IBM Randori

IBM's approach to Attack Surface Management

tomasz.zalewski@pl.ibm.com

What ASM solutions do?

First:

It finds all external targets – as seen by attacker

Why is it important?

- Shadow IT
- Zombie IT

How discovery works?

Just enter e-mail address

We analyse: business intelligence databases, DNZ zones, IP topology, whois, certificates, web pages content, etc

We run an undetected scan

What Randori does?

Second:

Prioritizes targets based on how tempting they are to attacker

What are “temptation” criteria?

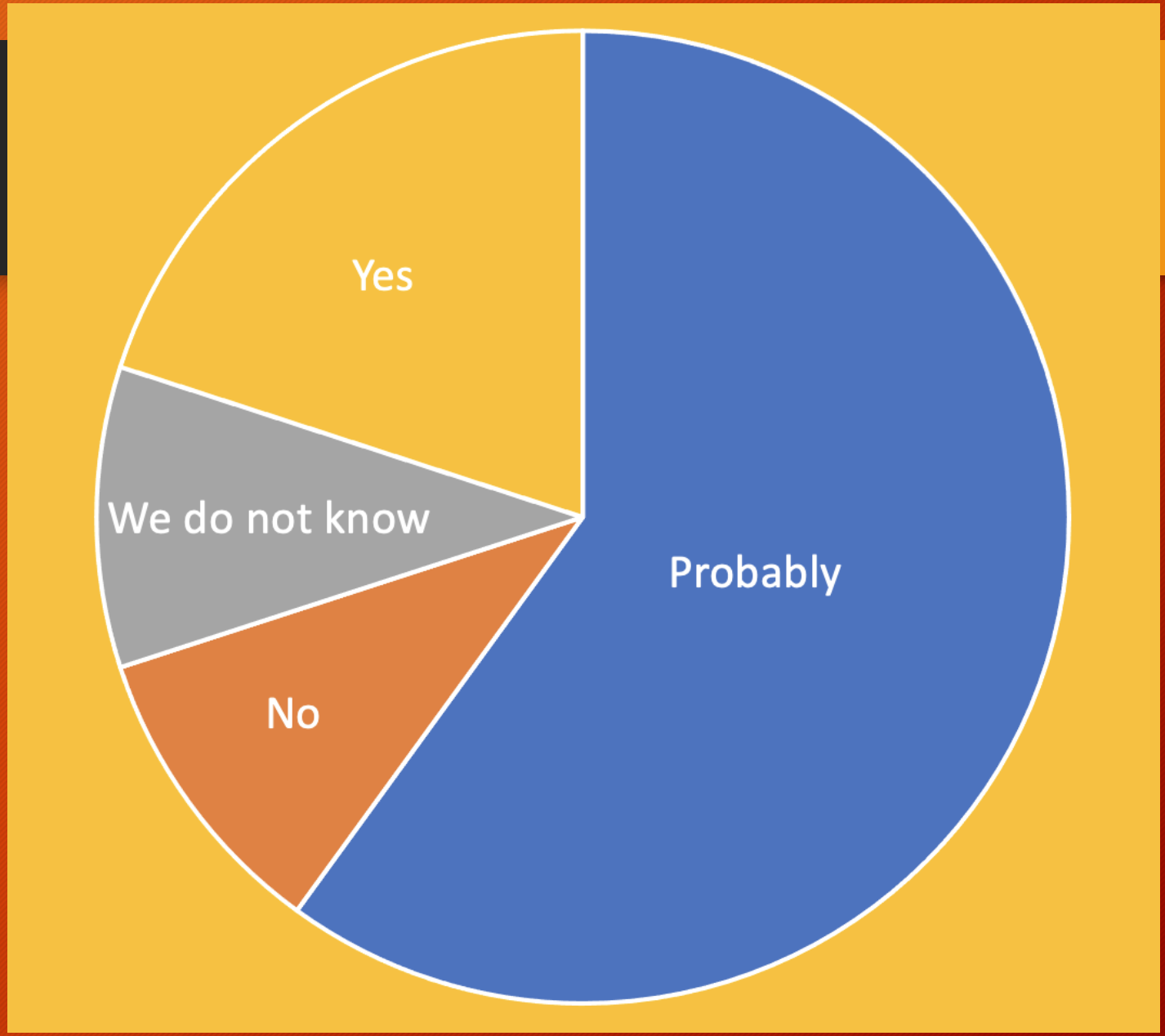
- Is the solution popular?
- Is target critical?
- Do we know version accurately?
- Do we have exploit?
- Can we prepare a “zero-day”?
- Can we orchestrate another attack?

But somehow they, @#$%, get in!

I dedided to check!

Here are 10 biggest incidents in 2022 according to Security Magazine

Can ASM deal with this?



