A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

DoD—Defense Industrial Base Collaborative Information Sharing Environment

12 May 25

Cyber Threat Roundup

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

Contents

Articles

Russia-Linked Coldriver Used LOSTKEYS Malware in Recent Attacks

Google's Threat Intelligence Group discovered LOSTKEYS, a new malware used by Russia-linked APT COLDRIVER, in recent attacks to steal files and gather system info. The ColdRiver APT (aka "Seaborgium", "Callisto", "Star Blizzard", "TA446") is a Russian cyberespionage group that targets government officials, military personnel, journalists and think tanks since at least 2015. COLDRIVER targets high-profile individuals and NGOs to steal credentials, emails, and contacts. They also deploy malware for file access. Recent victims include Western advisors, journalists, and Ukraine-linked individuals. Their main goal is intelligence gathering for Russian interests, with occasional hack-and-leak operations. LOSTKEYS is deployed via a multi-step chain starting with a fake CAPTCHA that tricks users into running PowerShell. This "ClickFix" method, used by COLDRIVER and others, fetches staged payloads from remote servers.

https://securityaffairs.com/177638/apt/russia-linked-coldriver-used-lostkeys-malware-in-recent-attacks.html

FBI: End-Of-Life Routers Hacked for Cybercrime Proxy Networks

The FBI warns that threat actors deploy malware on end-of-life (EoL) routers to convert them into proxies sold on the 5Socks and Anyproxy networks. These devices, which were released many years back and no longer receive security updates from their vendors, are vulnerable to external attacks leveraging publicly available exploits to inject persistent malware. Once compromised, they are added to residential proxy botnets that route malicious traffic. In many cases, these proxies are used by cybercriminals to conduct malicious activities or cyberattacks. The FBI warns that Chinese state-sponsored actors exploited known (n-day) vulnerabilities in these routers to conduct covert espionage campaigns, including operations targeting critical U.S. infrastructure. Common signs of compromise by a botnet include network connectivity disruptions, overheating, performance degradation, configuration changes, the appearance of rogue admin users, and unusual network traffic. The best way to mitigate the risk of botnet infections is to replace end-of-life routers with newer, actively supported models.

https://www.bleepingcomputer.com/news/security/fbi-end-of-life-routers-hacked-for-cybercrime-proxy-networks/

Supply Chain Attack Hits Npm Package with 45,000 Weekly Downloads

An npm package named 'rand-user-agent' has been compromised in a supply chain attack to inject obfuscated code that activates a remote access trojan (RAT) on the user's system. The 'rand-user-agent' package is a tool that generates randomized user-agent strings, which is helpful in web scraping, automated testing, and security research. Although the package has been deprecated, it remains fairly popular, averaging 45,000 downloads weekly. According to researchers at Aikido, threat actors took advantage of its semi-abandoned yet popular status to inject malicious code in unauthorized subsequent releases that are likely to have been downloaded by a significant number of downstream projects. Researchers found obfuscated code hidden in the 'dist/index.js' file that was only visible if the user scrolled horizontally in the source view on the npm site.

https://www.bleepingcomputer.com/news/security/supply-chain-attack-hits-npm-package-with-45-000-weekly-downloads/

Kickidler Employee Monitoring Software Abused in Ransomware Attacks

Ransomware operations are using legitimate Kickidler employee monitoring software for reconnaissance, tracking their victims' activity, and harvesting credentials after breaching their networks. In attacks observed by cybersecurity companies Varonis and Synacktiv, Qilin and Hunters International ransomware affiliates installed Kickidler, an employee monitoring tool that can capture keystrokes, take screenshots, and create videos of the screen. The attacks started with the threat actors taking out Google Ads displayed when people searched for RVTools, a free Windows utility for managing VMware vSphere deployments. Clicking on the advertisement led to a fake RVTools site (rv-tool[.]net), promoting a trojanized program version. The program is a malware loader that downloads and runs the SMOKEDHAM PowerShell .NET backdoor, which was used to deploy Kickidler on the device. To defend against potential security breaches, network defenders are advised to audit installed remote access tools and identify authorized RMM software.

https://www.bleepingcomputer.com/news/security/kickidler-employee-monitoring-software-abused-in-ransomware-attacks/

MirrorFace Targets Japan and Taiwan with ROAMINGMOUSE and ANEL Malware

A nation-state threat actor known as MirrorFace deployed malware dubbed ROAMINGMOUSE as part of a cyber espionage campaign directed against government agencies and public institutions in Japan and Taiwan. The activity, detected by Trend Micro in March 2025, involved the use of spear-phishing lures to deliver an updated version of a backdoor called ANEL. The China-aligned threat actor, also known as Earth Kasha, is likely a sub-cluster within APT10. In March 2025, ESET shed light on a campaign referred to as Operation AkaiRyū that targeted a diplomatic organization in the European Union in August 2024 with ANEL (aka UPPERCUT). Enterprises and organizations, especially those with high-value assets like sensitive data relating to governance, as well as intellectual property, infrastructure data, and access credentials should continue to be vigilant and implement proactive security measures to prevent falling victim to cyber attacks.

