

# Strategic Cyber Security Report — June 2023 Edition



Andre Camillo, CISSP

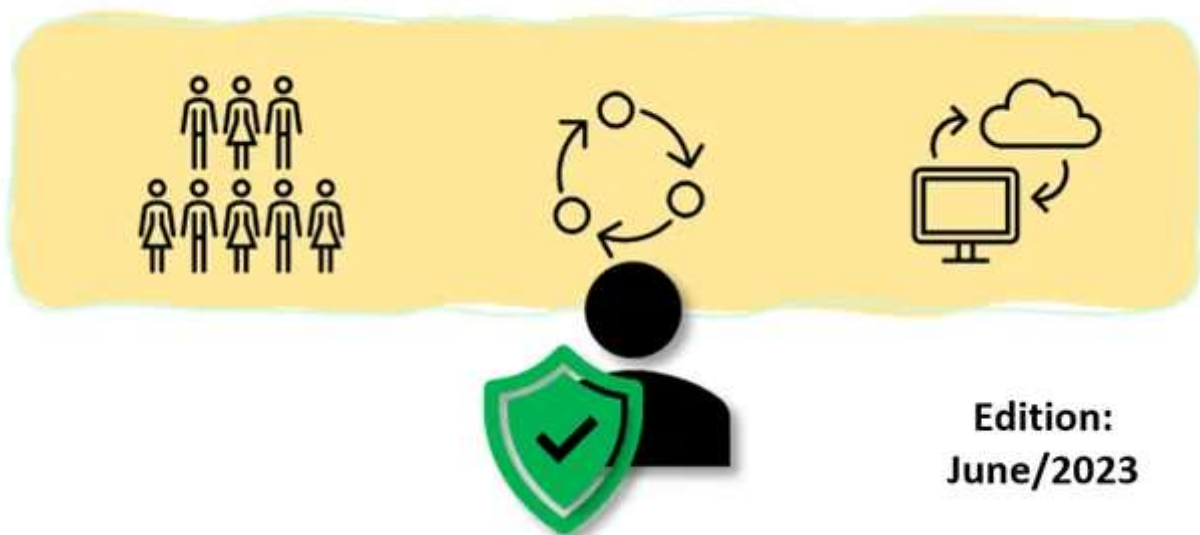
Published in CloudnSec · 5 min read · Jul 2, 2023



4



A Monthly summary of Strategic Information for Cyber Security Leaders



**Edition:  
June/2023**

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.

