



DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

20 May 25

Cyber Threat Roundup

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

Contents

| | |
|--|---|
| Articles | 2 |
| Experts Found Rogue Devices, Including Hidden Cellular Radios, in Chinese-made Power Inverters Used Worldwide | 2 |
| Ransomware Gangs Use Skitnet Malware for Stealthy Data Theft and Remote Access | 2 |
| Sarcoma Ransomware Unveiled: Anatomy of a Double Extortion Gang..... | 2 |
| Malicious PyPI Packages Exploit Instagram and TikTok APIs to Validate User Accounts | 2 |
| Beware! A Threat Actor Could Steal the Titles of Your Private (and Draft) WordPress Posts with this New Vulnerability! | 3 |
| Technical Analysis of TransferLoader | 3 |
| CTM360 Identifies Surge in Phishing Attacks Targeting Meta Business Users..... | 3 |

Articles

Experts Found Rogue Devices, Including Hidden Cellular Radios, in Chinese-made Power Inverters Used Worldwide

Investigators found “kill switches” in Chinese-made power inverters in US solar farm equipment. These hidden cellular radios could let Beijing remotely cripple power grids during a conflict. “While inverters are built to allow remote access for updates and maintenance, the utility companies that use them typically install firewalls to prevent direct communication back to China,” reported Reuters. “However, rogue communication devices not listed in product documents have been found in some Chinese solar power inverters by U.S experts who strip down equipment hooked up to grids to check for security issues, the two people said.” The US grid was successfully hacked in November by hackers belonging to foreign governments. Despite the attribution of the attacks is very difficult, security experts believe that Russia, Iran and China were behind the successful breach.

<https://securityaffairs.com/178005/hacking/rogue-devices-in-chinese-made-power-inverters-used-worldwide.html>

Ransomware Gangs Use Skitnet Malware for Stealthy Data Theft and Remote Access

Several ransomware actors are using a malware called Skitnet as part of their post-exploitation efforts to steal sensitive data and establish remote control over compromised hosts. “Skitnet has been sold on underground forums like RAMP since April 2024,” Swiss cybersecurity company PRODAFT told The Hacker News. “However, since early 2025, we have observed multiple ransomware operators using it in real-world attacks.” Skitnet, also called Bossnet, is a multi-stage malware developed by a threat actor tracked by the company under the name LARVA-306. A notable aspect of the malicious tool is that it uses programming languages like Rust and Nim to launch a reverse shell over DNS and evade detection. “Skitnet is a multi-stage malware that leverages multiple programming languages, and encryption techniques,” PRODAFT said. “By using Rust for payload decryption and manual mapping, followed by a Nim-based reverse shell communicating over DNS, the malware tries to evade traditional security measures.”

<https://thehackernews.com/2025/05/ransomware-gangs-use-skitnet-malware.html>

Sarcoma Ransomware Unveiled: Anatomy of a Double Extortion Gang

Sarcoma Ransomware, first detected in October 2024, has rapidly become one of the most active and dangerous ransomware groups. Known for its aggressive tactics, including zero-day exploits and the use of remote monitoring tools, Sarcoma has targeted over 100 victims, mainly in the USA, Italy, Canada, and Australia. High-profile breaches, such as the 40 GB data theft from Smart Media Group Bulgaria, highlight its advanced capabilities. The gang primarily targets high-value companies across various sectors, aiming to cause maximum disruption. In light of this growing threat, the Cybersecurity Observatory of Unipegaso has launched an in-depth investigation to analyze Sarcoma’s methods and support stronger defensive strategies. Experts stress the importance of timely patching, network segmentation, and user awareness to combat such sophisticated threats.

