Strategic Cyber Security Report — April 2023 Edition

Andre Camillo, CISSP

Published in InfoSec Write-ups · 7 min read · May 1, 2023

1

A Monthly summary of Strategic Information for Cyber Security Leaders

This is a series spun from a need I identified when talking to CISOs — as explained on the kick-off article, this series follows the format of:

> What’s Top of mind in 3 domains: People, Processes, Technology for CISOs.

People

The US Leak on Social Media

The US national security agencies and the Justice Department are investigating the release of dozens of classified documents. This could be the gravest leak of US secrets in years. The article provides information about the latest leak of US secrets.

According to Reuters: The information leaked include classification markings of NOFORN, meaning they cannot be shared with foreign intelligence agencies.

What sensitive information leaked according to Reuters:

> - *Ukraine: Details about Ukrainian air strikes, the country’s air defense vulnerabilities, and even the size of some Ukrainian military units.*
>
> - *Wagner group: Descriptions of a number of outreach efforts by the Russian mercenary group, including to Turkish “contacts,” Haitian government officials, and the organization’s growing presence in Mali.*

> *- Middle East: Updates related to Iran's nuclear activities as well as information about how the United Arab Emirates is in talks with Russia to help build a maintenance center for some weapons.*
>
> *- China: Predictions about how China would respond to Ukrainian strikes inside Russia, along with details about British plans in the Indo-Pacific region.*
>
> *- North Korea: Details about missile tests by Pyongyang and an assessment that a February parade likely oversold the ICBM threat to the United States.*
>
> *- South America: Information about Brazilian officials' plan to visit Moscow in April to discuss a Ukraine mediation scheme.*
>
> *- Africa: An assessment that France is likely to struggle to achieve security goals in west and central Africa.*

How did it leak?

Apparently, the leaker took photos of physical documents and shared in Discord.

According to Reuters:

> *Pictures of creased documents — suggesting that they might have been folded so they could be hidden before being removed from the top-secret spaces to which such materials are confined and photographed — were posted to social media sites.*
>
> *Those platforms included Discord, an instant messaging platform popular with gamers, the online messaging board 4Chan, the encrypted Telegram global messaging app, and Twitter.*

> *Although the documents only garnered widespread attention in the last few days, the open source investigation site Bellingcat said it had found evidence that the documents — or at least some of them — had appeared on social media as far back as March or even January.*
>
> *In an article about the documents' "improbable journey," Bellingcat traced the earliest references to the leak to a now-defunct Discord server and cited three former users as saying that a large number of documents had been shared there.*

Why did it leak?

The reason for leaking is one that leads to questions about how the human profiling could lead to risk reduction. As reported by BBC on YouTube, the suspect arrested, leaked the information to gain popularity amongst its gaming community.

How would they access to such information is unsure at this stage and this is particularly concerning, especially if we consider the profile of the leaker, very high-risk in my opinion: an early 20s male with no record of trust in the organization (or handling sensitive information).

In the BBC report, the US official makes an interesting statement though, we do not want to be tracked or monitored so deeply.

CSA Whitepaper: Security Implications of ChatGPT

Cloud Security Alliance has released a whitepaper with their view on Security implications of ChatGPT.

The document was released in #rsac2023 and covers:

- Limitations of ChatGPT

- How Malicious Actors can use ChatGPT

- How Security Defenders can use ChatGPT within Cybersecurity Program

- and more…

Interesting paper and also a good deck for reference.

