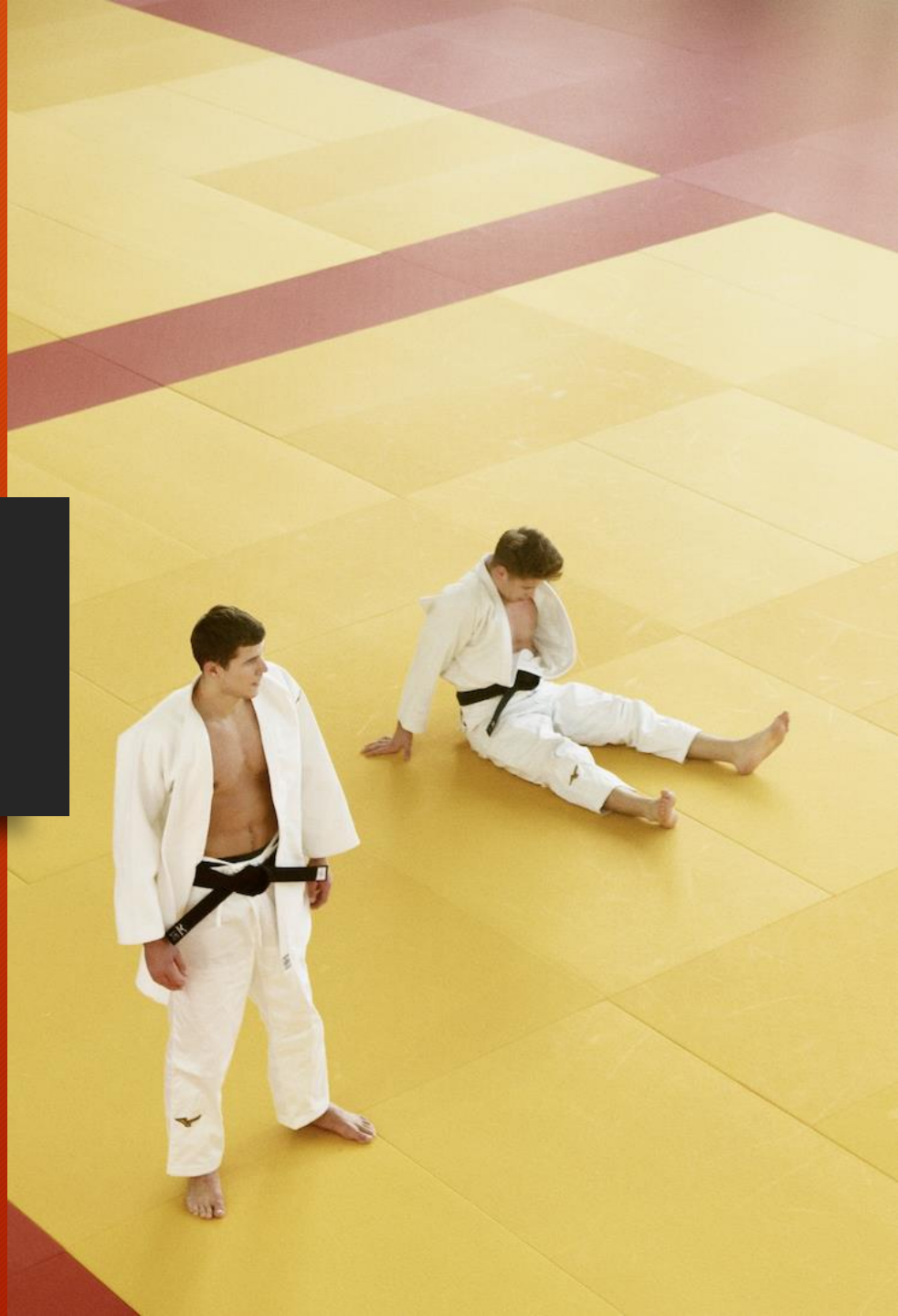
Randori
A year later

Biggest security incidents in 2022.

Could be avoided with Attack Surface Management?

