TA577 (Hive0118)

[/ˌtiː ˈeɪ faɪv ˈsɛv.ən ˈsɛv.ən/]

TA577 (Hive0118) is a Russian-speaking, financially motivated cybercrime group active since mid-2020, known for high-risk global phishing and credential theft campaigns. It is linked to Black Basta ransomware and primarily targets organizations in North America and Europe.

IDENTITY

Attribution : Russian-speaking (Russia-nexus) cybercrime group; financially motivated, not publicly assessed as state-directed.

Active Since : Mid-2020

Aliases : Hive0118 (identified by Microsoft Threat Intelligence)

Motivation : Financial gain through phishing, credential theft, and malware delivery; provides access to ransomware operators such as Black Basta.

TTPs

Initial Access : Conducts large-scale phishing campaigns using thread hijacking, reply-chain injection, and HTML smuggling. Frequently uses ZIP, OneNote, and ISO attachments containing malicious payloads.

Execution : Deploys Qbot (QakBot), IcedID, Latrodectus, and Pikabot as primary loaders. Utilizes legitimate binaries such as PowerShell and Rundll32 to execute payloads.

Persistence : Achieved through scheduled tasks, registry autoruns, and reuse of stolen credentials, including NTLM hashes.

Command & Control (C2) : Maintains communication via encrypted HTTPS channels, fast-flux DNS, and compromised WordPress or CMS sites.

Defense Evasion : Uses multi-stage payloads, obfuscated PowerShell scripts, sandbox evasion, and HTML smuggling techniques to bypass detection.

Credential Theft : Since early 2024, focuses on coercing NTLM authentication via phishing to capture hashes and enable lateral movement.

Tools & Malware : Relies on Qbot, IcedID, Pikabot, Latrodectus, credential dumpers, and PowerShell-based loaders.

TARGET PROFILE

Target Sectors

- Targets finance, technology, manufacturing, professional services, and healthcare sectors.
- Operates globally, with primary focus on North America and Europe.
- Exploits enterprise email gateways and Windows authentication mechanisms such as NTLM.

THREAT ASSESSMENT

Risk Level : High.

Most Recent Activity : Active between 2024–2025 with extensive phishing and NTLM hash theft campaigns.

Evolution : Transitioned from an initial access broker to an advanced credential theft and post-exploitation actor.

Ransomware Links : Frequently provides access to Black Basta and other ransomware operators.

NOTABLE OPERATIONS

- **August 2023:** Shifted from Qbot to Pikabot and Latrodectus after QakBot's takedown, ensuring continuity of operations.
- **February 2024:** Launched phishing campaigns aimed at coercing NTLM authentication to harvest hashes for credential theft.
- **October 2024:** Continued distributing multiple loaders alongside NTLM-focused phishing lures targeting global enterprises.
- **January 2025:** Expanded operations globally, with intrusions frequently leading to follow-on Black Basta ransomware attacks.