LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 13:46:27 UTC

Keeping our hand on Pulse. Mythic Likho cyberattacks on Russia's C.I.A

FileHash-MD5: 35 | **FileHash-SHA1:** 35 | **FileHash-SHA256:** 35 | **Domain:** 19

The Mythic Likho group has been conducting sophisticated cyberattacks on Russian critical infrastructure since September 2024, utilizing a variety of malware tools including the Loki backdoor and the Merlin bootloader. Key methodologies include extensive reconnaissance of targets, where the group gathers detailed information about victims' organizational structure, associated entities, email addresses, and business roles. This intelligence aids in crafting convincing phishing campaigns aimed at infiltrating target networks. Mythic Likho employs social engineering tactics, mimicking legitimate organizations to create trustworthy email addresses used for phishing. The group registers domains with Russian cloud services and often deploys virtual servers to facilitate their operations, leveraging platforms like Cloudflare to obscure their malicious IP addresses.

- 161 Subscribers

- 37 Subscribers

macOS Threat Infrastructure Leveraging Remote Agents via remotewd.com and rtmsprod.net

CIDR: 12 | **CVE:** 40 | **FileHash-MD5:** 223 | **FileHash-SHA1:** 523 | **FileHash-SHA256:** 2356 | **SSLCertFingerprint:** 302 | **URL:** 14263 | **Domain:** 3847 | **Email:** 223 | **Hostname:** 4449

This pulse identifies an actively observed macOS-focused remote access infrastructure abusing trusted native Apple agents (ARDAgent.app, SSMenuAgent.app) and communicating with a distributed network of C2-like endpoints under domains such as remotewd.com, idsremoteurlconnectionagent.app, and rtmsprod.net. The infrastructure is composed of dynamically generated subdomains — many in the form of device-<UUID>.remotewd.com — indicative of automated deployment, system tracking, or per-host remote access configurations. Additional indicators include HTTP/S URLs pointing directly to embedded binary paths within macOS agents, suggesting possible delivery vectors, staging, or persistence techniques. This campaign shows signs of structured, programmatic targeting and is highly likely to be pre-operational infrastructure for wide-scale surveillance or access operations. All listed indicators should be considered high-risk. If observed in your environment, initiate a full forensic and IR process immediately.

- 30 Subscribers

AISHAH LAZIM - Import Customs Data Records - ImportKey

CIDR: 2 | **CVE:** 2 | **FileHash-MD5:** 1014 | **FileHash-SHA256:** 56 | **URL:** 253 | **Domain:** 181 | **Email:** 26 | **Hostname:** 149

MacBook M2 chip bound to an unauthorized Microsoft Active Directory (AD) network, granting external control and command over the device. This situation has facilitated the illicit sale of personally identifiable information (PII) on the dark web. The criminal network responsible for this activity continues to grow at an alarming rate, while government authorities have remained largely inactive in addressing the issue.

- 30 Subscribers

- 316 Subscribers

- 316 Subscribers

- 32 Subscribers

RansomHub

CVE: 9 | **FileHash-SHA256:** 24 | **URL:** 103 | **Domain:** 19 | **Email:** 2 | **Hostname:** 20

RansomHub is a ransomware-as-a-service group focusing on financial gain through cyber extortion. It targets various sectors, including healthcare, government, and critical infrastructure, while explicitly avoiding attacks on certain countries like Cuba, North Korea, and China. Their methods include double extortion, where they encrypt victims' data and exfiltrate it for ransom, often demanding payment via a unique .onion URL. Victims receive a ransom note with a client ID and a deadline for payment before their data is leaked.

- 25 Subscribers

The Real Jane Doe Syndrome Files

CIDR: 3 | **FileHash-SHA256:** 219 | **URL:** 618 | **Domain:** 285 | **Email:** 21 | **Hostname:** 306

An array of scripts and files designed to completely compromise your MacBook and effectively erase your digital identity from the internet exists. This type of targeted attack is perpetrated by various groups for political or monetary agendas. It gradually takes over your devices and consumes your energy, time, career, and overall quality of life. In my case, the adversary involved is the DragonForce Malaysia Hacker Group.

- 30 Subscribers

Python: OVSAgentServer Document (autofilled name)

CIDR: 14 | **CVE:** 76 | **FileHash-MD5:** 52 | **FileHash-SHA1:** 48 | **FileHash-SHA256:** 841 | **URL:** 218 | **Domain:** 288 | **Email:** 33 | **Hostname:** 180

Here is the full text of the Vuze-dht-info script, which is written by "Patrik Karlsson" and followed by the following:-1-2-3. (Autofilled). This was pulled from a Windows 11 Hidden Folder from UAlberta Sample Device.

- 128 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

- 1,524 Subscribers

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