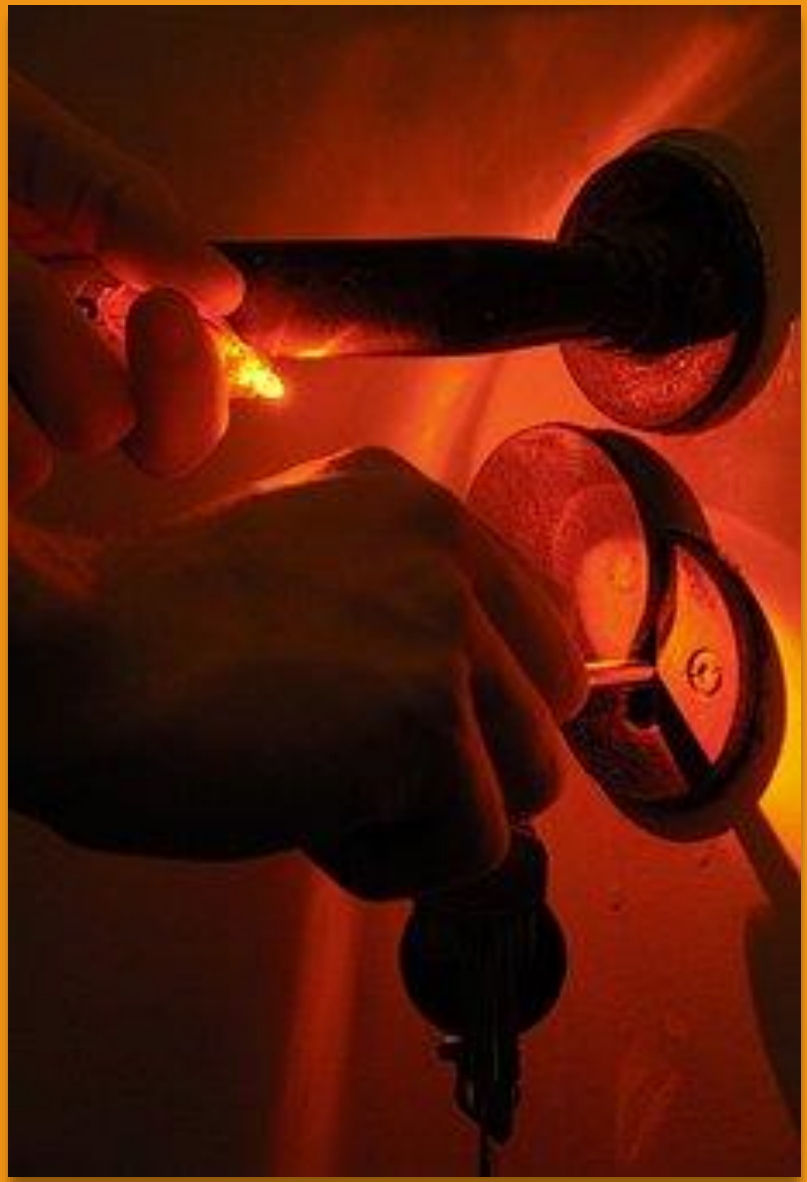


tomasz.zalewski@pl.ibm.com

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

I dedided to check!

Here are 10 biggest incidents in 2022 according to Security Magazine



10. SuperVPN, GeckoVPN i ChatVPN

- VPN services
- Data of 21M users (names, payment data, paswords etc)
- Attack vector:

threat actor claims that the data has been exfiltrated from publicly available databases that were left vulnerable by the VPN providers due to developers leaving default database credentials in use

9. Costa Rica government

- Government services ransomware
- 670 GB of data revealed
- National emergency
- Billions of dolars lost
- Attack vector: stolen password

8. Neopets

- Internet game
- Data of 69M users (names, addresses, birth dates etc)
- Attack vector: unknown

7. Twitter

- Data of 5.4M users (e-mail addresses, phone numbers etc)
- Attack vector:

Twitter API vulnerability disclosed in a bug bounty program

6. Uber

- Data of 57M users was not revealed – Uber paid 100k ransom
- CISO found guilty of criminal charges (hiding incident) – first such case
- Attack vector: stolen password

5. Twilio

- Messaging
- Data of 209 customers stolen
- Attack vector: stolen password (phishing)

4. DoorDash

- Food industry
- Data of 4.9M customers, employees, providers (names, addresses, e-mail addresses, phone numbers)
- Attack vector: stolen password

3. Optus

- Telecommunication
- Data of 21M users (names, payment data, passwords etc)
- Attack vector:

data breach occurred through an unprotected and publically exposed API. This API didn't require user authentication before facilitating a connection. A lack of an authentication policy meant anyone that discovered the API on the internet could connect to it without submitting a username or password

2. Los Angeles Unified School District

- 500 GB of data including: SSNs, passport numbers, tax forms, financial reports, bank account numbers, health data, criminal records, personality test data
- Attack vector: stolen password

1. Medibank

- Biggest Australian health insurance company
- Data of 9.7M customers
- Attack vector: stolen password

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?

