

FIN11

[/fɪn ɪˈlɛv.ən/]

This financially motivated cybercrime group has been active since at least 2014 and remains highly active through 2025, operating at a global scale. Known by multiple aliases including TA505 and Lace Tempest, it focuses on phishing-led intrusions, malware distribution, initial access brokerage, and ransomware enablement, targeting a wide range of industries worldwide.

IDENTITY

Attribution	: Financially motivated cybercrime group operating as part of the global cybercriminal underground.
Active Since	: At least 2014; sustained activity observed through 2025.
Aliases	: FIN11, DEV-0950, Lace Tempest, TA505, TEMP.Warlock, UNC902.
Motivation	: Monetization via malware distribution, credential theft, initial access sales, ransomware deployment, and extortion.

TTPs

Initial Access	- Large-scale phishing campaigns using invoice, payment, shipping, and business-themed lures. - Malicious attachments and links delivering loaders. - HTML smuggling to evade secure email gateways. - ISO, ZIP, and VHD containers to bypass macro restrictions.
Execution	- Use of loaders and droppers to stage secondary payloads. - Execution of malware families such as Dridex, ServHelper, FlawedAmmyy, and SDBbot. - PowerShell and native Windows tools for payload execution.
Persistence	- Scheduled tasks and registry run keys. - Services masquerading as legitimate software components. - Reinfection mechanisms via secondary loaders.
Command & Control (C2)	- Distributed C2 infrastructure using compromised servers and bulletproof hosting. - Encrypted HTTPS or custom protocols. - Frequent domain and IP rotation to evade blocking.
Defense Evasion	- Heavy obfuscation and packing of malware. - Delayed execution and environment checks to evade sandboxes. - Living-off-the-land techniques to reduce detection.
Data Exfiltration	- Credential theft and system reconnaissance data exfiltrated via encrypted channels. - Support of downstream data theft by ransomware affiliates.

TARGET PROFILE

Primary Sectors	: Financial services, healthcare, manufacturing, retail, logistics, professional services.
Secondary Sectors	: Small and medium-sized businesses with limited security maturity.
Geographic Focus	: Global; no regional restriction.

THREAT ASSESSMENT

Risk Level	: High – FIN11's scale, adaptability, and ecosystem role amplify downstream impact.
Recent Activity	: Ongoing phishing and loader campaigns supporting ransomware-as-a-service operations.
Evolution	: Reduced reliance on macros, increased use of HTML smuggling and containerized payloads, and stronger partnerships with ransomware groups.

NOTABLE OPERATIONS

- **TA505 Global Phishing Campaigns:** Massive email waves delivering Dridex and related malware worldwide.
- **Clop Ransomware Enablement:** Provision of access and tooling during early Clop ransomware campaigns.
- **Access Brokerage Operations:** Sale or handoff of compromised networks to ransomware and extortion actors.