



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

5 May 25

Cyber Threat Roundup

A collection of recent open-source items of interest to the Defense Industrial Base

Contents

Articles	2
SentinelOne Uncovers Chinese Espionage Campaign Targeting Its Infrastructure and Clients.....	2
Malware Attack Targets World Uyghur Congress Leaders via Trojanized UyghurEdit++ Tool.....	2
WordPress Plugin Disguised as a Security Tool Injects Backdoor.....	2
Claude AI Exploited to Operate 100+ Fake Political Personas in Global Influence Campaign.....	3
DarkWatchman, Sheriff Malware Hit Russia and Ukraine with Stealth and Nation-Grade Tactics	3
Nebulous Mantis Targets NATO-Linked Entities with Multi-Stage Malware Attacks	3
SonicWall: SMA100 VPN Vulnerabilities Now Exploited in Attacks	3
Iranian Hackers Maintain 2-Year Access to Middle East CNI via VPN Flaws and Malware	4
Malicious PyPI Packages Abuse Gmail, Websockets to Hijack Systems.....	4
RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control	4

Articles

SentinelOne Uncovers Chinese Espionage Campaign Targeting Its Infrastructure and Clients

Cybersecurity company SentinelOne has revealed that a China-nexus threat cluster dubbed PurpleHaze conducted reconnaissance attempts against its infrastructure and some of its high-value customers. PurpleHaze is assessed to be a hacking crew with loose ties to another state-sponsored group known as APT15, which is also tracked as Flea, Nylon Typhoon (formerly Nickel), Playful Taurus, Royal APT, and Vixen Panda. The adversarial collective has also been observed targeting an unnamed South Asian government-supporting entity in October 2024, employing an operational relay box (ORB) network and a Windows backdoor dubbed GoReShell. The implant, written in the Go programming language, repurposes an open-source tool called reverse_ssh to set up reverse SSH connections to endpoints under the attacker's control. Further analysis has determined that the same South Asian government entity was also targeted previously in June 2024 with ShadowPad (aka PoisonPlug), a known backdoor widely shared among China-nexus espionage groups. ShadowPad is considered to be a successor to another backdoor referred to as PlugX.

<https://thehackernews.com/2025/04/sentinelone-uncovers-chinese-espionage.html>

Malware Attack Targets World Uyghur Congress Leaders via Trojanized UyghurEdit++ Tool

In a new campaign detected in March 2025, senior members of the World Uyghur Congress (WUC) living in exile have been targeted by a Windows-based malware that's capable of conducting surveillance. The spear-phishing campaign involved the use of a trojanized version of a legitimate open-source word processing and spell check tool called UyghurEdit++ developed to support the use of the Uyghur language. The email messages impersonated a trusted contact at a partner organization and contained Google Drive links, which, when clicked, would download a password-protected RAR archive. Present within the archive was a poisoned version of UyghurEdit++ that profiled the compromised Windows system and sent the information to an external server ("tengri.ooguy[.]com"). The C++ spyware also comes with capabilities to download additional malicious plugins and run commands against those components after likely verifying the machine belongs to a target of interest.

<https://thehackernews.com/2025/04/malware-attack-targets-world-uyghur.html>

WordPress Plugin Disguised as a Security Tool Injects Backdoor

A new malware campaign targeting WordPress sites employs a malicious plugin disguised as a security tool to trick users into installing and trusting it. According to Wordfence researchers, the malware provides attackers with persistent access, remote code execution, and JavaScript injection. At the same time, it remains hidden from the plugin dashboard to evade detection. Wordfence first discovered the malware during a site cleanup in late January 2025, where it found a modified 'wp-cron.php' file, which creates and programmatically activates a malicious plugin named 'WP-antymalware-bot.php.' Lacking server logs to help identify the exact infection chain, Wordfence hypothesizes the infection occurs via a compromised hosting account or FTP credentials. Not much is known about the perpetrators, though the researchers noted that the command and control (C2) server is located in Cyprus.

<https://www.bleepingcomputer.com/news/security/wordpress-plugin-disguised-as-a-security-tool-injects-backdoor/>

Claude AI Exploited to Operate 100+ Fake Political Personas in Global Influence Campaign

Artificial intelligence (AI) company Anthropic has revealed that unknown threat actors leveraged its Claude chatbot for an "influence-as-a-service" operation to engage with authentic accounts across Facebook and X. The now-disrupted operation, Anthropic researchers said, prioritized persistence and longevity over vitality and sought to amplify moderate political perspectives that supported or undermined European, Iranian, the United Arab Emirates (U.A.E.), and Kenyan interests. These included promoting the U.A.E. as a superior business environment while being critical of European regulatory frameworks, focusing on energy security narratives for European audiences, and cultural identity narratives for Iranian audiences.

<https://thehackernews.com/2025/05/claude-ai-exploited-to-operate-100-fake.html>

DarkWatchman, Sheriff Malware Hit Russia and Ukraine with Stealth and Nation-Grade Tactics

Russian companies have been targeted as part of a large-scale phishing campaign that's designed to deliver a known malware called DarkWatchman. Targets of the attacks include entities in the media, tourism, finance and insurance, manufacturing, retail, energy, telecom, transport, and biotechnology sectors. The activity is assessed to be the work of a financially motivated group called Hive0117, which has been attributed by IBM X-Force to attacks aimed at users in Lithuania, Estonia, and Russia spanning telecom, electronic, and industrial sectors. The latest set of attacks involves sending phishing emails containing password-protected malicious archives that, once opened, deliver a variant of DarkWatchman with improved capabilities to evade detection. The disclosure comes as IBM X-Force said an unspecified entity within Ukraine's defense sector was targeted in the first half of 2024 with a previously undocumented Windows backdoor called Sheriff.

