CYBER PULSE

Edition 192
7th November 2022

by Richard Beck

Cryptojacking attacks continue to persist

The face value of digital currencies is fluctuating, however, cryptojacking attacks persistently target crypto firms and users. Researchers took the wraps off of a campaign, dubbed Purpleurchin, leveraging several public cloud platforms at once to launch an automated and massive cryptomining campaign. Purpleurchin abuses free trial accounts on continuous integration and continuous delivery CI/CD service providers such as GitHub, Heroku, and Buddy.Works, according to a report by Sysdig researchers. It is leveraging hacker-created user accounts on GitHub (300 accounts), Heroku (2,000 accounts), and Buddy.works (900 accounts). These accounts are leveraged by Purpleurchin to perform over a million function calls daily. These accounts are rotated and channelled through 130 Docker Hub images with mining containers. The campaign uses OpenVPN and Namecheap VPN to create large numbers of accounts with different IP addresses to evade GitHub's bot activity detection. The operation is using a linuxapp container, shell scripts, mining containers, and docker containers. In addition, it leverages several tools such as XDOTOOL, Wit, and Buster, to perform various functions such as bypassing defensive mechanisms. The campaign stealthily mines a range of crypto coins such as Yenten, Tidecoin, Sprint, Onyx, Surgarchain, Arionum, MintMe, and Bitweb.

The damage per account per month is estimated to be $15 for GitHub, and between $7 and $10 for Heroku and Buddy, which is significant. Overall, it has been identified that this campaign causes a loss of around $100,000 for service providers to mine one Monero, which is about ten times higher than the harm (around $11,000) caused by normal cryptojacking operations in terms of resource usage. It is suspected that with the success of this small and profitable campaign, Purplechin could soon switch to more profitable coins such as Monero or Bitcoin. Moreover, the hackers could potentially attempt to steal millions of dollars' worth of cryptocurrency by creating a network control majority of 51% on these small platforms. De-Fi protocols must watch out for such threats! Edited: Original source - Sysdig

New open-source tool scans public AWS S3 buckets for secrets

A new open-source 'S3crets Scanner' scanner allows researchers and red-teamers to search for 'secrets' mistakenly stored in publicly exposed or company's Amazon AWS S3 storage buckets. Amazon S3 (Simple Storage Service) is a cloud storage service commonly used by companies to store software, services, and data in containers known as buckets. Unfortunately, companies sometimes fail to properly secure their S3 buckets and thus publicly expose stored data to the Internet. This type of misconfiguration has caused data breaches in the past, with threat actors gaining access to employee or customer details, backups, and other types of data. In addition to application data, source code or configuration files in the S3 buckets can also contain 'secrets,' which are authentication keys, access tokens, and API keys.

If these secrets are improperly exposed and accessed by threat actors, they could allow them far greater access to other services or even the company's corporate network. During an exercise examining SEGA's recent assets exposure, security researcher Eilon Harel discovered that no tools for scanning accidental data leaks exist, so he decided to create his own automated scanner and release it as an open-source tool on GitHub. To help with the timely discovery of exposed secrets on public S3 buckets, Harel created a Python tool named "S3crets Scanner" that automatically performs the following actions:

- Use CSPM to get a list of public buckets
- List the bucket content via API queries
- Check for exposed textual files
- Download the relevant textual files
- Scan content for secrets
- Forward results to SIEM

Any buckets that were intended to be public are filtered out from the list before the textual files are downloaded for the "secrets scanning" step. When scanning a bucket, the script will examine the content of text files using the Trufflehog3 tool, an improved Go-based version of the secrets scanner that can check for credentials and private keys on GitHub, GitLab, filesystems, and S3 buckets. Edited: Original source - Medium

New LinkedIn Phishing Campaign Bypasses Google Protection

Armorblox spotted a new credential phishing campaign that comes with the capability of bypassing Google email security. The campaign is conducted on LinkedIn as social media continues to be a good source of targets for cybercriminals. The phishing campaign targeted 500 mailboxes of employees from a national travel organization. The email comes with the subject line - "We noticed some unusual activity" - pretending to be from LinkedIn. However, the attackers have misspelled LinkedIn and the domain was created on March 6. The phishing campaign bypassed detection by Google's email security controls after passing authentication checks via DMARC and SFP.

The campaign leveraged brand impersonation, social engineering, malicious URLs, and existing business workflow replication. LinkedIn emerged as the third-most impersonated brand in Q3, preceded by DHL and Microsoft. However, it was at the top of the list in the previous two quarters of the year. Threat actors have been creating fake employee accounts on LinkedIn, which couple AI-generated profile photos with text copied from legitimate users. The platform has introduced three new features to defend against fake profiles and malicious activities on the platform. LinkedIn has started showing more information about accounts to verify them, actively hunting for fake AIs, and warning users against suspicious messages. Edited: Original source - Armorblox

Samsung Galaxy Store Bug Could've Let Hackers Secretly Install Apps on Targeted Devices

A now-patched security flaw has been disclosed in the Galaxy Store app for Samsung devices that could potentially trigger remote command execution on affected phones. The vulnerability, which affects Galaxy Store version 4.5.32.4, relates to a cross-site scripting (XSS) bug that occurs when handling certain deep links. An independent security researcher has been credited with reporting the issue.

