LevelBlue - Open Threat Exchange

By CyberHunterAutoFeed

Archived: 2026-04-06 02:06:17 UTC

- 1,584 Subscribers

- 1,584 Subscribers

HYDRA SAIGA: COVERT ESPIONAGE AND INFILTRATION OF CRITICAL UTILITIES

FileHash-MD5: 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 6 | **URL:** 33 | **Domain:** 16 | **Hostname:** 8

Hydra Saiga, an alleged state-sponsored threat group from Kazakhstan, has been active since at least 2021 and focuses on infiltrating government and critical infrastructure sectors, particularly in Central Asia, Europe, and the Middle East. The group employs various tactics and tools for command-and-control (C2) operations, notably utilizing the Telegram Bot API and deploying both commodity and custom malware, including payloads written in languages such as Python, PowerShell, Golang, and Rust.

- 161 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 841 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 54 Subscribers

AI-augmented threat actor accesses FortiGate devices at scale

CVE: 3

Recent investigations by Amazon Threat Intelligence have revealed a troubling trend: financially motivated threat actors leveraging commercial AI tools to conduct large-scale cyberattacks, impacting over 600 FortiGate devices across more than 55 countries. This campaign spanned from January 11 to February 18, 2026, indicating a shift in the landscape where even less skilled individuals can execute significant operations through AI augments. The actions of this Russian-speaking actor primarily focused on exploiting weak security practices, notably exposed management ports and inadequate credential protection, as opposed to leveraging specific vulnerabilities within FortiGate appliances.

- 161 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

ThreatFox Hunt: Meterpreter IOCs - 2026-02-16

Automated ThreatFox hunt for Meterpreter indicators. 23 IOCs collected via Pattern 49 intelligence streaming. MITRE ATT&CK: T1055, T1059.001, T1105, T1027. Reference: https://analytics.dugganusa.com

- 152 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:Meterpreter