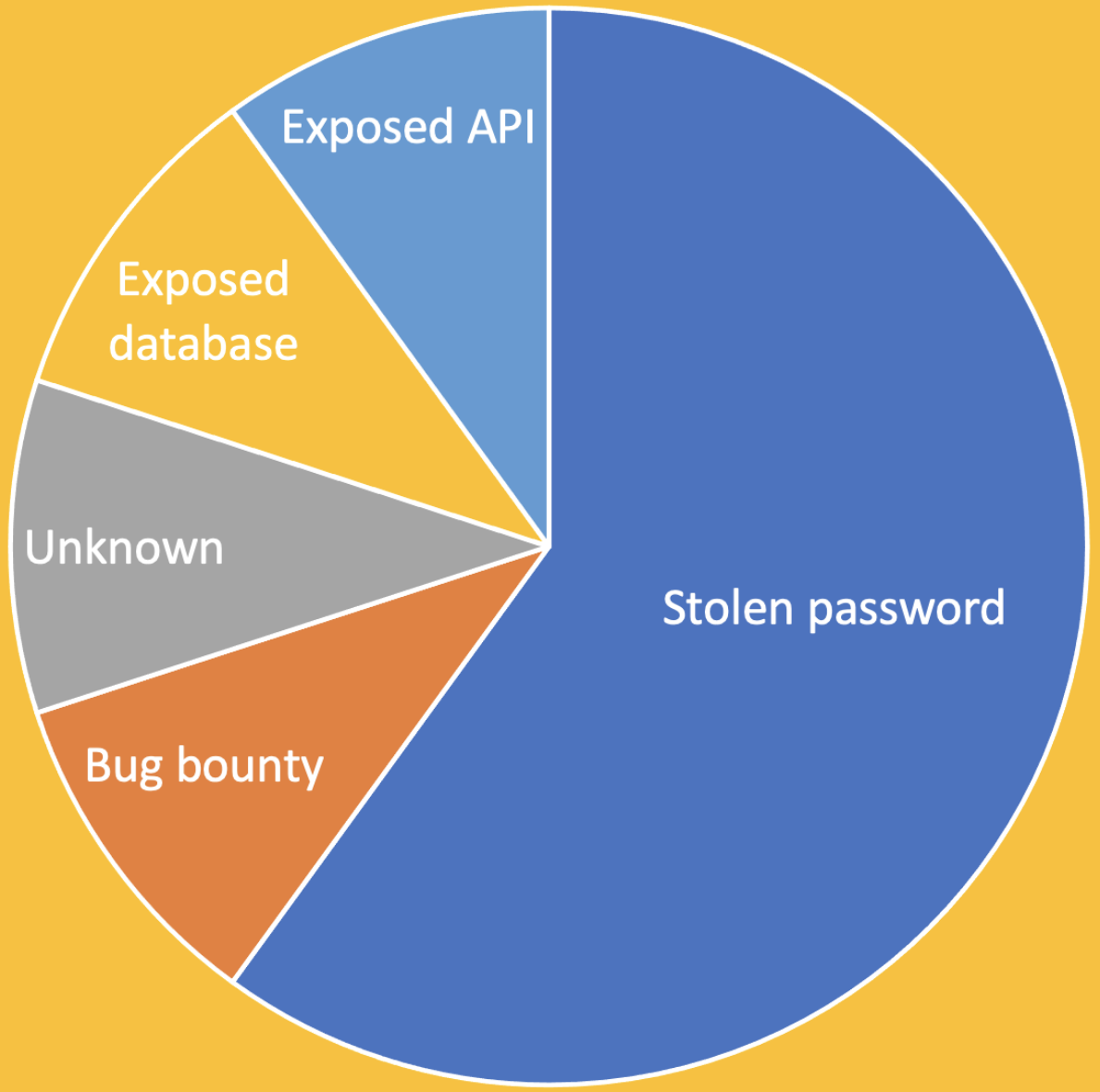
Second:

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?

Can ASM deal with this?



Exposed DB and API?