Presenting for a first time…

10 biggest security incidents 2023!

https://www.welivesecurity.com/en/cybersecurity/year-review-10-biggest-security-incidents-2023/

MOVEit

- File transfer service
- 2600 organisations / 83M individuals impacted
- Attack vector:

zero-day vulnerability

UK Electoral Comission

- PI of 40M voters leaked
- Attack vector: unpatched MS Exchange Server

Nothern Ireland Police

- 10K staff data leaked (incl. surveillance and intelligence)
- Two alleged terrorists had to be released
- Attack vector:

employee accidentally posted sensitive internal data to the WhatDoTheyKnow website in response to a Freedom of Information (FOI) request

DarkBeam

- Supplier cyber risk management (!)
- 3.8B ($3.8*10^9$) records leaked
- Attack vector: exposed ELK interface

Indian Council of Medical Research

- PI of 815M
- Attack vector: not disclosed

23andMe

- Genetics research company
- *stolen as many as 20 million pieces of data*
- Attack vector: credential stuffing

Multiple companies

- Rapid Reset DDOS
- Attack vector: HTTP/2 vulnerability

T-Mobile

- 37M customers impacted
- Attack vector:

On January 5, 2023, T-Mobile US, Inc. (the "Company," "we," or "our") identified that a bad actor was obtaining data through a single Application Programming Interface ("API") without authorization.

MGM International/Cesars

- Casinos
- 115M$ cost
- Attack vector: vishing

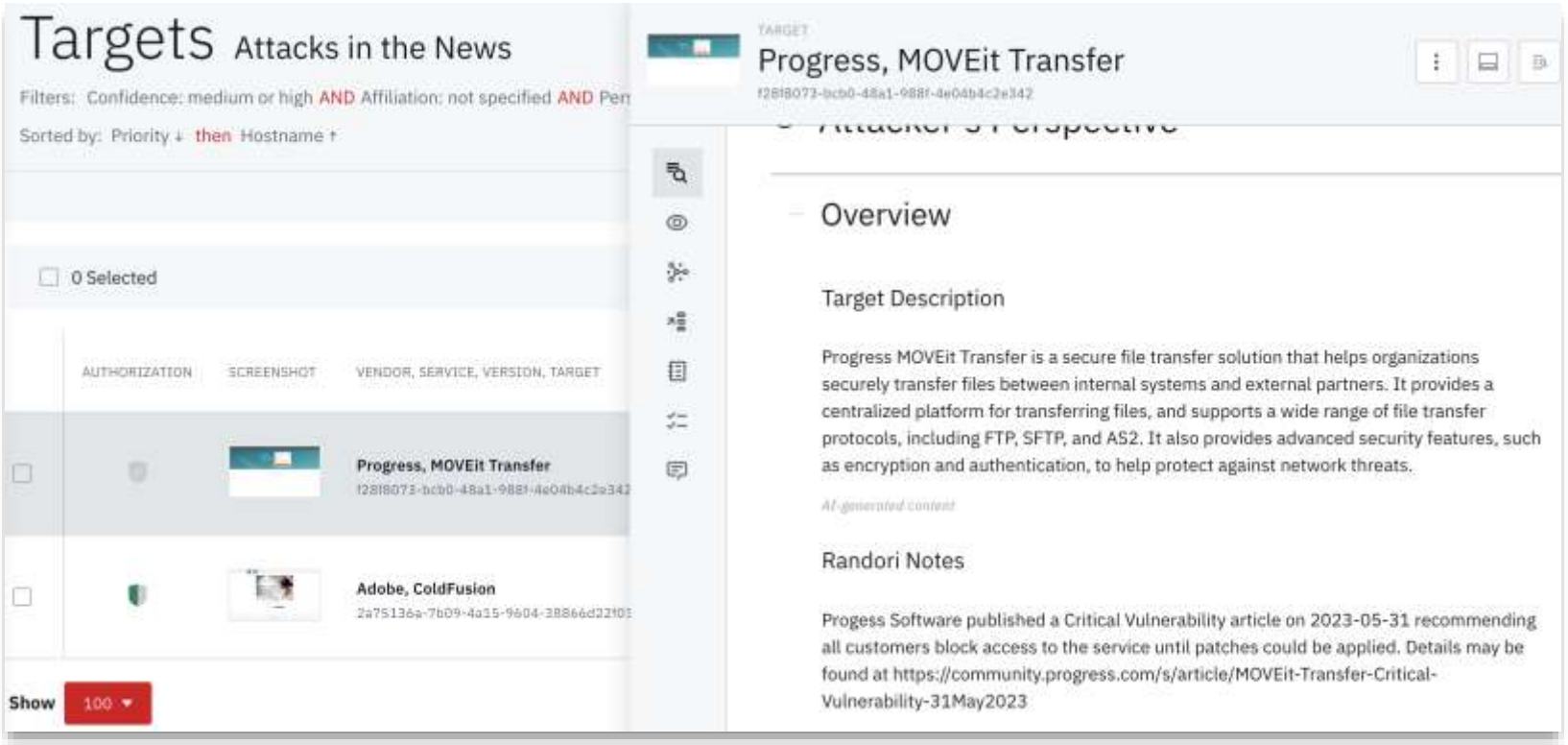
Pentagon

- *gave Russia a treasure trove of military intelligence for its war in Ukraine and undermined America's relationship with its allies*
- Attack vector:

21-year-old member of the intelligence wing of the Massachusetts Air National Guard, Jack Teixeira, leaked highly sensitive military documents to gain bragging rights with his Discord community

Could Randori have helped?

