

arrow_drop_down

HKCU:\Software\Classes\Registered

HKCU:\\Software\\Microsoft\\Windows\\Security

IPs and Domains

arrow_drop_down

136.244.67[.]59

95.179.252[.]217

45.61.138[.]170

5.181.156[.]84

rbcholding[.]press

broken-poetry-de86.nscimupf.workers[.]dev

calm-night-6067.bhrcaoqf.workers[.]dev

rough-grass-45e9.poecdjusb.workers[.]dev’

ksdkpwprtyvbxdobr0.tyvbxdobr0.workers[.]dev’)

ksdkpwpfrtyvbxdobr1.tiyvbxdobr1.workers[.]dev

wispy-surf-fabd.bhrcaoqf.workers[.]dev

noisy-cell-7d07.poecdjusb.workers[.]dev

wispy-fire-1da3.nscimupf.workers[.]dev

hello.tyvbxdobr0.workers[.]dev

curly-sound-d93e.ygrhxogxiogc.workers[.]dev

old-mud-23cb.tkbizulvc.workers[.]dev

In most cases, access to data found on a ransomware-infected device cannot be restored without decryption keys, which attackers hold for ransom. It is never advisable to pay a single cent. What Group-IB experts do recommend and consider extremely important is responding to ransomware attacks appropriately.

Get the help of our skilled global **Incident Response** team to ensure rapid and thorough containment of the most damaging cyberattacks, as well as remediation and recovery.
