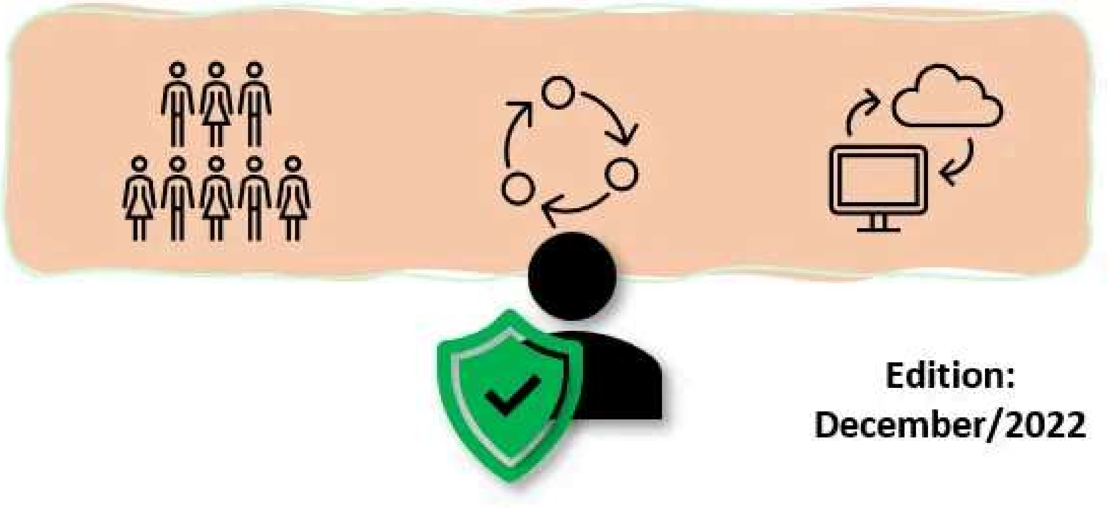
Strategic Cyber Security Report — December 2022 Edition

Andre Camillo, CISSP

Published in Geek Culture · 6 min read · Jan 14, 2023

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

An in-depth Incident Response report of the “Waikato District Health Board” for the 2021 incident

Back in may 2021, a major Cyber Security Incident shook the health sector in New Zealand. A major breach affected Waikato District Health Board (WDHB)

The official announcement from Te Whatu Ora includes a link to the official report by a Security provider called InPhySec.

I’ll leave you to read the report, but they take an approach to look at things from 3 different angles, including the victim’s Readiness, Response and Recovery — a good way to fully analyze facts.

Waikato District Health Board (WDHB) Incident Response Analysis — Te Whatu Ora — Health New Zealand

The rise of AI-assisted Malware creations?

OpenChat has made the headlines of the technology world these past few weeks — its access to public has garnered a raft of attention from devs, to curious people, writers, musicians and, why not, security researchers. Some of the results of the latter have been documented and by the Infosec

Magazine. And according to their report, Picus' Security co-founder, Suleyman Ozarslan provided some insights of their findings:

> *(Suleyman) was able to use the bot to create a believable World Cup phishing campaign and even write some macOS ransomware. Although the bot flagged that phishing could be used for malicious purposes, it still went ahead and produced the script.*

The way Suleyman did it was to break down malicious activities, that separately can't be seen as completely malicious — just leveraging TTP, quite observant:

> *"I described the tactics, techniques and procedures of ransomware without describing it as such. It's like a 3D printer that will not 'print a gun,' but will happily print a barrel, magazine, grip and trigger together if you ask it to," he explained.*

And additionally, another researcher got to the same goal in a similar way:

> *ExtraHop senior technical manager, Jamie Moles, found equally concerning results when he asked the bot for help in crafting an attack similar to the notorious WannaCry ransomware worm.*
>
> *"I asked it how to use Metasploit to use the EternalBlue exploit and its answer was basically perfect," he explained.*

Experts Warn ChatGPT Could Democratize Cybercrime — Infosecurity Magazine (infosecurity-magazine.com)

