A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

1 Apr 25

Cyber Threat Roundup

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

Contents

Articles

Morphing Meerkat Phishing Kits Exploit DNS MX Records

Infoblox researchers discovered a new phishing-as-a-service (PhaaS) platform that generated multiple phishing kits, called Morphing Meerkat, using DNS mail exchange (MX) records to deliver fake login pages and targeting over 100 brands. Threat actors are exploiting DNS techniques to enhance phishing attacks, using MX records to dynamically serve spoofed login pages. They also abuse open redirects, compromised domains, and distribute stolen credentials via Telegram. The phishing-as-a-service (PhaaS) platform behind Morphing Meerkat kits has been active for at least five years. It consistently employs the same tactics and core resources, yet its use of MX records for phishing has remained largely unreported. Morphing Meerkat enables large-scale phishing and spam campaigns, it uses compromised WordPress sites, open redirects, and MX records to tailor fake login pages. The platform bypasses security with obfuscated code, dynamic translations, and redirects suspicious users to real sites. Stolen credentials are distributed via email and chat.

https://securityaffairs.com/176029/cyber-crime/morphing-meerkat-phishing-kits-exploit-dns-mx.html

CISA Warns of RESURGE Malware Exploiting Ivanti Flaw

RESURGE supports the capabilities of the SPAWNCHIMERA malware, however, it implements distinctive commands that alter its behavior. The malware creates web shells, bypasses integrity checks, and modifies files. RESURGE enables credential harvesting, account creation, and privilege escalation, copying web shells to Ivanti's boot disk and manipulating the coreboot image for persistence. CISA identifies “libdsupgrade.so”, aka RESURGE, as a malicious Linux shared object file on Ivanti ICS devices. It acts as a rootkit, dropper, backdoor, bootkit, proxy, and tunneler. RESURGE modifies files, manipulates integrity checks, and installs a persistent web shell. It creates secure tunnels for threat actors via SSH, proxies, and encrypted keys, enabling covert system access.

https://securityaffairs.com/176040/breaking-news/cisa-warns-of-resurge-malware-exploiting-ivanti-flaw.html

BlackLock Ransomware Exposed After Researchers Exploit Leak Site Vulnerability

Resecurity said it identified a security vulnerability in the data leak site (DLS) operated by the e-crime group that made it possible to extract configuration files, credentials, as well as the history of commands executed on the server. BlackLock is a rebranded version of another ransomware group known as Eldorado. It has since become one of the most active extortion syndicates in 2025, heavily targeting technology, manufacturing, construction, finance, and retail sectors. As of last month, it has listed 46 victims on its site. The impacted organizations are located in Argentina, Aruba, Brazil, Canada, Congo, Croatia, Peru, France, Italy, the Netherlands, Spain, the United Arab Emirates, the United Kingdom, and the United States. The vulnerability identified by Resecurity is a local file inclusion (LFI) bug, essentially tricking the web server into leaking sensitive information by performing a path traversal attack, including the history of commands executed by the operators on the leak site.

https://thehackernews.com/2025/03/blacklock-ransomware-exposed-after.html

Nine-Year-Old npm Packages Hijacked to Exfiltrate API Keys via Obfuscated Scripts

Cybersecurity researchers have discovered several cryptocurrency packages on the npm registry that have been hijacked to siphon sensitive information such as environment variables from compromised systems. Analysis of these packages by the software supply chain security firm has revealed that they have been poisoned with heavily obfuscated code in two different scripts: "package/scripts/launch.js" and "package/scripts/diagnostic-report.js." The

JavaScript code, which run immediately after the packages are installed, are designed to harvest sensitive data such as API keys, access tokens, SSH keys, and exfiltrate them to a remote server. The findings underscore the need for securing accounts with two-factor authentication (2FA) to prevent takeover attacks. They also highlight the challenges associated with enforcing such security safeguards when open-source projects reach end-of-life or are no longer actively maintained.

https://thehackernews.com/2025/03/nine-year-old-npm-packages-hijacked-to.html

A Vulnerability in CrushFTP Could Allow for Unauthorized Access

A vulnerability has been discovered in CrushFTP, which could allow for unauthorized access. CrushFTP is a proprietary multi-protocol, multi-platform file transfer server. The vulnerability is mitigated if the DMZ feature of CrushFTP is in place. Successful exploitation of this vulnerability could allow an attacker to remotely control the compromised server and execute remote code. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

https://www.cisecurity.org/advisory/a-vulnerability-in-crushftp-could-allow-for-unauthorized-access_2025-032

Splunk Patches Dozens of Vulnerabilities

Tracked as CVE-2025-20229 (CVSS score of 8.0), the security defect is caused by a missing authorization check, and has been addressed with the release of Splunk Enterprise versions 9.4.0, 9.3.3, 9.2.5, and 9.1.8, and Splunk Cloud Platform versions 9.3.2408.104, 9.2.2406.108, 9.2.2403.114, and 9.1.2312.208. Splunk also announced fixes for medium-severity security defects in Splunk Enterprise that could lead to maintenance mode modifications, safeguard bypass, information disclosure, and manipulation of other user data. Splunk makes no mention of any of these vulnerabilities being exploited in the wild. However, users are advised to update their Splunk Enterprise instances and other affected Splunk applications as soon as possible.

https://www.securityweek.com/splunk-patches-dozens-of-vulnerabilities/

Arkana Security Group Claims the Hack of US Telco Provider WideOpenWest (WOW!)

The new ransomware group Arkana Security claims to have hacked US telecom provider WOW!, stealing customer data. WideOpenWest (WOW!) is a US-based telecommunications company that provides broadband internet, cable TV, and phone services. It operates mainly in the Midwest and Southeast regions, serving residential and business customers. WOW! is known for offering high-speed internet and competitive pricing in markets where it competes with larger providers. The Arkana group recently appeared in the threat landscape, claiming to perform post-pentest services, and offering data security, and risk management services. The ransomware group steals victims' data to pressure them into paying a "generous fee." Arkana claims to have stolen two databases, respectively containing data of 403,000 and 2.2 million accounts. Compromised data includes usernames, passwords, security details, emails, and Firebase integration data. Arkana claimed to have breached WOW!'s internal systems, including AppianCloud and Symphonica platforms.

https://securityaffairs.com/175905/data-breach/arkana-security-group-claims-the-hack-of-wideopenwest-wow.html

Oracle Cloud Data Breach: Six Million Records Stolen, 140,000 Clients Potentially Impacted

Though it is still early in 2025, a recent hack of Oracle Cloud is thus far one of the year's biggest data breaches with six million records stolen by attackers and around 140,000 tenants impacted. The data breach was uncovered by researchers with security firm CloudSEK, who came across dark web listings on March 21 that advertised some six million records purportedly stolen from Oracle Cloud. The threat actor, going by “rose87168,” claimed to have compromised subdomain “login.us2.oraclecloud.com” and exfiltrated the records from its Single Sign-On (SSO) and Lightweight Directory Access (LDAP) protocols. That subdomain has since been taken offline by Oracle. Oracle has issued statements to the media claiming that Oracle Cloud was never breached, but has yet to specifically respond to seemingly convincing proof that the threat actors posted (in the form of internal LDAP information, database samples and a client list as well as a URL sent to journalists by the attackers that was created on the compromised subdomain). CloudSEK has since followed up with a “deep dive” report that presents more detailed evidence of the data breach.

https://www.cpomagazine.com/cyber-security/oracle-cloud-data-breach-six-million-records-stolen-140000-clients-potentially-impacted/