

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!

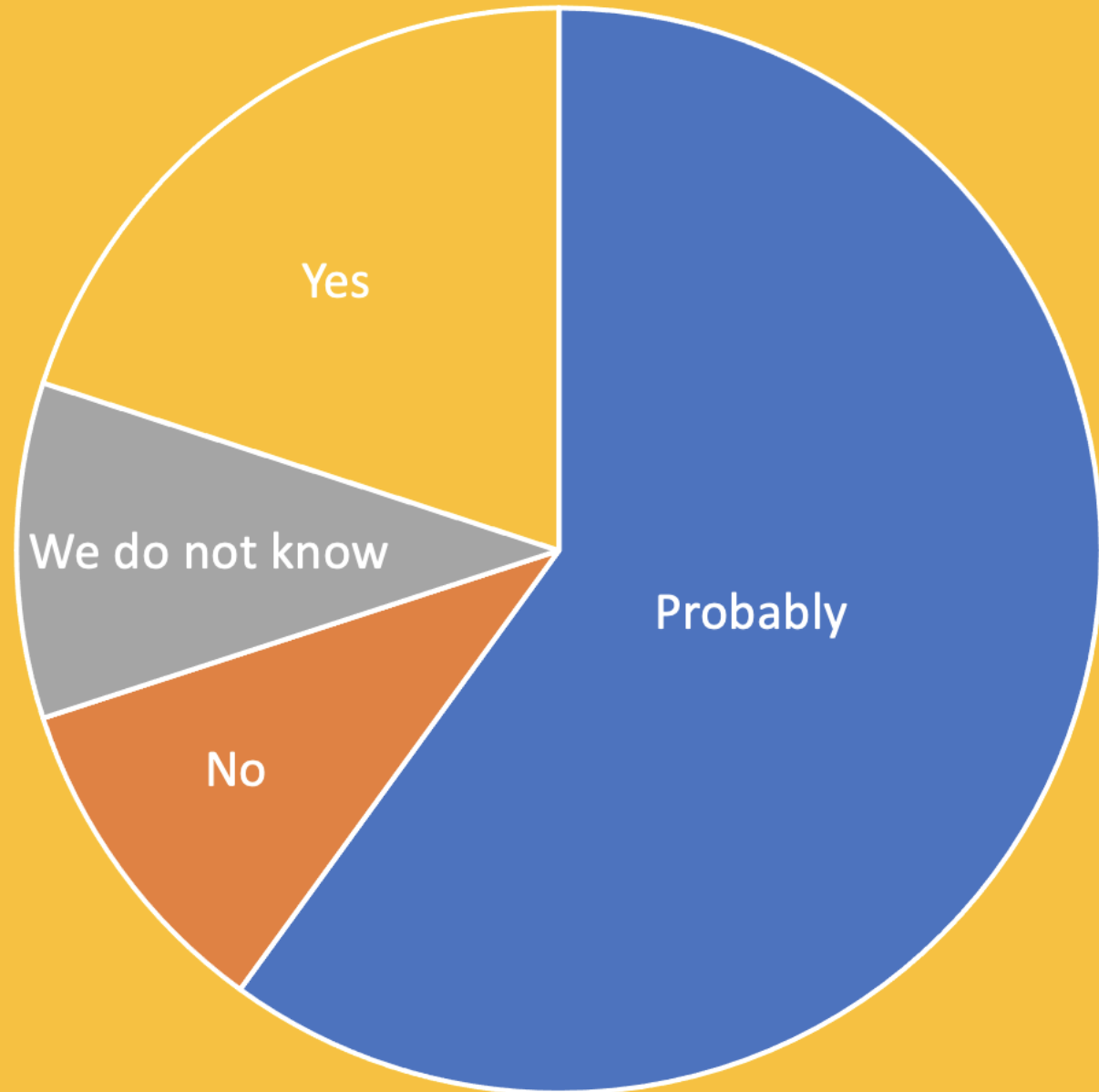


I dedided to check!

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/](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 Commission

- 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 ($3.8 \cdot 10^9$) 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

The screenshot displays a security tool interface with a 'Targets' section on the left and a detailed view on the right. The 'Targets' section is titled 'Attacks in the News' and includes filters for 'Confidence: medium or high AND Affiliation: not specified AND Pen' and sorting options for 'Priority' and 'then Hostname'. A table lists two targets: 'Progress, MOVEit Transfer' and 'Adobe, ColdFusion'. The detailed view for 'Progress, MOVEit Transfer' shows an 'Overview' section with a 'Target Description' and 'Randori Notes'. The description states that Progress MOVEit Transfer is a secure file transfer solution. The notes mention a critical vulnerability article published by Progress Software on 2023-05-31.

	AUTHORIZATION	SCREENSHOT	VENDOR, SERVICE, VERSION, TARGET
<input type="checkbox"/>			Progress, MOVEit Transfer f2818073-bcb0-48a1-988f-4e04b4c2e342
<input type="checkbox"/>			Adobe, ColdFusion 2a75136a-7b09-4a15-9604-38866d32101

Progress, MOVEit Transfer
f2818073-bcb0-48a1-988f-4e04b4c2e342

Overview

Target Description

Progress MOVEit Transfer is a secure file transfer solution that helps organizations securely transfer files between internal systems and external partners. It provides a centralized platform for transferring files, and supports a wide range of file transfer protocols, including FTP, SFTP, and AS2. It also provides advanced security features, such as encryption and authentication, to help protect against network threats.

AI-generated content

Randori Notes


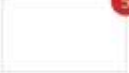






Progress Software published a Critical Vulnerability article on 2023-05-31 recommending all customers block access to the service until patches could be applied. Details may be found at <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023>

Known vulnerability?

A classis Randori use case

Exposed services?

A classic Randori use case

SCREENSHOT	VENDOR, SERVICE, VERSION, TARGET	LOCATION	PRIORITY	TEMPTATION
	86f9ab0f-65d1-4f7d-920b-4293137e3860	[REDACTED]	[REDACTED]	[REDACTED]
	The PHP Group, PHP, 5.2.6 dc157b79-ad92-4e5d-948b-49ba471359a8	[REDACTED]	HIGH	High
	Jenkins, Jenkins, 2.303.3 a9d9aa28-80ec-4f60-8f18-8d8534fa26a4	[REDACTED]	HIGH	High
	Oracle, MySQL, 5.7.40 c17fd775-f7f1-47f9-9038-910ab3cfb484	[REDACTED]	HIGH	High
	MariaDB, MariaDB, 10.3.38 8e264f9f-922c-4ae4-ac95-68ddf79eff74	[REDACTED]	HIGH	High
	The PHP Group, PHP, 5.5.38 099dfb3f-de02-4002-84bc-e21a926d60a3	[REDACTED]	HIGH	Medium
	Rock Lobster, contact-form-7, 4.3.1 223db80f-c905-49f1-af9c-53fe977a47cc	[REDACTED]	HIGH	High
	Fortinet, Fortigate SSL VPN	[REDACTED]	[REDACTED]	[REDACTED]

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