



# DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

17 Mar 25

## Cyber Threat Roundup

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

### Contents

Articles .....	2
Researchers Expose New Polymorphic Attack That Clones Browser Extensions to Steal Credentials.....	2
Desert Dexter Targets 900 Victims Using Facebook Ads and Telegram Malware Links.....	2
Moxa Issues Fix for Critical Authentication Bypass Vulnerability in PT Switches.....	2
SideWinder APT Targets Maritime, Nuclear, and IT Sectors Across Asia, Middle East, and Africa .....	3
Ballista Botnet Exploits Unpatched TP-Link Vulnerability, Infects Over 6,000 Devices.....	3
Over 400 IPs Exploiting Multiple SSRF Vulnerabilities in Coordinated Cyber Attack .....	3
Mozilla Warns Users to Update Firefox Before Certificate Expires .....	3
CISA: Medusa Ransomware Hit Over 300 Critical Infrastructure Orgs .....	4
North Korea's ScarCruft Deploys KoSpy Malware, Spying on Android Users via Fake Utility Apps.....	4
Malicious PyPI Packages Stole Cloud Tokens—Over 14,100 Downloads Before Removal.....	4

## Articles

### **Researchers Expose New Polymorphic Attack That Clones Browser Extensions to Steal Credentials**

Cybersecurity researchers have demonstrated a novel technique that allows a malicious web browser extension to impersonate any installed add-on. The polymorphic extensions create a pixel perfect replica of the target's icon, HTML popup, workflows and even temporarily disables the legitimate extension, making it extremely convincing for victims to believe that they are providing credentials to the real extension. The harvested credentials could then be abused by the threat actors to hijack online accounts and gain unauthorized access to sensitive personal and financial information. The attack affects all Chromium-based web browsers, including Google Chrome, Microsoft Edge, Brave, Opera, and others. Once a suitable target extension is identified, the attack moves to the next stage, causing it to morph into a replica of the legitimate extension. This is accomplished by changing the rogue extension's icon to match that of the target and temporarily disabling the actual add-on via the "chrome.management" API, which leads to it being removed from the toolbar.

<https://thehackernews.com/2025/03/researchers-expose-new-polymorphic.html>

### **Desert Dexter Targets 900 Victims Using Facebook Ads and Telegram Malware Links**

The Middle East and North Africa have become the target of a new campaign that delivers a modified version of a known malware called AsyncRAT since September 2024. The campaign, which leverages social media to distribute malware, is tied to the region's current geopolitical climate. The attackers host malware in legitimate online file-sharing accounts or Telegram channels set up specially for this purpose. The campaign is estimated to have claimed approximately 900 victims since the fall 2024, the Russian cybersecurity company added, indicating its widespread nature. A majority of the victims are located in Libya, Saudi Arabia, Egypt, Turkey, the United Arab Emirates, Qatar, and Tunisia. The activity, attributed to a threat actor dubbed Desert Dexter, was discovered in February 2025. It chiefly involves creating temporary accounts and news channels on Facebook. These accounts are then used to publish advertisements containing links to a file-sharing service or Telegram channel.

<https://thehackernews.com/2025/03/desert-dexter-targets-900-victims-using.html>

### **Moxa Issues Fix for Critical Authentication Bypass Vulnerability in PT Switches**

Cybersecurity researchers Taiwanese company Moxa has released a security update to address a critical security flaw impacting its PT switches that could permit an attacker to bypass authentication guarantees. The vulnerability, tracked as CVE-2024-12297, has been assigned a CVSS v4 score of 9.2 out of a maximum of 10.0. Multiple Moxa PT switches are vulnerable to an authentication bypass because of flaws in their authorization mechanism," the company said in an advisory released last week. Despite client-side and back-end server verification, attackers can exploit weaknesses in its implementation. This vulnerability may enable brute-force attacks to guess valid credentials or MD5 collision attacks to forge authentication hashes, potentially compromising the security of the device. Successful exploitation of the shortcoming, in other words, could lead to an authentication bypass and allow an attacker to gain unauthorized access to sensitive configurations or disrupt services.