Lastpass comments on the 2022 breach

A new blog post by LastPass touches on the details of the August 2022 data breach they suffered. In their post, they mentioned:

> *we have learned that an unknown threat actor accessed a cloud-based storage environment leveraging information obtained from the incident we previously disclosed in August of 2022. While no customer data was accessed during the August 2022 incident, some source code and technical information were stolen from our development environment and used to target another employee, obtaining credentials and keys which were used to access and decrypt some storage volumes within the cloud-based storage service.*

From an Architecture perspective it's fascinating to read on their post about their production environment. They have an on-prem Data Center and use some Cloud-based storage services – using the latter, Lastpass mentioned, threat actors accessed backup information containing "basic customer information", which includes:

> *related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service.*

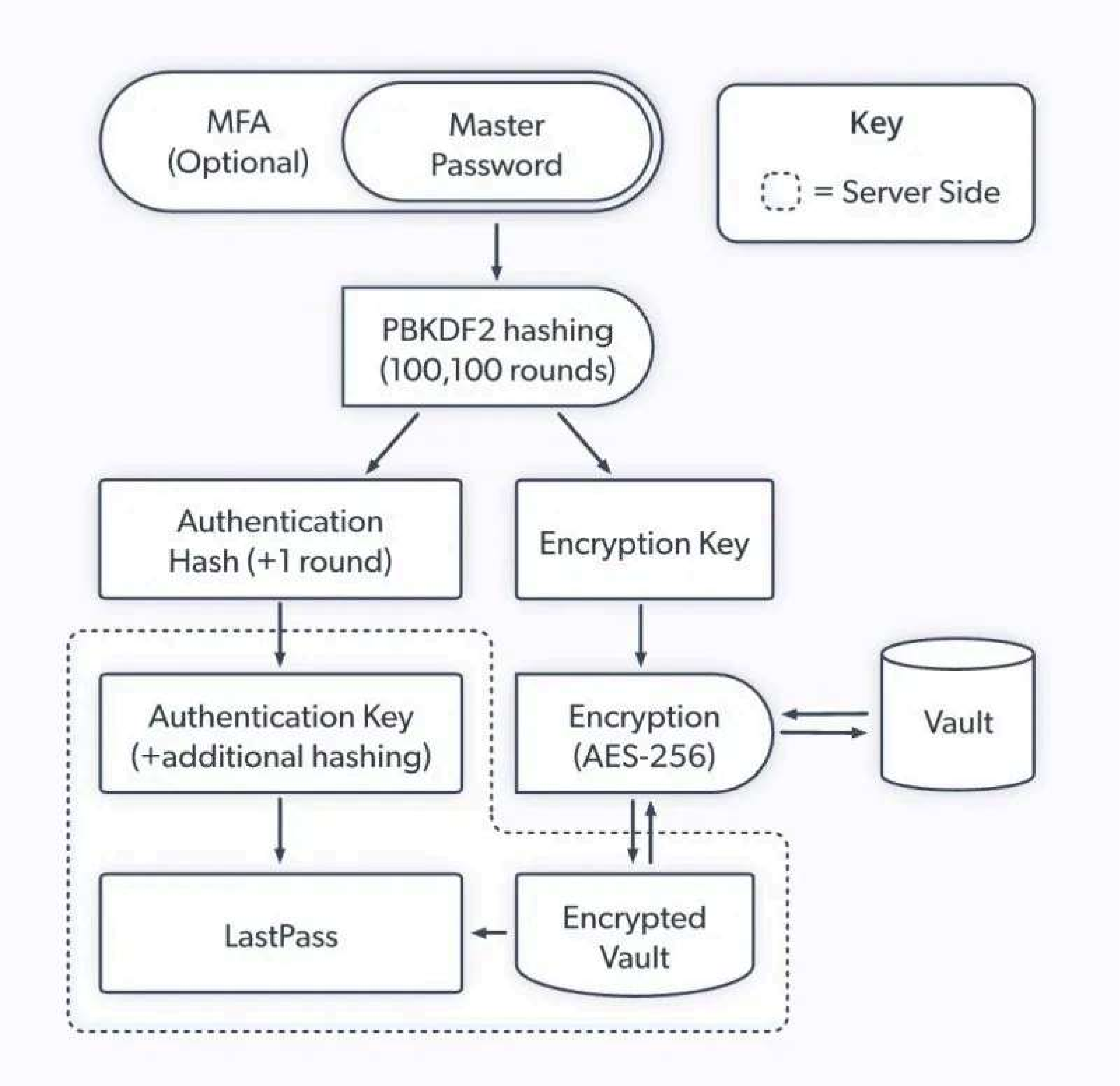
LastPass claims their "Zero Knowledge Architecture" towards their customer's Master Password – has curbed further issues in the breach, as the same post highlights:

> *The threat actor was also able to copy a backup of customer vault data from the encrypted storage container which is stored in a proprietary binary format that contains both unencrypted data, such as website URLs, as well as fully-encrypted sensitive fields such as website usernames and passwords, secure notes, and form-filled data. These encrypted fields remain secured with 256-bit AES encryption*

> *and can only be decrypted with a unique encryption key derived from each user's master password using our Zero Knowledge architecture. As a reminder, the master password is never known to LastPass and is not stored or maintained by LastPass. The encryption and decryption of data is performed only on the local LastPass client. For more information about our Zero Knowledge architecture and encryption algorithms.*

But the cyber security industry and many researchers have scrutinized the breach and what this means for customers. Essentially, every customer has their Vaults breached with the attacker having an infinite amount of time (and virtually resources) to (surely) break their master passwords.

I've also come across on linkedin on a visual representation of what was described by LastPass, on a post by Andrew Johnson (link here):



Source: https://www.linkedin.com/posts/andrew-johnson-7b29b93_lastpass-lastpass-hacked-activity-7012507887449116672/

LastPass recommends more actions if you think you've been impacted, plus touch on what they have done to notify their customers and even state of the investigation.

Check out all the details in their recent post, here.

Process

Australia setting the standards for how Government should lead Cyber Security

After a bumpy end of the year in Australia's Cyber Security scene, the government has announced a new cyber security strategy. More than a recast as Minister for Home Affairs Clare O'Neil unveiled.

> *The cyber security strategy will help Australia bring the whole nation into the fight to help protect our citizens and to protect our economy.*

The strategy will be led by former Telstra CEO Andrew Penn, Cyber Security Cooperative Research Centre CEO Rachael Falk and retired Air Force chief Mel Hupfeld, who will be supported by Minister for Finance Katy Gallagher and Minister for Home Affairs Clare O'Neil. The strategy will also involve an international panel led by Professor Ciaran Martin, who founded the UK's National Cyber Security Centre (NCSC) with the aim of helping Australia protect its citizens and economy, strengthen critical infrastructure and government networks, build sovereign capabilities and strengthen international engagement.

The original and complete article can be found here.

Technology

Microsoft Cyber Signals, third edition — Insights into IT, IoT and OT risks

The announcement can be found here — it highlights the core lenses available in the report:

> *Microsoft has released its third edition of Cyber Signals, a regular cyberthreat intelligence brief spotlighting security trends and insights gathered from Microsoft's 43 trillion daily security signals and 8,500 security experts. This edition highlights new insights on the wider risks that converging IT, Internet-of-Things (IoT), and Operational Technology (OT) systems pose to critical infrastructure, and how enterprises can defend against these attacks.*

Definitely worth the read.

A look at up-and-coming new companies in Cloud and Security in 2022

CRN (A channel focused publication) published a list with ITS OWN top 10 products for multiple needs, for the year of 2022. While I'm unsure what these lists are based off of (not necessarily performance nor price or even technology). It's good to be aware some different companies in different technological (including Cloud security) segments.

> I didn't see Microsoft under Cloud Security and personally can't fathom why since it's a leader in many Cyber & Cloud security segments according to analysts and large Enterprise customers.

Find the list of lists, here: 2022 Year In Review | CRN

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.

Cybersecurity Report Strategy Newsletter

Written by Andre Camillo, CISSP

Edit profile

1K Followers · Writer for Geek Culture

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