This is classic Randori use case

SCREENSHOT	VENDOR, SERVICE, VERSION, TARGET	LOCATION	PRIORITY	TEMPTATION
	86f9ab0f-65d1-4f7d-920b-4293137e3860			
5	**The PHP Group, PHP, 5.2.6** dc157b79-ad92-4e5d-948b-49ba471359a8		HIGH	High
	Jenkins, Jenkins, 2.303.3 a9d9aa28-80ec-4f60-8f18-8d8534fa26a4		HIGH	High
No Screenshot	**Oracle, MySQL, 5.7.40** c17fd775-f7f1-47f9-9038-910ab3cfb484		HIGH	High
No Screenshot	**MariaDB, MariaDB, 10.3.38** 8e264f9f-922c-4ae4-ac95-68ddf79eff74		HIGH	High
	The PHP Group, PHP, 5.5.38 099dfb3f-de02-4002-84bc-e21a926d60a3		HIGH	Medium
	Rock Lobster, contact-form-7, 4.3.1 223db80f-c905-49f1-af9c-53fe977a47cc		HIGH	High
2	**Fortinet, Fortigate SSL VPN**			

BTW… our last month 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

Stolen password

- Two options:
  - Password DB bought on darknet
  - Phishing

How to protect password?

- Check “the lock”
- Check “hostname”
- Do not re-use password
- Which of above rules IT guys do not care about?

How about “the lock”?

- Two reasons why it is important:
  - Hackers are predators
  - How to boil a frog?

Hackers think they are predators

And we are prey

In fact they are predators

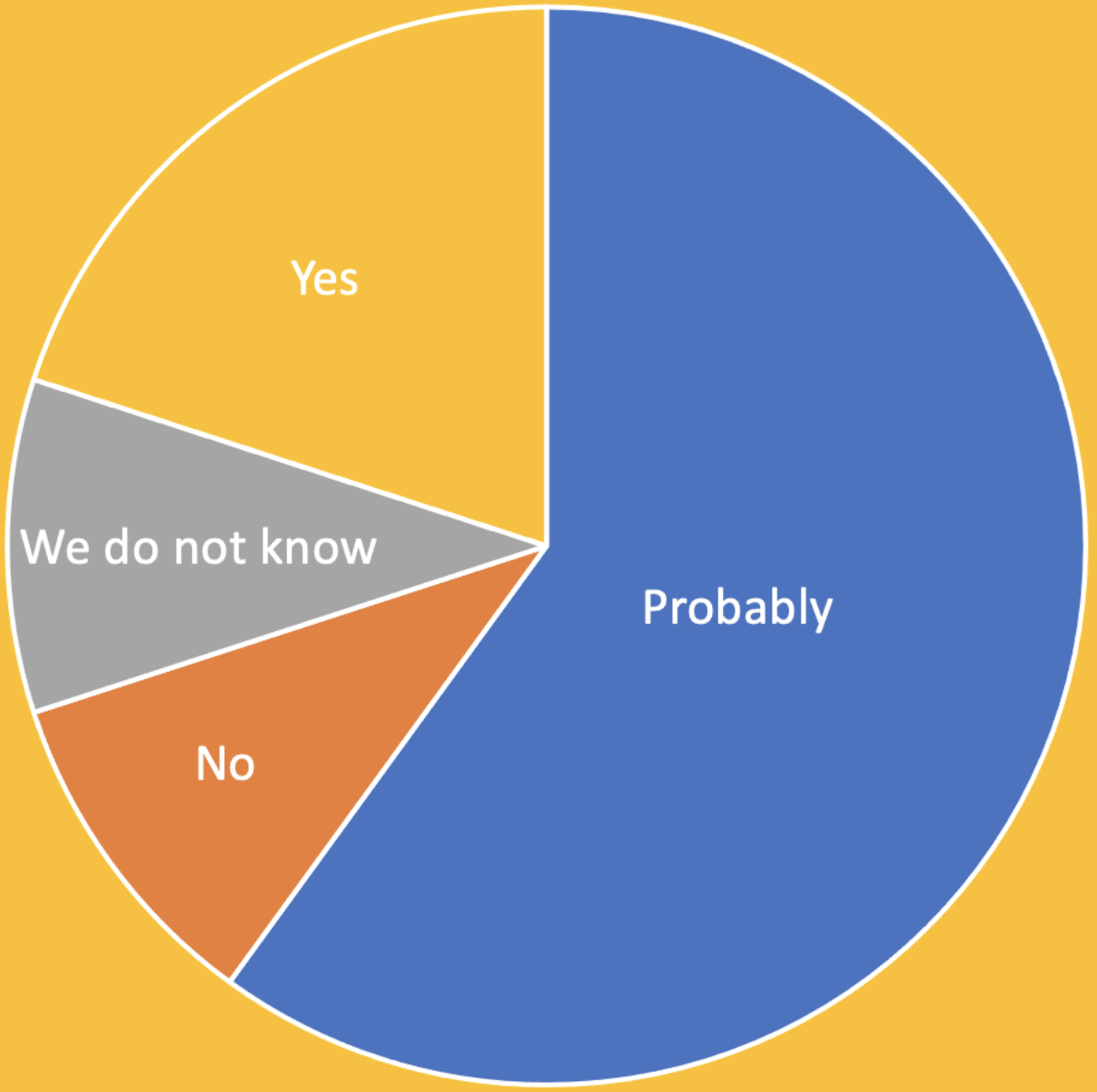
Because as every predator
they are lazy and opportunistic