<https://thehackernews.com/2025/03/moxa-issues-fix-for-critical.html>

## **SideWinder APT Targets Maritime, Nuclear, and IT Sectors Across Asia, Middle East, and Africa**

Maritime and logistics companies in South and Southeast Asia, the Middle East, and Africa have become the target of an advanced persistent threat (APT) group dubbed SideWinder. The attacks, observed by Kaspersky in 2024, spread across Bangladesh, Cambodia, Djibouti, Egypt, the United Arab Emirates, and Vietnam. Other targets of interest include nuclear power plants and nuclear energy infrastructure in South Asia and Africa, as well as telecommunication, consulting, IT service companies, real estate agencies, and hotels. SideWinder was previously the subject of an extensive analysis by the Russian cybersecurity company in October 2024, documenting the threat actor's use of a modular post-exploitation toolkit called StealerBot to capture a wide range of sensitive information from compromised hosts.

<https://thehackernews.com/2025/03/sidewinder-apt-targets-maritime-nuclear.html>

## **Ballista Botnet Exploits Unpatched TP-Link Vulnerability, Infects Over 6,000 Devices**

Lotus Unpatched TP-Link Archer routers have become the target of a new botnet campaign dubbed Ballista, according to new findings from the Cato CTRL team. The botnet exploits a remote code execution (RCE) vulnerability in TP-Link Archer routers (CVE-2023-1389) to spread itself automatically over the Internet. CVE-2023-1389 is a high-severity security flaw impacting TP-Link Archer AX-21 routers that could lead to command injection, which could then pave the way for remote code execution. The attack sequence entails the use of a malware dropper, a shell script ("dropbpb.sh") that's designed to fetch and execute the main binary on the target system for various system architectures such as mips, mipsel, armv5l, armv7l, and x86\_64. Once executed, the malware establishes an encrypted command-and-control (C2) channel on port 82 in order to take control of the device. This allows running shell commands to conduct further RCE and denial-of-service (DoS) attacks. In addition, the malware attempts to read sensitive files on the local system.

<https://thehackernews.com/2025/03/ballista-botnet-exploits-unpatched-tp.html>

## **Over 400 IPs Exploiting Multiple SSRF Vulnerabilities in Coordinated Cyber Attack**

Threat intelligence firm GreyNoise is warning of a "coordinated surge" in the exploitation of Server-Side Request Forgery (SSRF) vulnerabilities spanning multiple platforms. At least 400 IPs have been seen actively exploiting multiple SSRF CVEs simultaneously, with notable overlap between attack attempts," the company said, adding it observed the activity on March 9, 2025. The countries which have emerged as the target of SSRF exploitation attempts include the United States, Germany, Singapore, India, Lithuania, and Japan. Another notable country is Israel, which has witnessed a surge on March 11, 2025. GreyNoise said that many of the same IP addresses are targeting multiple SSRF flaws at once rather than focusing on one particular weakness, noting the pattern of activity suggests structured exploitation, automation, or pre-compromise intelligence gathering. Many modern cloud services rely on internal metadata APIs, which SSRF can access if exploited. SSRF can be used to map internal networks, locate vulnerable services, and steal cloud credentials.

<https://thehackernews.com/2025/03/over-400-ips-exploiting-multiple-ssrf.html>

## **Mozilla Warns Users to Update Firefox Before Certificate Expires**

Mozilla is warning Firefox users to update their browsers to the latest version to avoid facing disruption and security risks caused by the upcoming expiration of one of the company's root certificates. The Mozilla certificate is set to expire this Friday, March 14, 2025, and was used to sign content, including add-ons for various Mozilla projects and Firefox itself. Users need to update their browsers to Firefox 128 (released in July 2024) or later and ESR 115.13 or

later for 'Extended Support Release' (ESR) users. On 14 March a root certificate (the resource used to prove an add-on was approved by Mozilla) will expire, meaning Firefox users on versions older than 128 (or ESR 115) will not be able to use their add-ons. Users are recommended to check and confirm they're running Firefox version 128 and later via Menu > Help > About Firefox. This action should also automatically trigger a check for updates. It is noted that the problem impacts Firefox on all platforms, including Windows, Android, Linux, and macOS, except for iOS, where there's an independent root certificate management system.