https://thehackernews.com/2025/05/mirrorface-targets-japan-and-taiwan.html

CoGUI Phishing Platform Sent 580 Million Emails to Steal Credentials

A new phishing kit named 'CoGUI' sent over 580 million emails to targets between January and April 2025, aiming to steal account credentials and payment data. The messages impersonate major brands like Amazon, Rakuten, PayPal, Apple, tax agencies, and banks. The activity culminated in January 2025, where 170 campaigns sent 172,000,000 phishing messages to targets, but the following months maintained equally impressive volumes. Proofpoint researchers who discovered the CoGUI campaigns noted that it's the highest volume phishing campaign they currently track. The attacks mainly target Japan, though smaller-scale campaigns were also directed at the United States, Canada, Australia, and New Zealand. CoGUI has been active since at least October 2024, but Proofpoint started tracking it in December and onward. The best way to mitigate phishing risks is never to act with haste when receiving emails requesting urgent action, and always log in to the claimed platform independently instead of following embedded links.

https://www.bleepingcomputer.com/news/security/cogui-phishing-platform-sent-580-million-emails-to-steal-credentials/

Samsung Magicinfo Flaw Exploited Days After PoC Exploit Publication

Threat actors exploited a vulnerability in Samsung MagicINFO days after a PoC exploit was published. Arctic Wolf researchers observed threat actors exploiting CVE-2024-7399 (CVSS score: 8.8), in the Samsung MagicINFO content management system (CMS) just days after proof-of-concept (PoC) exploit code was publicly released. The vulnerability is an improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1050, an attacker can exploit the flaw to write arbitrary file as system authority. CVE-2024-7399 is a flaw in Samsung MagicINFO 9 Server’s input validation, it allows unauthenticated attackers to upload JSP files and execute code with system-level access. Samsung first disclosed the flaw in August 2024, and at the time, there were no signs of it being exploited. However, just days after a proof-of-concept (PoC) was published on 30 Apr 25, threat actors began taking advantage of it. Given how easy it is to exploit, and the public availability of the PoC, experts believe that the attacks are likely to continue. Samsung addressed the vulnerability with the release of MagicINFO 9 Server version 21.1050 in August 2024.

https://securityaffairs.com/177529/hacking/samsung-magicinfo-vulnerability-exploited-after-poc-publication.html

Linux Wiper Malware Hidden in Malicious Go Modules on Github

A supply-chain attack targets Linux servers with disk-wiping malware hidden in Golang modules published on GitHub. The campaign was detected last month and relied on three malicious Go modules that included “highly obfuscated code” for retrieving remote payloads and executing them. The attack appears designed specifically for Linux-based servers and developer environments, as the destructive payload - a Bash script named done.sh, runs a ‘dd’ command for the file-wiping activity. An analysis from supply-chain security company Socket shows that the command overwrites with zeroes every byte of data, leading to irreversible data loss and system failure. The target is the primary storage volume, /dev/sda, that holds critical system data, user files, databases, and configurations.

https://www.bleepingcomputer.com/news/security/linux-wiper-malware-hidden-in-malicious-go-modules-on-github/

Smishing on a Massive Scale: ‘Panda Shop’ Chinese Carding Syndicate

Resecurity identified a new smishing kit known as ‘Panda Shop,’ based on the same principles used by the Smishing Triad. The kit’s structure and scripting scenarios analyzed by Resecurity mimic the same product but include specific improvements and new supported templates. Resecurity identified multiple actors leveraging the Panda Shop smishing kit for Google Wallet and Apple Pay, harvesting traditional credit card and PII data, and intercepting transactions. The investigators noted that, besides Google RCS and Apple iMessage being used as the primary smishing delivery methods, the group also uses SMS gateways, specialized equipment for network operators. Telemarketing companies also use similar devices to send messages to mobile subscribers for legitimate purposes, which appears to be misused by Chinese cybercriminals in combination with other methods. One identified threat actor can send up to 2,000,000 smishing messages daily. The negative aspect of this is that cybercriminals have everything needed for this, which may mean that the Smishing Triad and similar groups could easily target up to 60,000,000 victims per month, or 720,000,000 per year, enough to target every person in the US at least twice every year.

https://securityaffairs.com/177502/cyber-crime/smishing-on-a-massive-scale-panda-shop-chinese-carding-syndicate.html

Wormable AirPlay Flaws Enable Zero-Click RCE on Apple Devices via Public Wi-Fi

Cybersecurity researchers disclosed a series of now-patched security vulnerabilities in Apple's AirPlay protocol that, if successfully exploited, could enable an attacker to take over susceptible devices supporting the proprietary wireless technology. The shortcomings are collectively codenamed AirBorne by Israeli cybersecurity company Oligo. Some of the vulnerabilities, like CVE-2025-24252 and CVE-2025-24132, can be strung together to fashion a wormable zero-click RCE exploit, enabling bad actors to deploy malware that propagates to devices on any local network the infected device connects to. This includes chaining CVE-2025-24252 and CVE-2025-24206 to achieve a zero-click RCE on macOS devices that are connected to the same network as an attacker. However, for this exploit to succeed, the AirPlay receiver needs to be on and set to the "Anyone on the same network" or "Everyone" configuration.

https://thehackernews.com/2025/05/wormable-airplay-flaws-enable-zero.html