LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 17:00:55 UTC

ClickFix Resurgence in 2026: Matanbuchus 3.0 and AstarionRAT Drive Advanced Multi-Stage Intrusion Campaign

FileHash-SHA256: 8 | **URL:** 2 | **Domain:** 4 | **Hostname:** 1

In February 2026, a targeted intrusion by the Huntress Tactical Response team highlighted a resurgence of the ClickFix infection method, which exploits social engineering tactics to manipulate users into executing malicious commands. This technique had become a primary vector for initial access, favored by both cybercriminals and nation-state actors throughout 2025. The ClickFix method bypasses conventional security protocols by turning users into unwitting spreaders of malware. A notable combination unveiled during the incident was that of ClickFix and Matanbuchus 3.0, the latter of which re-emerged after a brief pause in May 2025. Matanbuchus is introduced through ClickFix's prompts and uses silent MSI installations as part of its intricate execution chain.

- 161 Subscribers

- 174 Subscribers

DanaBot

FileHash-MD5: 27 | **FileHash-SHA1:** 27 | **FileHash-SHA256:** 95 | **Domain:** 50 | **Hostname:** 1

- 174 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

- 1,584 Subscribers

Interesting | OTC AlienVault.com connection issues for me | alienvault.io =404 |

FileHash-SHA256: 11 | **Domain:** 3 | **Hostname:** 1

Found on a victims devices. Targets abused in an unethical manner by andvesarial entities. Waged against targets such as victims of crime , journalists , researchers , students. Target Users: Serves public safety, enterprise, and government sectors, aiding first responders, investigators, prosecutors, and analysts. How it's Used Law enforcement uses it to unlock devices and retrieve evidence like messages, location history, and app data for criminal investigations. It helps uncover critical information from digital devices, even recovering data that users thought was permanently deleted. Controversy & Privacy Concerns While marketed as a tool for lawful investigations, its powerful data extraction capabilities raise significant privacy concerns and ethical debates.

- 134 Subscribers

Danabot

FileHash-MD5: 200 | **FileHash-SHA1:** 200 | **FileHash-SHA256:** 1000

- 174 Subscribers

Cross-Chain TxDataHiding Crypto Heist: A Very Chainful Process.

FileHash-MD5: 3 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 20 | **URL:** 3 | **Domain:** 1 | **Hostname:** 1

In September 2025, an investigation by Ransom-ISAC into a sophisticated breach linked to North Korean threat actors uncovered a multi-layered attack targeting cryptocurrency and data theft through a weaponized GitHub repository. Initially identified as a phishing campaign, the operation utilized blockchain-based command-and-control (C2) infrastructures paired with cross-platform malware that affected development environments on a wide scale. The attack leveraged two primary types of C2 channels: a Python dropper utilizing an HTTP API over port 27017 and a Loader/RAT employing both HTTP API and http://Socket.IO channels over ports 27017 and 443. Each C2 channel exhibited distinctive characteristics, including specific HTTP header configurations tailored to maintain covert communication and server persistence. For instance, the Keep-Alive header was configured to ensure timely requests from victims, ultimately aiding in the communication interval with the C2 server.

- 161 Subscribers

Danabot Malware Reemerges with Version 669 After Operation Endgame

BitcoinAddress: 1 | **URL:** 1

Danabot, a banking malware, has resurfaced with its new version 669 following the disruption caused by Operation Endgame in May 2025. This marks a notable return for the malware, which had been relatively inactive for nearly six months. The refreshed activity suggests that the threat actors behind Danabot have adapted and evolved their strategies, continuing to pose significant risks to organizations. Recent observations by security researchers reveal the deployment of multiple new command-and-control (C2) servers. This diversification in infrastructure indicates a calculated effort by the threat actors to enhance their operational resilience and evade detection, thereby strengthening their capability to orchestrate cyber attacks.

- 161 Subscribers

- 1,584 Subscribers

- 410 Subscribers

Remote access, real cargo: cybercriminals targeting trucking and logistics

FileHash-MD5: 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 6 | **URL:** 1 | **Domain:** 29 | **Hostname:** 2

Cybercriminals are targeting trucking and logistics companies to steal cargo freight through elaborate attack chains. They compromise companies and use their access to bid on cargo shipments, which they then steal and sell. The threat actors typically deliver remote monitoring and management (RMM) tools as a first-stage payload. This cyber-enabled theft is part of a multi-million-dollar criminal enterprise that has increased due to digital transformation. The attackers use tactics such as compromising load boards, email thread hijacking, and direct targeting via email campaigns. They deliver RMM tools like ScreenConnect, SimpleHelp, and PDQ Connect, which grant full control of compromised machines. The activity has been observed since at least June 2025, with nearly two dozen campaigns in the last two months alone.

- 373,947 Subscribers

- 54 Subscribers

Dark Covenant 3.0: Controlled Impunity and Russias Cybercriminals.

URL: 1 | **Domain:** 3 | **Email:** 4

The Russian cybercrime landscape is currently undergoing significant changes due to intensified international law enforcement operations, notably Operation Endgame, which commenced in May 2024. This initiative targets key elements of the ransomware ecosystem, including operators, money laundering services, and related infrastructures within Russia. Historically, Russia has maintained a non-interference stance on domestic cybercrime; however, recent enforcement actions signal a notable shift towards increased state management of cybercriminal activities.

- 161 Subscribers

Threat Actor Profile: Interlock Ransomware.

CVE: 2 | **FileHash-MD5:** 11 | **FileHash-SHA1:** 14 | **FileHash-SHA256:** 11 | **URL:** 1 | **Domain:** 2

Interlock (aka Nefarious Mantis) is an opportunistic ransomware operator first observed September 2024 and active across North America and Europe through 2025, targeting education, healthcare, technology, government, and other sectors. Law enforcement advisories (CISA/FBI) in mid-2025 noted upgrades to Interlock tooling, including encryptors for both Windows and Linux and capability to encrypt virtual machines.

- 161 Subscribers

- 841 Subscribers

Steam games abused to deliver malware once again.

FileHash-MD5: 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 4 | **URL:** 20 | **Domain:** 2

The cybercriminal known as EncryptHub, also referred to as Larva-208, has exploited the online gaming platform Steam to distribute information-stealing malware. The method involved embedding malicious files within the game files of Chemia, an adventure survival game that is currently in early access on Steam. As of July 22, 2025, EncryptHub introduced a Trojan downloader into Chemia, which operates adjacent to the legitimate game application. This downloader maintains persistence on the infected systems and subsequently disseminates various types of malware, specifically Fickle Stealer, HijackLoader, and Vidar.

- 161 Subscribers

BladedFeline: Unmasking the Iran-Aligned Cyberespionage Group

FileHash-MD5: 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 2 | **URL:** 5 | **Domain:** 5 | **Hostname:** 5

Dive into ESET's comprehensive analysis of BladedFeline, an Iran-aligned APT group with likely ties to OilRig. This report uncovers the group's sophisticated cyberespionage operations targeting Kurdish and Iraqi government officials. Learn about their advanced tools, including the Whisper backdoor and PrimeCache IIS module, and their persistent efforts to maintain access to high-ranking officials.

- 161 Subscribers
