10 Mar 25

Cyber Threat Roundup

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

Contents

Articles

Microsoft: North Korean Hackers Join Qilin Ransomware Gang

A dataset used to train large language models (LLMs) has been found to contain nearly 12,000 live secrets, which allow for successful authentication. The findings once again highlight how hard-coded credentials pose a severe security risk to users and organizations alike, not to mention compounding the problem when LLMs end up suggesting insecure coding practices to their users. Truffle Security said it downloaded a December 2024 archive from Common Crawl, which maintains a free, open repository of web crawl data. The massive dataset contains over 250 billion pages spanning 18 years. The company's analysis found that there are 219 different secret types in Common Crawl, including Amazon Web Services (AWS) root keys, Slack webhooks, and Mailchimp API keys.

https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/

FIN7, FIN8, and Others Use Ragnar Loader for Persistent Access and Ransomware Operations

Threat hunters have shed light on a "sophisticated and evolving malware toolkit" called Ragnar Loader that's used by various cybercrime and ransomware groups like Ragnar Locker (aka Monstrous Mantis), FIN7, FIN8, and Ruthless Mantis (ex-REvil). Ragnar Loader plays a key role in keeping access to compromised systems, helping attackers stay in networks for long-term operations. Ragnar Loader, also referred to as Sardonic, was first documented by Bitdefender in August 2021 in connection with an unsuccessful attack carried out by FIN8 aimed at an unnamed financial institution located in the U.S. It's said to have been put to use since 2020. The core functionality of Ragnar Loader is its ability to establish long-term footholds within targeted environments, while employing an arsenal of techniques to sidestep detection and ensure operational resilience. The malware utilizes PowerShell-based payloads for execution, incorporates strong encryption and encoding methods (including RC4 and Base64) to conceal its operations, and employs sophisticated process injection strategies to establish and maintain stealthy control over compromised systems.

https://thehackernews.com/2025/03/fin7-fin8-and-others-use-ragnar-loader.html

This Malicious PyPI Package Stole Ethereum Private Keys via Polygon RPC Transactions

Cybersecurity researchers have discovered a malicious Python package on the Python Package Index (PyPI) repository that's equipped to steal a victim's Ethereum private keys by impersonating popular libraries. The package in question is set-utils, which has received 1,077 downloads to date. It's no longer available for download from the official registry. Disguised as a simple utility for Python sets, the package mimics widely used libraries like python-utils (712M+ downloads) and utils (23.5M + downloads). This deception tricks unsuspecting developers into installing the compromised package, granting attackers unauthorized access to Ethereum wallets. The package aims to target Ethereum developers and organizations working with Python-based blockchain applications, particularly Python-based wallet management libraries like eth-account.

https://thehackernews.com/2025/03/this-malicious-pypi-package-stole.html

EncryptHub Deploys Ransomware and Stealer via Trojanized Apps, PPI Services, and Phishing

The financially motivated threat actor known as EncryptHub has been observed orchestrating sophisticated phishing campaigns to deploy information stealers and ransomware, while also working on a new product called EncryptRAT. EncryptHub has been observed targeting users of popular applications, by distributing trojanized versions. Furthermore, the threat actor has also made use of third-party Pay-Per-Install (PPI) distribution services. The cybersecurity company described the threat actor as a hacking group that makes operational security errors and as someone who incorporates exploits for popular security flaws into their attack campaigns. EncryptHub, also tracked by Swiss cybersecurity company PRODAFT as LARVA-208, is assessed to have become active towards the end of June 2024, relying on a variety of approaches ranging from SMS phishing (smishing) to voice phishing (vishing) in an attempt to trick prospective targets into installing remote monitoring and management (RMM) software.

https://thehackernews.com/2025/03/encrypthub-deploys-ransomware-and.html

Chinese APT Lotus Panda Targets Governments with New Sagerunex Backdoor Variants

The threat actor known as Lotus Panda has been observed targeting government, manufacturing, telecommunications, and media sectors in the Philippines, Vietnam, Hong Kong, and Taiwan with updated versions of a known backdoor called Sagerunex. Lotus Blossom has been using the Sagerunex backdoor since at least 2016 and is increasingly employing long-term persistence command shells and developing new variants of the Sagerunex malware suite. Lotus Panda, also known as Billbug, Bronze Elgin, Lotus Blossom, Spring Dragon, and Thrip, is a suspected Chinese hacking crew that's active since at least 2009. The threat actor was first exposed by Broadcom-owned Symantec in June 2018. In late 2022, Symantec detailed the threat actor's attack on a digital certificate authority as well as government and defense agencies located in different countries in Asia that involved the use of backdoors like Hannotog and Sagerunex.