<https://thehackernews.com/2025/05/darkwatchman-sheriff-malware-hit-russia.html>

Nebulous Mantis Targets NATO-Linked Entities with Multi-Stage Malware Attacks

Cybersecurity researchers have shed light on a Russian-speaking cyber espionage group called Nebulous Mantis that has deployed a remote access trojan called RomCom RAT since mid-2022. RomCom "employs advanced evasion techniques, including living-off-the-land (LOTL) tactics and encrypted command and control (C2) communications, while continuously evolving its infrastructure – leveraging bulletproof hosting to maintain persistence and evade detection. Nebulous Mantis, also tracked by the cybersecurity community under the names CIGAR, Cuba, Storm-0978, Tropical Scorpius, UAC-0180, UNC2596, and Void Rabisu, is known to target critical infrastructure, government agencies, political leaders, and NATO-related defense organizations. Attack chains mounted by the group typically involve the use of spear-phishing emails with weaponized document links to distribute RomCom RAT. The domains and command-and-control (C2) servers used in these campaigns have been hosted on bulletproof hosting (BPH) services like LuxHost and Aeza. The infrastructure is managed and procured by a threat actor named LARVA-290.

<https://thehackernews.com/2025/04/nebulous-mantis-targets-nato-linked.html>

SonicWall: SMA100 VPN Vulnerabilities Now Exploited in Attacks

Cybersecurity company SonicWall has warned customers that several vulnerabilities impacting its Secure Mobile Access (SMA) appliances are now being actively exploited in attacks. On Tuesday, SonicWall updated security advisories for the CVE-2023-44221 and CVE-2024-38475 security flaws to tag the two vulnerabilities as "potentially being exploited in the wild." CVE-2024-38475, is rated as a critical severity flaw caused by improper escaping of

output in `mod_rewrite` in Apache HTTP Server 2.4.59 and earlier. Successful exploitation can allow unauthenticated, remote attackers to gain code execution by mapping URLs to file system locations permitted to be served by the server. The two vulnerabilities impact SMA 200, SMA 210, SMA 400, SMA 410, and SMA 500v devices and are patched in firmware version 10.2.1.14-75sv and later.

<https://www.bleepingcomputer.com/news/security/sonicwall-sma100-vpn-vulnerabilities-now-exploited-in-attacks/>

Iranian Hackers Maintain 2-Year Access to Middle East CNI via VPN Flaws and Malware

An Iranian state-sponsored threat group has been attributed to a long-term cyber intrusion aimed at a critical national infrastructure (CNI) in the Middle East that lasted nearly two years. The activity, which lasted from at least May 2023 to February 2025, entailed "extensive espionage operations and suspected network prepositioning – a tactic often used to maintain persistent access for future strategic advantage. The network security company noted that the attack exhibits tradecraft overlaps with a known Iranian nation-state threat actor called Lemon Sandstorm (formerly Rubidium), which is also tracked as Parisite, Pioneer Kitten, and UNC757. It's been assessed to be active since at least 2017, striking aerospace, oil and gas, water, and electric sectors across the United States, the Middle East, Europe, and Australia. According to industrial cybersecurity company Dragos, the adversary has leveraged known virtual private network (VPN) security flaws in Fortinet, Pulse Secure, and Palo Alto Networks to obtain initial access.

<https://thehackernews.com/2025/05/iranian-hackers-maintain-2-year-access.html>

Malicious PyPI Packages Abuse Gmail, Websockets to Hijack Systems

Seven malicious PyPi packages were found using Gmail's SMTP servers and WebSockets for data exfiltration and remote command execution. The packages were discovered by Socket's threat research team, who reported their findings to the PyPI, resulting in the removal of the packages. However, some of these packages were on PyPI for over four years, and based on third-party download counters, one was downloaded over 18,000 times. The malicious functionality Socket discovered in these packages centers on covert remote access and data exfiltration through Gmail. The packages used hardcoded Gmail credentials to log into the service's SMTP server (`smtp.gmail.com`), sending reconnaissance information to allow the attacker to remotely access the compromised system.

<https://www.bleepingcomputer.com/news/security/malicious-pypi-packages-abuse-gmail-websockets-to-hijack-systems/>

RansomHub Went Dark April 1; Affiliates Fled to Qilin, DragonForce Claimed Control

Cybersecurity researchers have revealed that RansomHub's online infrastructure has "inexplicably" gone offline as of April 1, 2025, prompting concerns among affiliates of the ransomware-as-a-service (RaaS) operation. Singaporean cybersecurity company Group-IB said that this may have caused affiliates to migrate to Qilin, given that "disclosures on its DLS [data leak site] have doubled since February." RansomHub, which first emerged in February 2024, is estimated to have stolen data from over 200 victims. It replaced two high-profile RaaS groups, LockBit and BlackCat, to become a frontrunner, courting their affiliates, including Scattered Spider and Evil Corp, with lucrative payment splits. RansomHub's ransomware is designed to work on Windows, Linux, FreeBSD, and ESXi as well as on x86, x64, and ARM architectures, while avoiding attacking companies located in the Commonwealth of Independent States (CIS), Cuba, North Korea, and China. It can also encrypt local and remote file systems via SMB and SFTP.

<https://thehackernews.com/2025/04/ransomhub-went-dark-april-1-affiliates.html>