They kill the weakest animal

How to boil a frog

Do not let your users and employees to get used to bad certificate hygiene!

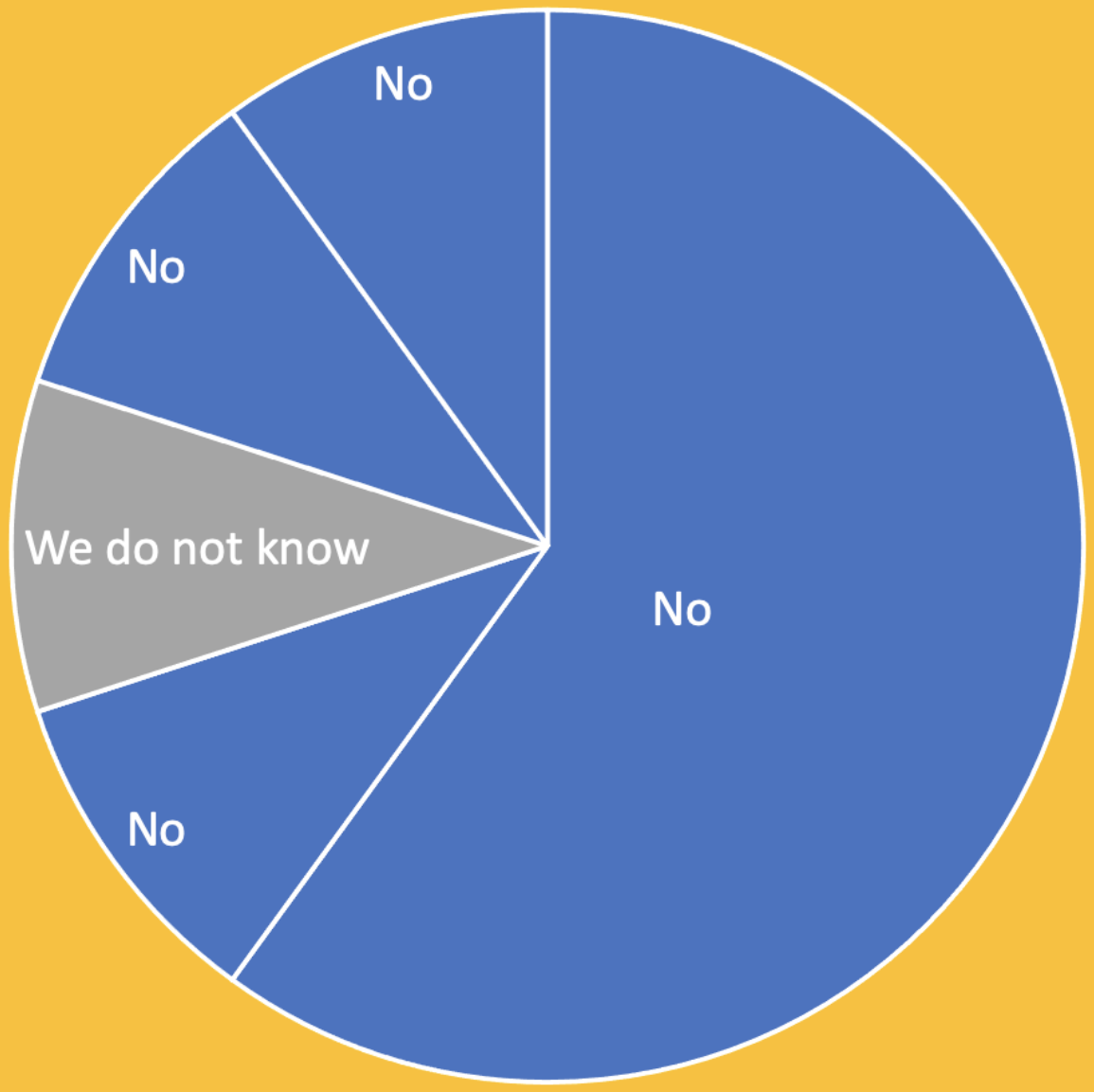
Can ASM deal with this?



