LARVA 208

[/ ˈlɑːrvə /]

Larva208, a Russia-aligned actor active since 2023, blends ransomware and espionage. High-risk operations include data extortion and stealthy intrusions targeting European governments, NATO states, North America, and APAC.

IDENTITY

Attribution	: Russia-aligned eCrime and APT-linked actor
Active Since	: At least 2023, with campaigns continuing into 2025
Aliases	: Larva208
Motivation	: Mixed: financially motivated ransomware and extortion, combined with espionage-linked activity against government and defense

TTPs

Initial Access	: Exploitation of VPN and edge device vulnerabilities, spearphishing with malicious attachments, credential theft
Persistence	: Scheduled tasks, use of stolen administrator accounts, tunneling tools for long-term access
C2 Infrastructure	: Proxy-based infrastructure, anonymization via TOR and compromised servers
Malware & Tools	: Custom loaders, infostealers, ransomware payloads, commodity RATs for staging
Techniques	: Data exfiltration prior to encryption, selective extortion without encryption, blending espionage tradecraft with ransomware TTPs

TARGET PROFILE

Target Sectors	: Government ministries, defense contractors, financial institutions, technology and telecom providers
Geographies Targeted	: Primary: Europe and NATO member states, Secondary: North America and APAC enterprises with focus on IT and telecom supply chain

THREAT ASSESSMENT

Risk Level	: High: proven ability to compromise critical government and enterprise systems while maintaining flexibility between espionage and financial operations
Most Recent Activity	• 2025: Targeting of European government networks with loaders and infostealers • 2025: Data extortion operations against financial services in North America • 2024: Opportunistic campaigns against telecom providers in APAC
Evolution	: Shift from pure ransomware campaigns toward hybrid espionage-extortion model, with growing sophistication in initial access and persistence techniques

NOTABLE OPERATIONS

- **2023:** First identified campaigns linked to opportunistic ransomware targeting Eastern European enterprises
- **2024:** Intrusions into APAC telecom and IT providers exploiting VPN zero-days
- **2025:** European government compromises leading to data theft and extortion without encryption