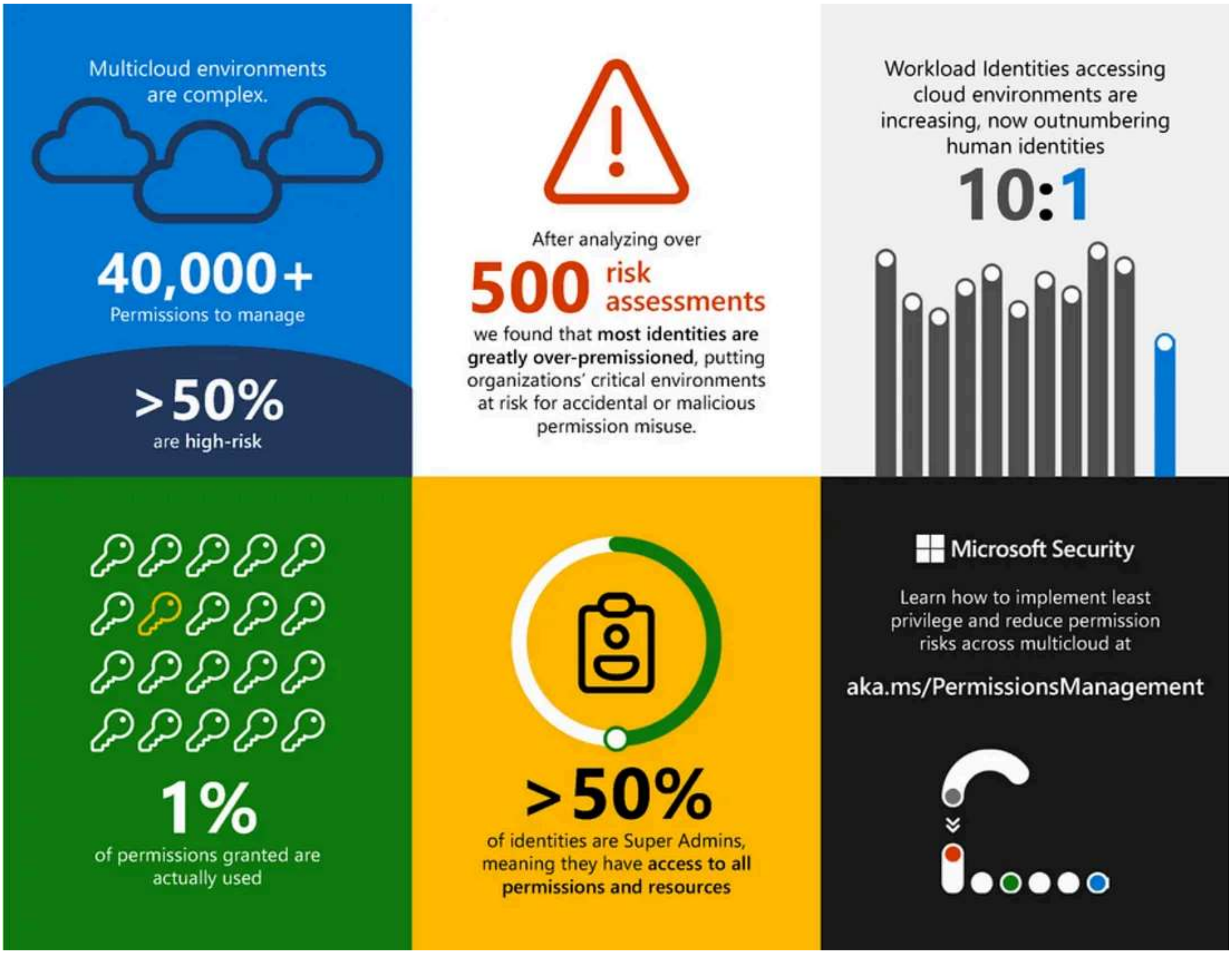
Both publications can be found here.

Process

Report: 2023 State of Cloud Permissions Risks

Microsoft released a report on the State of Cloud permissions risks for 2023. This is in line with their “*CIEM*” solution, Entra Permissions Management.

The report covers key risk findings surrounding identities and permissions across multicloud infrastructures.



Source: 2023 State of Cloud Permissions Risks report now published — Microsoft Community Hub

Find the blog post and report here.

CISA Zero Trust Maturity Model

CISA has released a draft for public comment of its Zero Trust Maturity model 2.0. This is a follow up to the version 1.0 released in 2021.

The original post by CISA can be found here and it states the following:

> *CISA's* Zero Trust Maturity Model *is one of many roadmaps that agencies can reference as they transition towards a zero-trust architecture. The maturity model aims to assist agencies in the development of zero trust strategies and*

> *implementation plans and to present ways in which various CISA services can support zero trust solutions across agencies.*
>
> *The maturity model, which includes five pillars and three cross-cutting capabilities, is based on the foundations of zero trust. Within each pillar, the maturity model provides specific examples of traditional, initial, advanced, and optimal zero trust architectures.*

The draft for public comment can be found here.

Where this seems to be perfect in its execution is a summarization of other US Federal agencies models, it mentions NIST's, NSA's and it's own previous model Architectures on page 4 onwards.

A must read for architects.