https://thehackernews.com/2025/03/chinese-apt-lotus-panda-targets.html

Seven Malicious Go Packages Found Deploying Malware on Linux and macOS Systems

Cybersecurity researchers are alerting of an ongoing malicious campaign targeting the Go ecosystem with typosquatted modules that are designed to deploy loader malware on Linux and Apple macOS systems. The threat actor has published at least seven packages impersonating widely used Go libraries, including one (github[.]com/shallowmulti/hypert) that appears to target financial-sector developers. These packages share repeated malicious filenames and consistent obfuscation techniques, suggesting a coordinated threat actor capable of pivoting rapidly. While all of them continue to be available on the official package repository, their corresponding GitHub repositories barring "github[.]com/ornatedoctrin/layout" are no longer accessible.

https://thehackernews.com/2025/03/seven-malicious-go-packages-found.html

Over 37,000 VMware ESXi Servers Vulnerable to Ongoing Attacks

Over 37,000 internet-exposed VMware ESXi instances are vulnerable to CVE-2025-22224, a critical out-of-bounds write flaw that is actively exploited in the wild. This massive exposure is being reported by threat monitoring platform The Shadowserver Foundation, which reported a figure of around 41,500 yesterday. Today, ShadowServer now reports that 37,000 are still vulnerable, indicating that 4,500 devices were patched yesterday.CVE-2025-22224 is a critical-severity VCMI heap overflow vulnerability that enables local attackers with administrative privileges on the VM guest to escape the sandbox and execute code on the host as the VMX process. Broadcom warned customers

about it along with two other flaws, CVE-2025-22225 and CVE-2025-22226, on Tuesday, March 4, 2025, informing that all three were being exploited in attacks as zero-days. The flaws were discovered by Microsoft Threat Intelligence Center, which observed their exploitation as zero days for an undisclosed period. Also, no information about the origin of the attacks and the targets has been shared yet.

https://www.bleepingcomputer.com/news/security/over-37-000-vmware-esxi-servers-vulnerable-to-ongoing-attacks/

Hackers Use ClickFix Trick to Deploy PowerShell-Based Havoc C2 via SharePoint Sites

Cybersecurity researchers are calling attention to a new phishing campaign that employs the ClickFix technique to deliver an open-source command-and-control (C2) framework called Havoc. The threat actor hides each malware stage behind a SharePoint site and uses a modified version of Havoc Demon in conjunction with the Microsoft Graph API to obscure C2 communications within trusted, well-known services. The ClickFix bait used in the newly discovered campaign informs the user that there is an error connecting to Microsoft OneDrive, and that they need to rectify the issue by updating the DNS cache manually. If the person falls for the gambit, they inadvertently activate the infection process by running the PowerShell script.

https://thehackernews.com/2025/03/hackers-use-clickfix-trick-to-deploy.html

Hackers Exploit Paragon Partition Manager Driver Vulnerability in Ransomware Attacks

Threat actors have been exploiting a security vulnerability in Paragon Partition Manager's BioNTdrv.sys driver in ransomware attacks to escalate privileges and execute arbitrary code. The zero-day flaw (CVE-2025-0289) is part of a set of five vulnerabilities that was discovered by Microsoft, according to the CERT Coordination Center (CERT/CC). These include arbitrary kernel memory mapping and write vulnerabilities, a null pointer dereference, insecure kernel resource access, and an arbitrary memory move vulnerability. The vulnerabilities have since been addressed by Paragon Software with version 2.0.0 of the driver, with the susceptible version of the driver added to Microsoft's driver blocklist.

https://thehackernews.com/2025/03/hackers-exploit-paragon-partition.html

Researchers Link CACTUS Ransomware Tactics to Former Black Basta Affiliates

Threat actors deploying the Black Basta and CACTUS ransomware families have been found to rely on the same BackConnect (BC) module for maintaining persistent control over infected hosts, a sign that affiliates previously associated with Black Basta may have transitioned to CACTUS. Once infiltrated, it grants attackers a wide range of remote control capabilities, allowing them to execute commands on the infected machine. This enables them to steal sensitive data, such as login credentials, financial information, and personal files. It's worth noting that details of the BC module, which the cybersecurity company is tracking as QBACKCONNECT owing to overlaps with the QakBot loader, was first documented in late January 2025 by both Walmart's Cyber Intelligence team and Sophos, the latter of which has designated the cluster the name STAC5777.

https://thehackernews.com/2025/03/researchers-link-cactus-ransomware.html