A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

2 Jun 25

Cyber Threat Roundup

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

Contents

Articles

Microsoft: Windows 11 Might Fail to Start After Installing KB5058405

Microsoft confirmed some Windows 11 systems might fail to start after installing the KB5058405 cumulative update released during this month's Patch Tuesday. On affected devices, users see 0xc0000098 recovery errors in ACPI.sys, warning that the device has to be repaired because the operating system couldn't be loaded. ACPI.sys is the Windows Advanced Configuration and Power Interface (ACPI) driver, a kernel-mode driver critical for power management and device configuration on Windows with an ACPI BIOS. "Your PC/Device needs to be repaired. The operating system couldn't be loaded because a required file is missing or contains errors," the error warns. This issue impacts Windows 11 22H2/23H2 systems in enterprise environments and mainly affects Azure Virtual Machines, Azure Virtual Desktop, and on-premises virtual machines hosted on Citrix or Hyper-V.

https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-11-might-fail-to-start-after-installing-kb5058405/

China-Linked Hackers Exploit SAP and SQL Server Flaws in Attacks Across Asia and Brazil

The China-linked threat actor behind the recent in-the-wild exploitation of a critical security flaw in SAP NetWeaver has been attributed to a broader set of attacks targeting organizations in Brazil, India, and Southeast Asia since 2023. "The threat actor mainly targets the SQL injection vulnerabilities discovered on web applications to access the SQL servers of targeted organizations," Trend Micro security researcher Joseph C Chen said in an analysis published this week. "The actor also takes advantage of various known vulnerabilities to exploit public-facing servers." Some of the other prominent targets of the adversarial collective include Indonesia, Malaysia, the Philippines, Thailand, and Vietnam. The cybersecurity company is tracking the activity under the moniker Earth Lamia, stating the activity shares some degree of overlap with threat clusters documented by Elastic Security Labs as REF0657, Sophos as STAC6451, and Palo Alto Networks Unit 42 as CL-STA-0048.

https://thehackernews.com/2025/05/china-linked-hackers-exploit-sap-and.html

Websites Selling Hacking Tools to Cybercriminals Seized

A coordinated effort involving an international disruption of an online software crypting syndicate which provides services to cybercriminals to assist them with keeping their malicious software (malware) from being detected has resulted in the seizure of four domains and their associated server, announced U.S. Attorney Nicholas J. Ganjei. Crypting is the process of using software to make malware difficult for antivirus programs to detect. The seized domains offered services to cybercriminals, including counter-antivirus (CAV) tools. When used together, CAV and crypting services allow criminals to obfuscate malware, making it undetectable and enabling unauthorized access to computer systems. According to the affidavit filed in support of these seizures, authorities made undercover purchases from seized websites and analyzed the services, confirming they were designed for cybercrime. Court documents also allege authorities reviewed linked email addresses and other data connecting the services to known ransomware groups that have targeted victims both in the United States and abroad, including in the Houston area.

https://www.justice.gov/usao-sdtx/pr/websites-selling-hacking-tools-cybercriminals-seized

Cybercriminals Target AI Users with Malware-Loaded Installers Posing as Popular Tools

Fake installers for popular artificial intelligence (AI) tools like OpenAI ChatGPT and InVideo AI are used as lures to propagate various threats, such as the CyberLock and Lucky_Gh0$t ransomware families, and a new malware dubbed Numero. "CyberLock ransomware, developed using PowerShell, primarily focuses on encrypting specific files on the victim's system," Cisco Talos researcher Chetan Raghuprasad said in a report published today. "Lucky_Gh0$t ransomware is yet another variant of the Yashma ransomware, which is the sixth iteration of the Chaos ransomware series, featuring only minor modifications to the ransomware binary." Numero, on the other hand, is a destructive malware that impacts victims by manipulating the graphical user interface (GUI) components of their Windows operating system, thereby rendering the machines unusable. The cybersecurity company said the legitimate versions of the AI tools are popular in the business-to-business (B2B) sales domain and the marketing sector, suggesting that individuals and organizations in these industries are the primary focus of the threat actors behind the campaign.

https://thehackernews.com/2025/05/cybercriminals-target-ai-users-with.html

Microsoft OneDrive File Picker Flaw Grants Apps Full Cloud Access

Cybersecurity researchers discovered a security flaw in Microsoft's OneDrive File Picker that, if successfully exploited, could allow websites to access a user's entire cloud storage content, as opposed to just the files selected for upload via the tool. "This stems from overly broad OAuth scopes and misleading consent screens that fail to clearly explain the extent of access being granted," the Oasis Research Team said in a report shared with The Hacker News. "This flaw could have severe consequences, including customer data leakage and violation of compliance regulations." It's assessed that several apps are affected, such as ChatGPT, Slack, Trello, and ClickUp, given their integration with Microsoft's cloud service. The problem, Oasis said, is the result of excessive permissions requested by the OneDrive File Picker, which seeks read access to the entire drive, even in cases only a single file is uploaded due to the absence of fine-grained OAuth scopes for OneDrive. Compounding matters further, the consent prompt users are presented with prior to a file upload is vague and does not adequately convey the level of access being granted, thereby exposing users to unexpected security risks.

https://thehackernews.com/2025/05/microsoft-onedrive-file-picker-flaw.html

Microsoft Authenticator Now Warns to Export Passwords Before July Cutoff

The Microsoft Authenticator app is now issuing notifications warning that the password autofill feature is being deprecated in July, suggesting users move to Microsoft Edge instead. Microsoft Authenticator is a free mobile authenticator app that provides secure sign-in for mobile accounts using multi-factor authentication (MFA) methods like time-based one-time passwords (TOTPs), push notifications, biometrics-based confirmations, and password-less logins to Microsoft accounts. Earlier this month, BleepingComputer reported about the upcoming deprecation, which warned that users had until August 1 to export their passwords before they become unavailable in the app. Today, the Microsoft Authenticator app began issuing notifications about the upcoming changes, showing a fullscreen banner warning to export saved passwords before July 1 or switch to Microsoft Edge.

https://www.bleepingcomputer.com/news/security/microsoft-authenticator-now-warns-to-export-passwords-before-july-cutoff/

Threat Actors Abuse Google Apps Script in Evasive Phishing Attacks

Threat actors are abusing the ‘Google Apps Script’ development platform to host phishing pages that appear legitimate and steal login credentials. This new trend was spotted by security researchers at Cofense, who warn that the fraudulent login window is "carefully designed to look like a legitimate login screen.The attack uses an email masquerading as an invoice, containing a link to a webpage that uses Google Apps Script, a development platform integrated across Google's suite of products," Cofense explains. Google Apps Script is a JavaScript-based cloud scripting platform from Google that allows users to automate tasks and extend the functionality of Google Workspace products like Google Sheets, Docs, Drive, Gmail, and Calendar. Attackers write a Google Apps Script that displays a fake login page to capture the credentials victims enter. The data is exfiltrated to the attacker's server via a hidden request.

https://www.bleepingcomputer.com/news/security/threat-actors-abuse-google-apps-script-in-evasive-phishing-attacks/