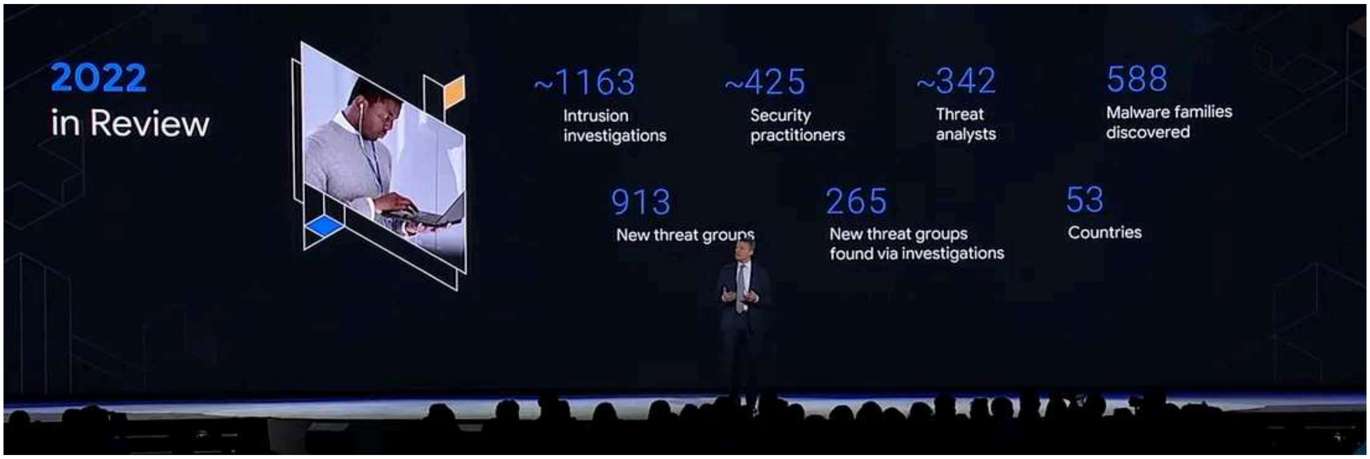
Mandiant's Year in Review at RSA

During RSA conference, Mandiant presented its "year in review" for incidents and threats they saw in 2022. The keynote is available in full on YouTube, link below.

Amongst the many interesting findings, they mentioned:

- Insider threat is very real, for years it has been, and they keep seeing it in their investigations.
- Notable Groups are really important to determine possible outcomes of on-going attacks.

Since an image is worth a thousand words:



2022 in Review

~1163 Intrusion investigations

~425 Security practitioners

~342 Threat analysts

588 Malware families discovered

913 New threat groups

265 New threat groups found via investigations

53 Countries

They also touched on the evolution of Victim Zero throughout decades, the big shift from Spear phishing leading the charts of method to vulnerabilities' exploits in the last few years.

The full video is available here.

Technology

RSA 2023 news

The RSA conference 2023 happened in the US, in late April and it garnered the attention of many cyber security professionals and vendors. I myself didn't attend — but did find a great article summarizing all announcements from vendors during the conference. This article by CSO online covers all announcements per day, between them, some of the ones I found interesting are:

- Microsoft, with multiple announcements including keynotes about the use of AI in its platform. The official summary available here mentions:

> *Microsoft Security Copilot is the first security product to enable defenders to move at the speed and scale of AI. Security Copilot combines this advanced large language model with a security-specific model from Microsoft. This security-specific model in turn incorporates a growing set of security-specific skills and is informed by Microsoft's unique global threat intelligence and more than 65 trillion daily signals. Security Copilot also delivers an enterprise-grade security and privacy-compliant experience as it runs on Microsoft Azure's hyperscale infrastructure.*

- Cisco XDR — it took them a few years to join the XDR platform club in my opinion, curious to see what that looks like. According to CRN in this article:

> *Cisco XDR is differentiated by providing "high-fidelity data" from across the company's various first-party security tools, such as Cisco Secure Client (formerly AnyConnect) for endpoint, he said. The XDR platform integrates a significant number of major third-party security products as well. Those include EDR tools (Microsoft Defender, Cybereason, Palo Alto Networks Cortex XDR, SentinelOne Singularity and Trend Micro Vision One); email security (Microsoft Defender for Office, Proofpoint); next-generation firewall from Palo Alto Networks; SIEM from Microsoft Sentinel*

- Eclypsium Supply Chain Security Platform — which according to CSO:

> *The Eclypsium Supply Chain Security Platform is designed to allow IT security and operations teams to continuously identify and monitor software bills of materials (SBOMs), integrity, and vulnerability of components and system code in each device. It generates an SBOM for each component and system code in enterprise devices in an industry-standard format.*

- Google Cloud Security AI Workbench, which according to CRN's report:

> *Google Cloud unveiled its Security AI Workbench offering that's powered by a new, security-specific large language model known as Sec-PaLM. The model utilizes Google Cloud's security intelligence via Google's broad visibility into threat data and Mandiant's esteemed threat intel around vulnerabilities and malware, as well as threat actors and threat indicators, according to Google Cloud.*

Microsoft — App governance included in Defender for Cloud Apps

All customers with a standalone, E5 Security, or Microsoft 365 E5, or any other license that includes Defender for Cloud Apps, will have access to App Governance, **at no additional cost**.

> ***Because we are seeing a continued rise in app-based attacks, we believe this is a foundational capability for customers. That's why today, we are excited to announce that going forward the App Governance add-on will be included in Defender for Cloud Apps at no additional cost. On June 1, 2023, new and existing customers will be able to start the opt-in process to begin using these capabilities.***

App governance can be used in your advanced Threat hunting for more signals of malicious activity…

Learn more about this in Microsoft's public post here.

Learn more about my Cloud and Security Projects: https://linktr.ee/acamillo

Consider subscribing to Medium (here) to access more content that will empower you!

Thank you for reading and leave your thoughts/comments!

References

Scattered throughout the document

Report Cybersecurity News Hacking AI

Written by Andre Camillo, CISSP

Edit profile

1K Followers · Writer for InfoSec Write-ups

Cloud and Security technologies, Career, Growth Mindset. Follow: https://linktr.ee/acamillo .
Technical Specialist @Microsoft. Opinions are my own.

More from Andre Camillo, CISSP and InfoSec Write-ups