“Buy I already own a VM scanner”

- The ones from “top 10” had these too
- Known vulnerabilities are a root cause of 7 to 26 % of incidents

Can VM scanner deal with this?



Hey, but my scanner also checks this…

- Yes, but it needs to know where to check
- First Randori!
- Then scanner!

30%

of assets are *unknown* or *unmanaged* to an organization due to rapid transformation.

FORRESTER

7 in 10

organizations have been compromised by an *unknown* or *unmanaged* asset in the past year.

ESG

Summary – what will Randori find?

- Vulnerable targets – if there are any
- Unknown targets – in initial scan
- New targets – on regular basis
- BAD IT HYGIENE – MOST IMPORTANT

So you “only” do reconnaissance?

- Not only!
- Randori Attack – full automated pentesting platform
- How does it work?
  - Run reconnaissance
  - Autorize targets to attack
  - Check if attack worked

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Randori | Dashboard

demo.randori.io/webernets-ibm/dashboard

Gmail YouTube Maps

Webernets - IBM

Search

DASHBOARD

ATTACK SURFACE
- Targets 58
- Services 36
- Detections 128

ATTACK ACTIVITY
- Runbooks 10
- Implants 3
- Redirectors 3

RISK MANAGEMENT
- Policies 10
- Reports 24

ACTIVE ASSETS
- Hostnames 41
- IP Addresses 13
- Networks 1
- Social 8

INTEGRATIONS
- Marketplace
- Recipes

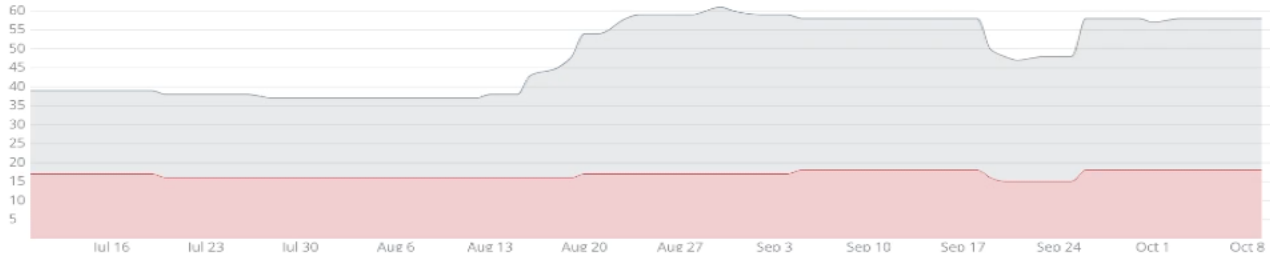
3	1	18	2	0
Implants	Target Needs Attention	High Priority Targets	Unknown Targets	New Targets
0 Delayed, 3 Checking-In	1 Needs Investigation	12 Hostnames 3 IPs		

Attack Surface Over Time

Over the Last Three Months

Targets	Services	Hostnames	IP Addresses	Networks
58	36	41	13	1
↑ 19	↓ 0	↓ 0	↑ 1	↑ 1

All Targets
High Priority Targets



Activity

Business Context | Attack Summary

0%
Targets Assigned Impact
Assign Additional Impact through Policies

2%
Targets Marked With Status
Mark Additional Status through Policies

Favorite Saved Views

Randori Saved Views | Other Saved Views

Attacks in the News	6
Domains	1
Domains Expiring/Expired	0
End-Of-Life Software	2
High Risk Ports	4
Interesting Hostnames	4
Potential Subdomain Takeover	0
Screenshot Not On 80/443	2
Unencrypted Login Pages	0

View All Randori Saved Views

Characteristics By Priority

Targets | Hostnames | IP Addresses

Login 12

NoCSS 11

Interested?

Let’s check your attack surface