<https://securityaffairs.com/178072/malware/sarcoma-ransomware-unveiled-anatomy-of-a-double-extortion-gang.html>

Malicious PyPI Packages Exploit Instagram and TikTok APIs to Validate User Accounts

Cybersecurity researchers have uncovered malicious packages uploaded to the Python Package Index (PyPI) repository that act as checker tools to validate stolen email addresses against TikTok and Instagram APIs. The

checker-SaGaF package is designed to send HTTP POST requests to TikTok's password recovery API and Instagram's account login endpoints to determine if an email address passed as input is valid, meaning there exists an account holder corresponding to that email address. The second package "steinlurks," in a similar manner, targets Instagram accounts by sending forged HTTP POST requests mimicking the Instagram Android app to evade detection. It achieves this by targeting different API endpoints. "Sinnercore," on the other hand, aims to trigger the forgot password flow for a given username, targeting the API endpoint "b.i.instagram[.]com/api/v1/accounts/send_password_reset/" with fake HTTP requests containing the target's username. Further analysis has determined that the package's backdoor technique using GSocket resembles that of Phoenix Hyena (aka DumpForums or Silent Crow), a hacktivist group known for targeting Russian entities, including Doctor Web, in the aftermath of the Russo-Ukrainian war in early 2022.

<https://thehackernews.com/2025/05/malicious-pypi-packages-exploit.html>

Beware! A Threat Actor Could Steal the Titles of Your Private (and Draft) WordPress Posts with this New Vulnerability!

Imperva discovered and reported a vulnerability potentially affecting all WordPress sites, enabling a threat actor to potentially exfiltrate sensitive private and draft post titles. To protect your site, you're strongly encouraged to update your WordPress site with the latest version and disable the XMLRPC endpoint if you don't use it. We discovered that an attacker could leak the titles of all private or draft posts via a specifically crafted XMLRPC payloads. The attack consists of a series of POST requests sent to the XMLRPC endpoint of the victim's site. According to the way the server responds to the request, the attacker can progressively exfiltrate the titles of private and draft posts.

<https://www.imperva.com/blog/beware-a-threat-actor-could-steal-the-titles-of-your-private-and-draft-wordpress-posts/>

Technical Analysis of TransferLoader

Zscaler ThreatLabz has identified a new malware loader that we have named TransferLoader, which has been active since at least February 2025. ThreatLabz has identified three different components (a downloader, a backdoor, and a specialized loader for the backdoor) embedded in TransferLoader binaries. In addition, ThreatLabz has observed TransferLoader being used to deliver Morpheus ransomware. All components of TransferLoader share similarities including various anti-analysis techniques and code obfuscation. TransferLoader is a new malware loader that has been active since at least February 2025. It includes various embedded components, notably a downloader, a backdoor, and a backdoor loader, all of which employ anti-analysis techniques to evade detection and examination. Based on code similarities and the shared use of evasion methods observed in the binaries, we believe that the developers of TransferLoader are the same as those behind its embedded components. Considering TransferLoader's consistent use in deploying additional payloads including ransomware, we anticipate that threat actors will continue to rely on it in future attacks.

<https://www.zscaler.com/blogs/security-research/technical-analysis-transferloader>

CTM360 Identifies Surge in Phishing Attacks Targeting Meta Business Users

A new global phishing threat called "Meta Mirage" has been uncovered, targeting businesses using Meta's Business Suite. This campaign specifically aims at hijacking high-value accounts, including those managing advertising and official brand pages. Cybersecurity researchers at CTM360 revealed that attackers behind Meta Mirage impersonate official Meta communications, tricking users into handing over sensitive details like passwords and security codes (OTP). Cybercriminals cleverly hosted fake pages leveraging trusted cloud platforms like GitHub, Firebase, and Vercel, making it harder to spot the scams. This method aligns closely with recent findings

from Microsoft, which highlighted similar abuse of cloud hosting services to compromise Kubernetes applications, emphasizing how attackers frequently leverage trusted platforms to evade detection. CTM360's report also outlines a structured and calculated approach used by the attackers to maximize effectiveness. Victims are initially contacted with mild, non-alarming notifications that progressively escalate in urgency and severity. Initial notices might mention generic policy violations, while subsequent messages warn of immediate suspensions or permanent deletion of accounts. This incremental escalation induces anxiety and urgency, driving users to act quickly without thoroughly verifying the authenticity of these messages.

<https://thehackernews.com/2025/05/ctm360-identifies-surge-in-phishing.html>