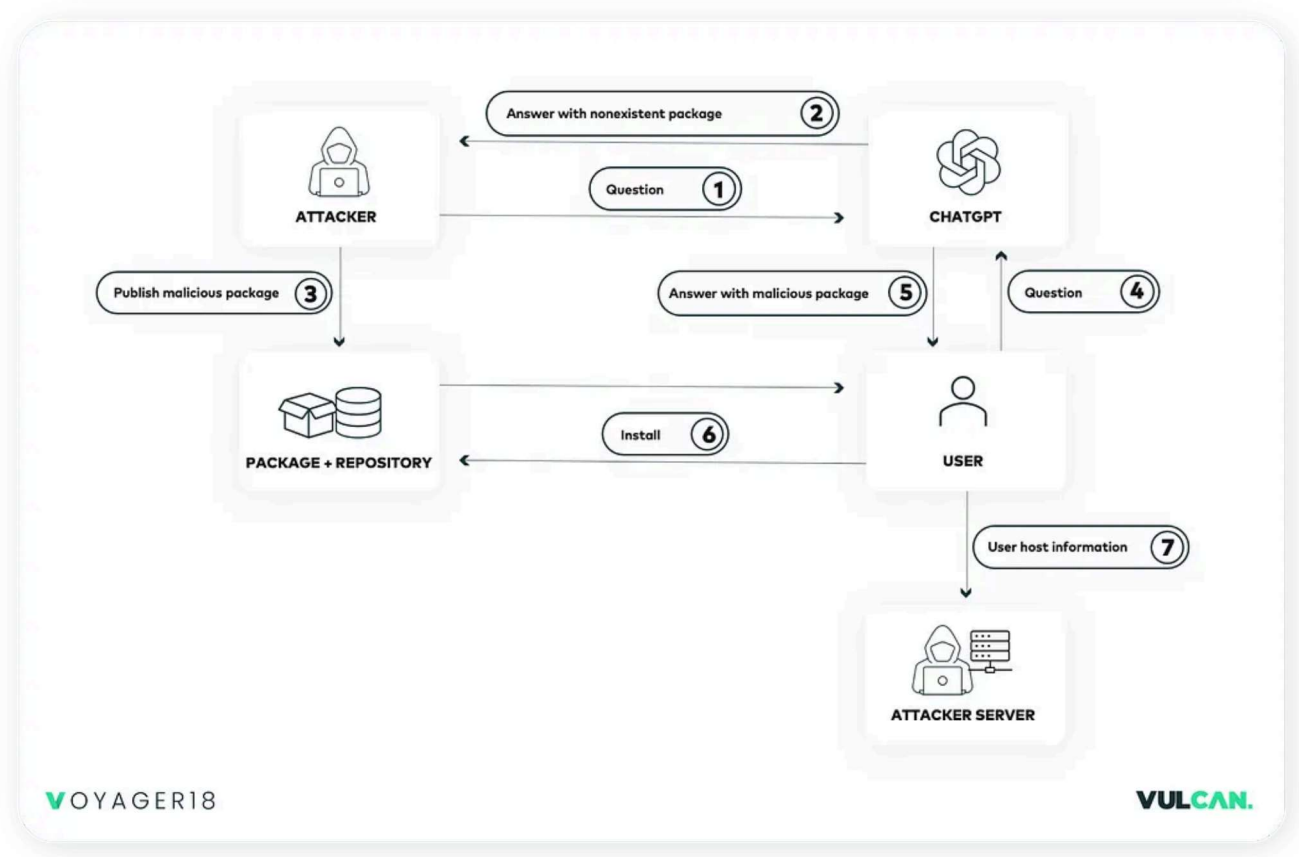
## People

### **New attacks based on AI hallucination — “Halluhack”?**

Reports from Vulcan ([source here](#)) indicate a new attack method leveraging a very common occurrence in popular LLM AI models, such as ChatGPT, for instance.

Attackers can learn from LLMs what inexistent code packages are recommended by the platform (in an episode of hallucination). Attackers can then upload malicious code fronting with these fake packages to public code repos.

Regular LLM AI users who go looking for code package recommendations might be recommended the hallucinated packages and then look for the fake package in public repos, thus getting hacked.



Other news outlets have reported this as well:

[ChatGPT's False Information Generation Enables Code Malware \(hackread.com\)](#)

[Cybercrooks Scrape OpenAI API Keys to Pirate GPT-4 \(darkreading.com\)](#)

Let's ensure our users are well trained before allowing them to use AI for development.

## Microsoft Cyber Signals Report

Microsoft released a new report with findings of the frontlines looking at Microsoft Threat Intelligence stats from April 2022 to April 2023. The Cyber

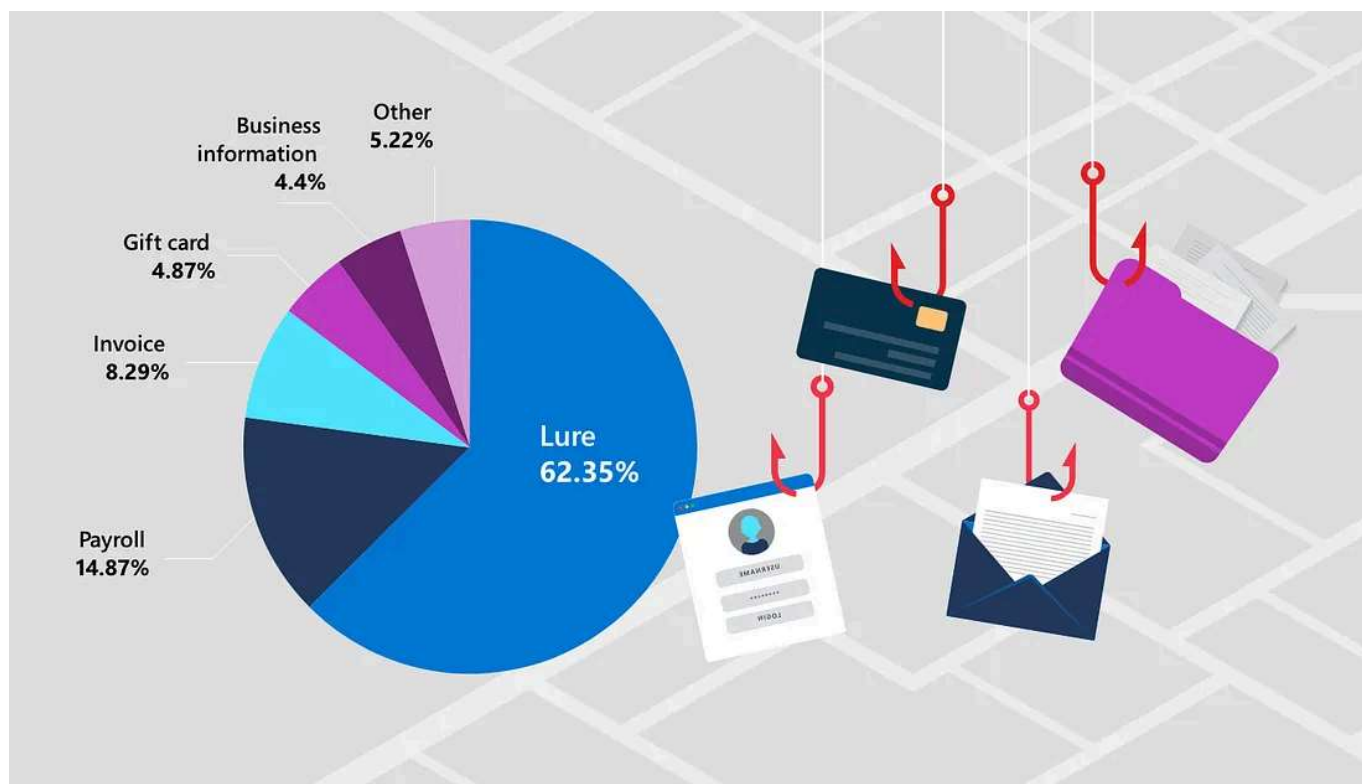
Signals report number 4 focuses on Phishing, Business Email Compromise campaigns and measures to mitigate these risks. The page states:

*Microsoft has observed an increase in sophistication and tactics by threat actors specializing in business email compromise (BEC), including leveraging residential internet protocol (IP) addresses to make attack campaigns appear locally generated.*

One of the key takeaways from the report was that there was significant raise in Cybercrime-as-a-service targeting business emails — the report states:

*Microsoft's Digital Crimes Unit has observed a 38 percent increase in Cybercrime-as-a-Service targeting business email between 2019 and 2022.*

BEC by email type is represented by the report:



source: [Microsoft Cyber Signals Report 4](#). Data represents a snapshot of BEC phishing by type January 2023 through April 2023

The report's methodology is disclosed and extremely appreciated:

*Methodology: For snapshot data, Microsoft platforms including Microsoft Defender for Office, Microsoft Threat Intelligence, and Microsoft Digital Crimes Unit (DCU) provided anonymized data on device vulnerabilities and data on threat actor activity and trends. In addition, researchers used data from public sources, such as the Federal Bureau of Investigation (FBI) 2022 Internet Crime Report and Cybersecurity & Infrastructure Security Agency (CISA)*

Read the [full report here](#).

## **Process**

### **Artificial Intelligence Regulation in EU**

The AI Act from Europe aims at regulating some AI aspects.

Where this comes from? European parliament explains:

*In April 2021, the European Commission proposed the first EU regulatory framework for AI. It says that AI systems that can be used in different applications are analysed and classified according to the risk they pose to users. The different risk levels will mean more or less regulation. Once approved, these will be the world's first rules on AI.*

The 2023 AI act aims at:

*The new rules establish obligations for providers and users depending on the level of risk from artificial intelligence. While many AI systems pose minimal risk, they*

---

*need to be assessed.*

---

The Act proposes banning AI for use cases with “Unacceptable risk” — determined by threats it poses to people, which include:

---

*Cognitive behavioural manipulation of people or specific vulnerable groups: for example voice-activated toys that encourage dangerous behaviour in children*

*Social scoring: classifying people based on behaviour, socio-economic status or personal characteristics.*

*Real-time and remote biometric identification systems, such as facial recognition*

---

Then, “High risk” applications — defined by “negatively affect safety or fundamental rights”, will be assessed before being put on the market.

A full list of what categories are included in High risk can be found in the original article, [here](#).

The goal of the EU Parliament is now to talk to EU countries and counties and reach an agreement by the end of 2023.

This comes as a reflection of EU’s failure to regulate past waves of big tech, such as social media. This failure, some experts argue, led to risks to youth and society that could have been mitigated were it somewhat regulated.

### **MITRE paper on Regulatory Framework for AI Security**

This should be a relevant paper for all of us — MITRE’s “*Regulatory Framework for AI Security*”. According to them:

“This paper explores potential options for AI regulation and makes recommendations on how to establish guardrails to shape the development and use of AI.”

