OLDGREMLIN

[/ ˈoʊld ˈgrɛmlɪn /]

OldGremlin is a high-risk, Russian-speaking, financially motivated threat group active since ~2020, combining double-extortion ransomware with APT-level stealth and long-term access to steal data, targeting enterprises across Europe, the Americas, and Russia.

IDENTITY

Attribution	: Russian-speaking cybercriminal group exhibiting Advanced Persistent Threat (APT)–level sophistication.
Active Since	: Early 2020; ongoing operations through 2025.
Aliases	: N/A — maintains a consistent and unique malware/tooling profile.
Motivation	: Financially driven ransomware extortion; secondary focus on data theft and prolonged network access.

TTPs

Initial Access	- Spear-phishing emails in Russian, English, and Spanish. - Impersonation of media outlets, financial institutions, and supply-chain vendors. - Malicious documents with macro-based loaders and trojanized attachments. - Compromised VPN/RDP credentials.
Execution	- Deployment of custom backdoors, including TinyNode, TinyShell, and other bespoke implants. - Extensive PowerShell automation for reconnaissance. - Controlled and delayed activation of ransomware.
Persistence	- Scheduled tasks. - Registry run keys. - Web shells. - Hijacked VPN sessions.
C2 Infrastructure	- Encrypted communications via cloud services. - Proxy-chained callbacks with low frequency to avoid detection. - Compromised hosts used as internal pivots.
Lateral Movement	- Abuse of legitimate tools (LOLbins). - RDP pivoting across internal environments. - Credential dumping with Mimikatz and custom scripts. - Mapping of backup servers and domain controllers.
Exfiltration & Ransomware Deployment	- Targeted exfiltration of business-critical data. - Custom-built ransomware compiled per victim. - Double extortion via encryption + leak site pressure.

TARGET PROFILE

Sectors	: Finance, manufacturing, logistics, healthcare, retail.
Geographies	: Russia (initial focus), expanding to Europe, North America, and Latin America.
Victim Characteristics	: Mid-to-large enterprises with complex infrastructure and valuable intellectual property or financial data.

THREAT ASSESSMENT

Risk Level	: High — meticulous, stealthy, human-operated intrusions.
Most Recent Activity	: 2024–2025 ransomware campaigns leveraging enhanced implant modularity and cloud exfiltration.
Evolution	: Transition from ransomware-only operations to APT-grade reconnaissance and prolonged persistence.

NOTABLE OPERATIONS

- **2020:** Targeted Russian healthcare and logistics organizations using COVID-themed phishing.
- **2021:** Expanded into European manufacturing and retail firms; weeks-long dwell times observed.
- **2022–2023:** Shift toward North American victims; multilingual phishing; improved backdoors.
- **2024:** Supply-chain impersonation techniques refined; invoice/shipping lures used extensively.
- **2025:** New ransomware families and advanced data exfiltration via cloud relay nodes.