A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

29 Jul 22

Cyber Threat Roundup

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

Contents

Articles

Moxa NPort Device Flaws Can Expose Critical Infrastructure to Disruptive Attacks

The vulnerabilities can be exploited by a remote attacker to cause the targeted device to enter a denial of service (DoS) condition. Exploitation of both vulnerabilities requires just a network connection to the targeted device.

https://www.securityweek.com/moxa-nport-device-flaws-can-expose-critical-infrastructure-disruptive-attacks?&web_view=true

APT-Like Phishing Threat Mirrors Landing Pages

A phishing campaign is underway that uses mirror images of target organizations' landing pages to trick victims into entering login credentials. From there, the phishing page will either request the email twice as validation or use the credentials in real time in order to verify the password.

https://www.darkreading.com/endpoint/apt-phishing-mirrors-landing-pages-credential-harvesting

Threat Actors Use New Attack Techniques After Microsoft Blocked Macros by Default

Threat actors are devising new attack tactics in response to Microsoft's decision to block macros by default. In response to Microsoft's decision steps to block Excel 4.0 (XLM or XL4) and Visual Basic for Applications (VBA) macros by default in Microsoft Office applications, threat actors are adopting new attack techniques.

https://securityaffairs.co/wordpress/133764/hacking/attacks-after-microsoft-blocked-macros.html

Cyberspies Use Google Chrome Extension to Steal Emails Undetected

A North Korean-backed threat group tracked as "Kimsuky" is using a malicious browser extension to steal emails from Google Chrome or Microsoft Edge users reading their webmail. The extension, dubbed "SHARPEXT" by Volexity researchers who spotted this campaign in September, supports three Chromium-based web browsers (Chrome, Edge, and Whale) and can steal mail from Gmail and AOL accounts.

https://www.bleepingcomputer.com/news/security/cyberspies-use-google-chrome-extension-to-steal-emails-undetected/

Austrian Hackers-for-Hire Knotweed Serve Up Subzero Malware

The Austrian group KNOTWEED spreads malware via Microsoft products, new malware-infested apps pop up in the Google Play store, and more. Microsoft's Security Response Center dubbed the group "KNOTWEED", and stated their belief that the group developed the Subzero malware, used in these various attacks against the company's customers.

https://securityboulevard.com/2022/07/the-week-in-cybersecurity-austrian-hackers-for-hire-knotweed-serve-up-subzero-malware/

Ransom Payments Fall as Fewer Victims Choose to Pay Hackers

In Q2 2022, the average ransom payment was $228,125 (up by 8% from Q1 ’22). However, the median ransom payment was $36,360, a steep fall of 51% compared to the previous quarter.

https://www.bleepingcomputer.com/news/security/ransom-payments-fall-as-fewer-victims-choose-to-pay-hackers

Patch Now: Atlassian Confluence Bug Under Active Exploit

A critical Atlassian Confluence vulnerability that was disclosed last week is now being actively exploited in the wild, researchers are warning. Admins should note: the bug only exists when the “Questions for Confluence” app is enabled, and it does not impact the Confluence Cloud instance.

https://www.darkreading.com/cloud/patch-now-atlassian-confluence-bug-active-exploit