The paper summarizes threats and risks that AI poses to environments, strictly to IT and cyber security perspectives — it does not look at AI from a sociological standpoint.

It then talks about Regulatory approaches that could be taken into account for AI.

It then presents a “table that highlights the three that are most critical for immediate action”:

	AI Vulnerabilities	AI Threats	AI Risks
AI as a Subsystem	Reduce vulnerabilities by enhancing industry-specific approaches		
AI Augmenting Humans		Limit threat and hence risk scaling through human penalty, supported by increased auditability	
AI with Agency			Reduce risks via critical infrastructure hardening and enable safe research

Access the full document for details on each of the above, and much more.  
[Read the full article here.](#)

## Technology

### Forrester Wave for Enterprise Email Security Q2 23

Forrester has analysed cyber security vendors for Email Security and made comments to the top 15 providers in the latest “Enterprise Email security Forrester Wave for Q2, 2023”.

The official public report is available here: [The Forrester Wave™: Enterprise Email Security, Q2 2023](#)

They call out that the industry has mature and has entered a golden age. The exact words are:

*“Email security is now entering a golden age after stagnating for the better part of a decade. Mass customer migration to cloud email, rapid adoption of machine learning, and the widespread use of APIs to connect systems and share data have brought forth improved offerings and capabilities and innovative roadmaps from legacy providers and newer players.”*

They mention that most customers are using a combination of security vendors in the space — and according to customers this provides greater efficacy.



*“of the 37 customer references interviewed for this research, only two were working with a single enterprise email security vendor.”*

---

They then make recommendations as to what customers of these solutions should be looking for:

- **Offer flexibility in deployments and integrations.**
- **Make it easy for security teams to respond.**
- **Look beyond email to deliver holistic human protection.**

[Access the full report with all vendor scores and comments by Forrester here.](#)

Figure 1

Forrester Wave™: Enterprise Email Security, Q2 2023

## THE FORRESTER WAVE™

Enterprise Email Security

Q2 2023



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: [Forrester](#)

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

Strategy

Microsoft

Security

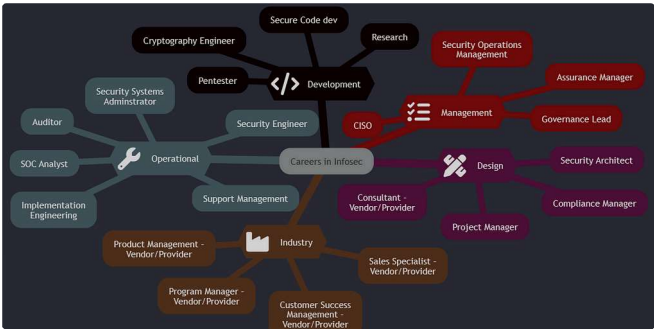



**Written by Andre Camillo, CISSP**

Edit profile

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 CloudnSec




 Andre Camillo, CISSP in CloudnSec

Cybersecurity Careers and Jobs for 2024

I've recently had the chance to talk about Diversity & Inclusion & the cyber security fiel...

🌟 Feb 21 🖱️ 52 💬 2 📌 ⋮

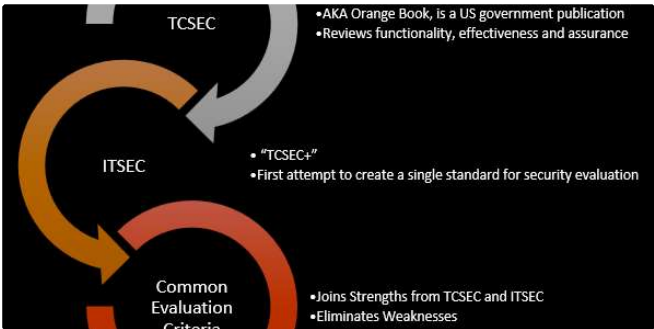



 Andre Camillo, CISSP in CloudnSec

Microsoft Defender Threat Intelligence—All you need to get...

Since Microsoft Ignite 2023, Microsoft Defender Threat Intelligence has had a “Free...

🌟 Apr 5 🖱️ 21 📌 ⋮




 Andre Camillo, CISSP in CloudnSec

Security Architecture & Evaluation Criteria Framework | CISSP Bits

The Common Criteria as a Global Standard for Cybersecurity



 Andre Camillo, CISSP in CloudnSec

Microsoft Defender for Endpoint on Linux—Manual Scan Tips

Deploying and managing Defender for Endpoint on linux at Scale is something you'l...