"Here, by not checking the deep link securely, when a user accesses a link from a website containing the deeplink, the attacker can execute JS code in the webview context of the Galaxy Store application," SSD Secure Disclosure said in an advisory posted last week.

XSS attacks allow an adversary to inject and execute malicious JavaScript code when visiting a website from a browser or another application. The issue identified in the Galaxy Store app has to do with how deep links are configured for Samsung's Marketing & Content Service (MCS), potentially leading to a scenario where arbitrary code injected into the MCS website could lead to its execution. This could then be leveraged to download and install malware-laced apps on the Samsung device when visiting the link.
"To be able to successfully exploit the victim's server, it is necessary to have HTTPS and CORS bypass of chrome," the researchers noted. Edited: Original source - SSD

Largest EU copper producer Aurubis suffers cyberattack

German copper producer Aurubis has announced that it suffered a cyberattack that forced it to shut down IT systems to prevent the attack's spread. Aurubis is Europe's largest copper producer and the second largest in the world, with 6,900 employees worldwide, and produces one million tonnes of copper cathodes yearly. In an announcement published on their website, Aurubis says they shut down various systems at their locations but that it has not impacted production.

"The production and environmental protection facilities at the smelter sites are running, and incoming and outgoing goods are also being maintained manually," comments Aurubis' announcement.

At this time, the company is still assessing the impact of the cyberattack and is working closely with the authorities to speed up the process. The priority now is to maintain the production volumes at normal levels and keep the raw material supply and the delivery of finished goods unruffled. For this reason, some operations have turned to manual mode to keep the flow of incoming and outgoing goods adequate for as long as required until computer-assisted automation returns at the smelters. Aurubis states that it's impossible to estimate how long it will take for all its systems to return to normal operations. Until that happens, there's a plan to establish transitional solutions that will give the company and its customers an alternative communication channel. For now, the only way to reach Aurubis is via the phone. While all the above carry the typical signs of a ransomware attack, Aurubis has not provided any details on its cyberattack. However, Aurubis states that the attack "part of a larger attack on the metals and mining industry." Edited: Original source - Aurubis

Malware-as-a-Service (MaaS) targeting government users in Hungary.

According to researchers from FortiGuard Labs, the purported phishing emails inform users that their credentials to a government portal have changed and that new ones are attached within. The portal in question is used to conduct official business online such as submitting documents and ordering IDs. The attachment is a zip file that contains an executable pretending to be a PDF. Upon execution, the PDF extracts Warzone RAT to memory and runs it. The attack also uses .dll files and reverse engineering techniques to increase the level of obfuscation. The ultimate goal of the campaign is to gain remote access to Microsoft Windows.

Warzone RAT is a well-known malware that is publicly available on the internet, and anybody can access it through a subscription model. The malware is often referred to as Ave Maria Stealer as it borrows source code from the latter. It offers a wide range of functionality to its subscribers. These include recording keystrokes, harvesting cookies, providing remote access to a desktop and webcam, pilfering passwords, and maintaining persistence, among others. Warzone also provides multiple ways to escalate privileges depending on the Windows version. While remote access tools are providing versatile support to organizations, these tools have become increasingly popular among cybercriminals to launch cyberattacks. Using remote access tools such as Warzone as final payloads can enable cybercriminals to perform various malicious activities that can impact an organization’s credentials and other data. As the malware is primarily distributed via phishing emails, organizations must have proper email security checks installed to thwart such threats. Edited: Original source - FortiGuard

VMware declares vulnerability already being exploited

VMware over the weekend warned of the existence of a public exploit targeting a recently addressed critical remote code execution (RCE) vulnerability in NSX Data Center for vSphere (NSX-V). An end-of-life (EOL) product installed as a plug-in to VMware vCenter Server, NSX-V is a network virtualization solution offering networking and security functionality, including VPN, logical switching and routing, and more. The product is bundled within VMware Cloud Foundation. Last week, VMware announced the availability of patches for CVE-2021-39144 (CVSS score of 9.8), an RCE flaw via the open source library XStream, warning that it could allow a remote attacker to execute arbitrary code in the context of 'root' on the appliance.
The company also notes that, while it typically does not mention EOL products in advisories, the severity of this bug led to the release of a patch as an exception. Over the weekend, VMware updated its advisory on CVE-2021-39144 to warn that an exploit targeting this vulnerability already exists.

“VMware has confirmed exploit code leveraging CVE-2021-39144 against VCF (NSX-V) has been published,” the company says.

In an accompanying FAQ, VMware warns that successful exploitation of this vulnerability could allow a malicious actor who has network access to the NSX-V Manager to take over the appliance. According to the company, all NSX-V configurations are impacted and no in-product workarounds are available. VMware addressed the vulnerability with the release of NSX-V version 6.4.14. The company urges all customers to upgrade their installations to this product iteration. Edited: Original source - VMware