A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

9 Sep 22

Cyber Threat Roundup

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

Contents

Articles

CISA Orders Agencies to Patch Chrome, D-Link Flaws Used in Attacks

CISA has added 12 more security flaws to its list of bugs exploited in attacks, including two critical D-Link vulnerabilities and two (now-patched) zero-days in Google Chrome and the Photo Station QNAP software. Last but not least, the two critical D-Link security flaws (CVE-2022-28958 and CVE-2022-26258) are being targeted by the Mirai-based MooBot botnet to gain remote code execution and take over unpatched devices.

https://www.bleepingcomputer.com/news/security/cisa-orders-agencies-to-patch-chrome-d-link-flaws-used-in-attacks/

Ex-Members of the Conti Ransomware Gang Target Ukraine

Some members of the Conti ransomware gang were involved in financially motivated attacks targeting Ukraine from April to August 2022. Researchers from Google's Threat Analysis Group (TAG) reported that some former members of the Conti cybercrime group were involved in five different campaigns targeting Ukraine between April and August 2022.

https://securityaffairs.co/wordpress/135447/cyber-crime/conti-ransomware-members-target-ukraine.html

Microsoft: Iranian Hackers Encrypt Windows Systems Using BitLocker

Microsoft says an Iranian state-sponsored threat group it tracks as DEV-0270, also known as "Nemesis Kitten", has been abusing the BitLocker Windows feature in attacks to encrypt victims' systems. Microsoft has seen DEV-0270 using BitLocker, a data protection feature that provides full-volume encryption on devices running Windows 10, Windows 11, or Windows Server 2016 and above. DEV-0270 has been seen using setup.bat commands to enable BitLocker encryption, which leads to the hosts becoming inoperable.

https://www.bleepingcomputer.com/news/microsoft/microsoft-iranian-hackers-encrypt-windows-systems-using-bitlocker/

New Mirai Botnet Variant Detection: MooBot Sample Targets D-Link Routers

Security researchers are raising the alarm on a new Mirai botnet variant dubbed "MooBot" that targets D-Link devices. MooBot first surfaced in 2019, hijacking LILIN digital video recorders and Hikvision video surveillance products and co-opting them into a family of denial-of-service bots.

https://socprime.com/blog/new-mirai-botnet-variant-detection-moobot-sample-targets-d-link-routers/

Warning Issued About Vice Society Ransomware Gang

A ransomware gang that has been increasingly disproportionately targeting the education sector is the subject of a joint warning issued by the FBI, CISA, and MS-ISAC. The "Vice Society" ransomware group has been breaking into schools and colleges, exfiltrating sensitive data, and demanding ransom payments.

https://www.tripwire.com/state-of-security/security-data-protection/warning-issued-vice-society-ransomware-gang/

Threat Actors Exploiting Dormant Accounts to Bypass MFA

Security researchers have witnessed APT29 (“Cozy Bear”) targeting dormant Microsoft accounts in hopes of being the first available to enroll it within multi-factor authentication (MFA). APT29 gathered a list of accounts from one organization and was able to figure out the password of an account that was configured, but never used. This allowed the group to configure MFA the first time they logged in with the stolen account.

https://securityboulevard.com/2022/09/threat-actors-exploiting-dormant-accounts-to-bypass-mfa-what-you-need-to-know/