- 3 cases: Human action (intended and unintended leak, vishing)
- 2 cases: known vulnerability (Exchange, HTTP/2)
- 2 cases: exposed services (ELK, API)
- 1 case: attack vector not disclosed
- 1 case: credential stuffing
- 1 case: zero-day vulnerability

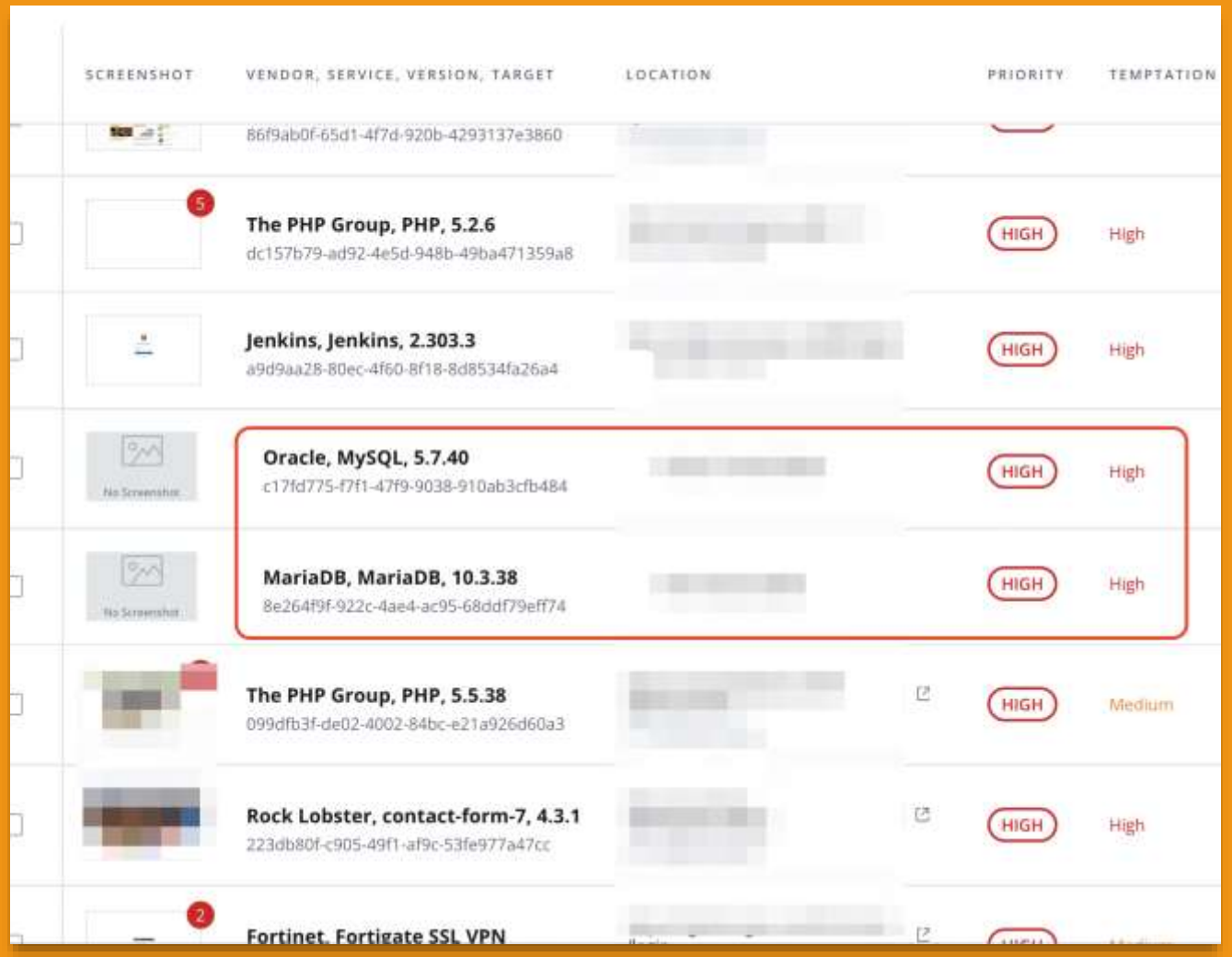


Known vulnerability?

A classis Randori use case

Exposed services?

A classic Randori use case



Credential stuffing

- Randori Attack (full pentest platform) checks leaked passwords too!

BTW… our real-life findings…

- Folder with important files (no authentication)
- Gambling and porn webpage z hosted in customer domain
- Network monitoring system interface
- EOL 2016
- Unencrypted login
- VNC, RDP, SSH…
- Open space webcam

Could Randori have helped?

2 cases: known vulnerability (Exchange, HTTP/2)

2 cases: exposed services (ELK, API)

1 case: credential stuffing

Could vulnerability scanner have helped?

2 cases: known vulnerability (Exchange, HTTP/2)

IBM Security Randori,
An Offensive Security Platform

Interested?

Let’s check your attack surface