DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

3 Mar 25

Cyber Threat Roundup

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

Contents

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

Articles

Qilin Ransomware Gang Claimed Responsibility for the Lee Enterprises Attack

The Qilin ransomware group claimed responsibility for the recent cyberattack on Lee Enterprises, which impacted dozens of local newspapers. Lee Enterprises, Inc. is a publicly traded American media company. It publishes 79 newspapers in 25 states, and more than 350 weekly, classified, and specialty publications. The company reported to the SEC that a Feb. 3 cyberattack led to unauthorized access, file withdrawals, and encryption of critical applications. At least 79 newspapers faced publication disruptions, subscriber access issues, and disabled newsroom phones. After the cyber attack, many sites displayed maintenance notices.

https://securityaffairs.com/174831/data-breach/qilin-ransomware-group-claims-responsibility-lee-enterprises-attack.html

Ransomware Gangs Exploit a Paragon Partition Manager BioNTdrv.sys Driver Zero-Day

Microsoft discovered five vulnerabilities in the Paragon Partition Manager BioNTdrv.sys driver. The IT giant reported that one of these flaws is exploited by ransomware groups in zero-day attacks. Paragon Partition Manager, available in Community and Commercial versions, manages hard drive partitions using the BioNTdrv.sys driver. This kernel-level driver enables low-level access with elevated privileges for data management. The researchers discovered five vulnerabilities in Paragon Partition Manager's BioNTdrv.sys driver, versions before 2.0.0. The flaws include arbitrary kernel memory mapping and write vulnerabilities, a null pointer dereference, insecure kernel resource access, and an arbitrary memory move vulnerability.

https://securityaffairs.com/174789/cyber-crime/ransomware-gangs-paragon-partition-manager-biontdrv-sys-driver-zero-day-attacks.html

US Seizes $31 Million Worth of Crypto Stolen in Uranium Finance Hack

Last week, the US government announced that it seized roughly $31 million worth of cryptocurrency stolen in April 2021 from Uranium Finance. Uranium Finance was hacked twice in April 2021, with the total losses amounting to over $53 million, making it one of the largest hacks in decentralized finance (DeFi) at the time. According to blockchain intelligence firm TRM Labs, which investigated the transactions linked to the heist and helped authorities trace the stolen funds, the attackers exploited vulnerabilities in Uranium Finance's smart contract code to steal various tokens.

https://www.securityweek.com/us-seizes-31-million-worth-of-crypto-stolen-in-uranium-finance-hack/

Black Basta Leak Offers Glimpse Into Group's Inner Workings

A massive hoard of internal chats has been leaked from the Black Basta ransomware group, rivalling the Conti leaks of late February 2022. A 47 Mb JSON file of internal Black Basta chat logs was leaked by an actor named ExploitWhispers on February 11, 2025. Its existence did not become general knowledge until February 20, when the threat intelligence firm Prodaft posted brief details.The post included a note from ExploitWhispers, written in Russian, suggesting the leak happened because Black Basta had 'hacked domestic banks' (that is, Russian banks) and in doing so they had crossed the line. Prodaft also suggested that Black Basta has been largely inactive since the beginning of the year 'due to internal conflicts'.

https://www.securityweek.com/black-basta-leak-offers-glimpse-into-groups-inner-workings/

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   🐦 @DC3DCISE · @DC3Forensics   🔗 DC3 Cyber Crime Center

2

Vo1d Botnet's Peak Surpasses 1.59M Infected Android TVs, Spanning 226 Countries

Brazil, South Africa, Indonesia, Argentina, and Thailand have become the targets of a campaign that has infected Android TV devices with a botnet malware dubbed Vo1d. The improved variant of Vo1d has been found to encompass 800,000 daily active IP addresses, with the botnet scaling a peak of 1,590,299 on January 19, 2025, spanning 226 countries and regions. As of February 25, 2025, India has experienced a notable surge in infection rate, increasing from less than 1% (3,901) to 18.17% (217,771). "Vo1d has evolved to enhance its stealth, resilience, and anti-detection capabilities," QiAnXin XLab said. "RSA encryption secures network communication, preventing [command-and-control] takeover even if [the Domain Generation Algorithm] domains are registered by researchers. Each payload uses a unique Downloader, with XXTEA encryption and RSA-protected keys, making analysis harder."

https://thehackernews.com/2025/03/vo1d-botnets-peak-surpasses-159m.html

DoD CYBER CRIME CENTER

DC3.DCISE@us.af.mil   410-981-0104 | www.dc3.mil | DC3.Information@us.af.mil   @DC3DCISE · @DC3Forensics   DC3 Cyber Crime Center

3