<https://www.bleepingcomputer.com/news/software/mozilla-warns-users-to-update-firefox-before-certificate-expires/>

### **CISA: Medusa Ransomware Hit Over 300 Critical Infrastructure Orgs**

CISA says the Medusa ransomware operation has impacted over 300 organizations in critical infrastructure sectors in the United States until last month. This was revealed in a joint advisory issued today in coordination with the Federal Bureau of Investigation (FBI) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). As of February 2025, Medusa developers and affiliates have impacted over 300 victims from a variety of critical infrastructure sectors with affected industries including medical, education, legal, insurance, technology, and manufacturing. As the advisory explains, to defend against Medusa ransomware attacks, defenders are advised to take the following measures. Mitigate known security vulnerabilities to ensure operating systems, software, and firmware are patched within a reasonable timeframe. Segment networks to limit lateral movement between infected devices and other devices within the organization, and filter network traffic by blocking access from unknown or untrusted origins to remote services on internal systems.

<https://www.bleepingcomputer.com/news/security/cisa-medusa-ransomware-hit-over-300-critical-infrastructure-orgs/>

### **North Korea's ScarCruft Deploys KoSpy Malware, Spying on Android Users via Fake Utility Apps**

The North Korea-linked threat actor known as ScarCruft is said to have been behind a never-before-seen Android surveillance tool named KoSpy targeting Korean and English-speaking users. KoSpy can collect extensive data, such as SMS messages, call logs, location, files, audio, and screenshots via dynamically loaded plugins. The malicious artifacts masquerade as utility applications on the official Google Play Store, using the names File Manager, Phone Manager, Smart Manager, Software Update Utility, and Kakao Security to trick unsuspecting users into infecting their own devices. ScarCruft, also called APT27 and Reaper, is a North Korean state-sponsored cyber espionage group active since 2012. Attack chains orchestrated by the group primarily leverage RokRAT as a means to harvest sensitive data from Windows systems. RokRAT has since been adapted to target macOS and Android. The malicious Android apps, once installed, are engineered to contact a Firebase Firestore cloud database to retrieve a configuration containing the actual command-and-control (C2) server address.

<https://thehackernews.com/2025/03/north-koreas-scarcruft-deploys-kospy.html>

### **Malicious PyPI Packages Stole Cloud Tokens—Over 14,100 Downloads Before Removal**

Cybersecurity researchers have warned of a malicious campaign targeting users of the Python Package Index (PyPI) repository with bogus libraries masquerading as "time" related utilities, but harboring hidden functionality to steal sensitive data such as cloud access tokens. Software supply chain security firm ReversingLabs said it discovered two sets of packages totaling 20 of them. The packages have been cumulatively downloaded over 14,100 times. While the first set relates to packages that are used to upload data to the threat actor's infrastructure, the second cluster consists of packages implementing cloud client functionalities for several services like Alibaba Cloud, Amazon Web Services, and Tencent Cloud. The disclosure comes as Fortinet FortiGuard Labs said it

discovered thousands of packages across PyPI and npm, some of which have been found to embed suspicious install scripts designed to deploy malicious code during installation or communicate with external servers. Suspicious URLs are a key indicator of potentially malicious packages, as they are often used to download additional payloads or establish communication with command-and-control (C&C) servers, giving attackers control over infected systems

<https://thehackernews.com/2025/03/malicious-pypi-packages-stole-cloud.html>