Cloud Consultancy

DIGITALIZATION & SECURITY

# CCDS CYBER SECURITY PICKS

47th Release February 2023

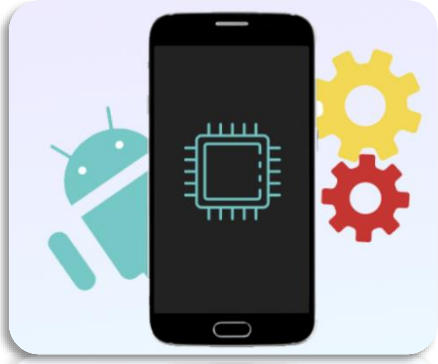
Uncovering the Risks & Realities of Third-Party Connected Apps

## Shocking Findings from the 2023 Third-Party App Access Report

Organizations with 10,000 SaaS users that use M365 and Google Workspace average over 4,371 additional connected apps.

SaaS-to-SaaS (third-party) app installations are growing *nonstop* at organizations around the world. When an employee needs an additional app to increase their efficiency or productivity, they rarely think twice before installing. Most employees don't even realize that this SaaS-to-SaaS connectivity, which requires scopes like the ability to read, update, create, and delete content, increases their organization's attack surface in a significant way.

Source:https://thehackernews.com/2023/02/shocking-findings-from-2023-third-party.html



## Google Teams Up with Ecosystem Partners to Enhance Security of SoC Processors

Google said it's working with ecosystem partners to harden the security of firmware that interacts with Android.

While the Android operating system runs on what's called the application processor (AP), it's just one of the many processors of a system-on-chip (SoC) that cater to various tasks like cellular communications and multimedia processing.

"Securing the Android Platform requires going beyond the confines of the Application Processor," the Android team said. "Android's defense-in-depth strategy also applies to the firmware running on bare-metal environments in these microcontrollers, as they are a critical part of the attack surface of a device."

The tech giant said the goal is to bolster the security of software running on these secondary processors
Source:https://thehackernews.com/2023/02/google-teams-up-with-ecosystem-partners.html

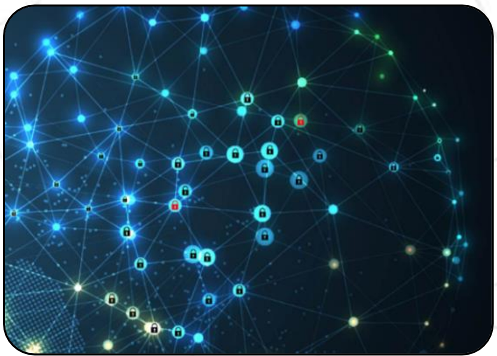
## How to Use AI in Cybersecurity and Avoid Being Trapped

The use of AI in cybersecurity is growing rapidly and is having a significant impact on threat detection, incident response, fraud detection, and vulnerability management.

According to a report by Juniper Research, the use of AI for fraud detection and prevention is expected to save businesses $11 billion annually by 2023.

In terms of detecting and responding to security threats in a more efficient and effective manner, AI has been helping businesses in lots of ways.

Source:
https://thehackernews.com/2023/02/how-to-use-ai-in-cybersecurity-and.html



## 3 Steps to Automate Your Third-Party Risk Management Program

If you Google "third-party data breaches" you will find many recent reports of data breaches that were either caused by an attack at a third party or sensitive information stored at a third-party location was exposed. Organizations are now sharing data with an average of 730 third-party vendors, according to a report by Osano, and with the acceleration of digital transformation, that number will only grow

Source:https://thehackernews.com/2023/02/3-steps-to-automate-your-third-party.html

## Python Developers Warned of Trojanized PyPI Packages Mimicking Popular Libraries

Cybersecurity researchers are warning of "imposter packages" mimicking popular libraries available on the Python Package Index (PyPI) repository.

The 41 malicious PyPI packages have been found to pose as typosquatted variants of legitimate modules such as HTTP, AIOHTTP, requests, urllib, and urllib3.

Source:https://thehackernews.com/2023/02/python-developers-warned-of-trojanized.html

## Hackers Using Trojanized macOS Apps to Deploy Evasive Cryptocurrency Mining Malware

Trojanized versions of legitimate applications are being used to deploy evasive cryptocurrency mining malware on macOS systems.

Jamf Threat Labs, which made the discovery, said the XMRig coin miner was executed by means of an unauthorized modification in Final Cut Pro, a video editing software from Apple.

"This malware makes use of the Invisible Internet Project (i2p) to download malicious components and send mined currency to the attacker's wallet," Jamf researchers Matt Benyo, Ferdous Saljooki, and Jaron Bradley said in a report shared with The Hacker News.

An earlier iteration of the campaign was documented exactly a year ago by Trend Micro, which pointed out the malware's use of i2p to conceal network traffic and speculated that it may have been delivered as a DMG file for Adobe Photoshop CC 2019.

Source: https://thehackernews.com/2023/02/hackers-using-trojanized-macos-apps-to.html

## MyloBot Botnet Spreading Rapidly Worldwide: Infecting Over 50,000 Devices Daily

A sophisticated botnet known as MyloBot has compromised thousands of systems, with most of them located in India, the U.S., Indonesia, and Iran.

That's according to new findings from BitSight, which said it's "currently seeing more than 50,000 unique infected systems every day," down from a high of 250,000 unique hosts in 2020.

MyloBot, which emerged on the threat landscape in 2017, was first documented by Deep Instinct in 2018, calling out its anti-analysis techniques and its ability to function as a downloader.

"What makes MyloBot dangerous is its ability to download and execute any type of payload after it infects a host," Lumen's Black Lotus Labs said in November 2018. "This means at any time it could download any other type of malware the attacker desires."

Source: https://thehackernews.com/2023/02/mylobot-botnet-spreading-rapidly.html

Cloud Consultancy

*Contact Us*

**Cloud Consultancy for Digitalization & Security – CCDS's is a Specialized Company in IT and Information Security Services, which has its international headquarters in the UAE. It also has branch offices throughout the MENA Region with its premier office in Saudi Arabia. Innovative and professional in its approach, it always partners with best-in-class products and services, to identify and solve security threats and issues for its clients.**