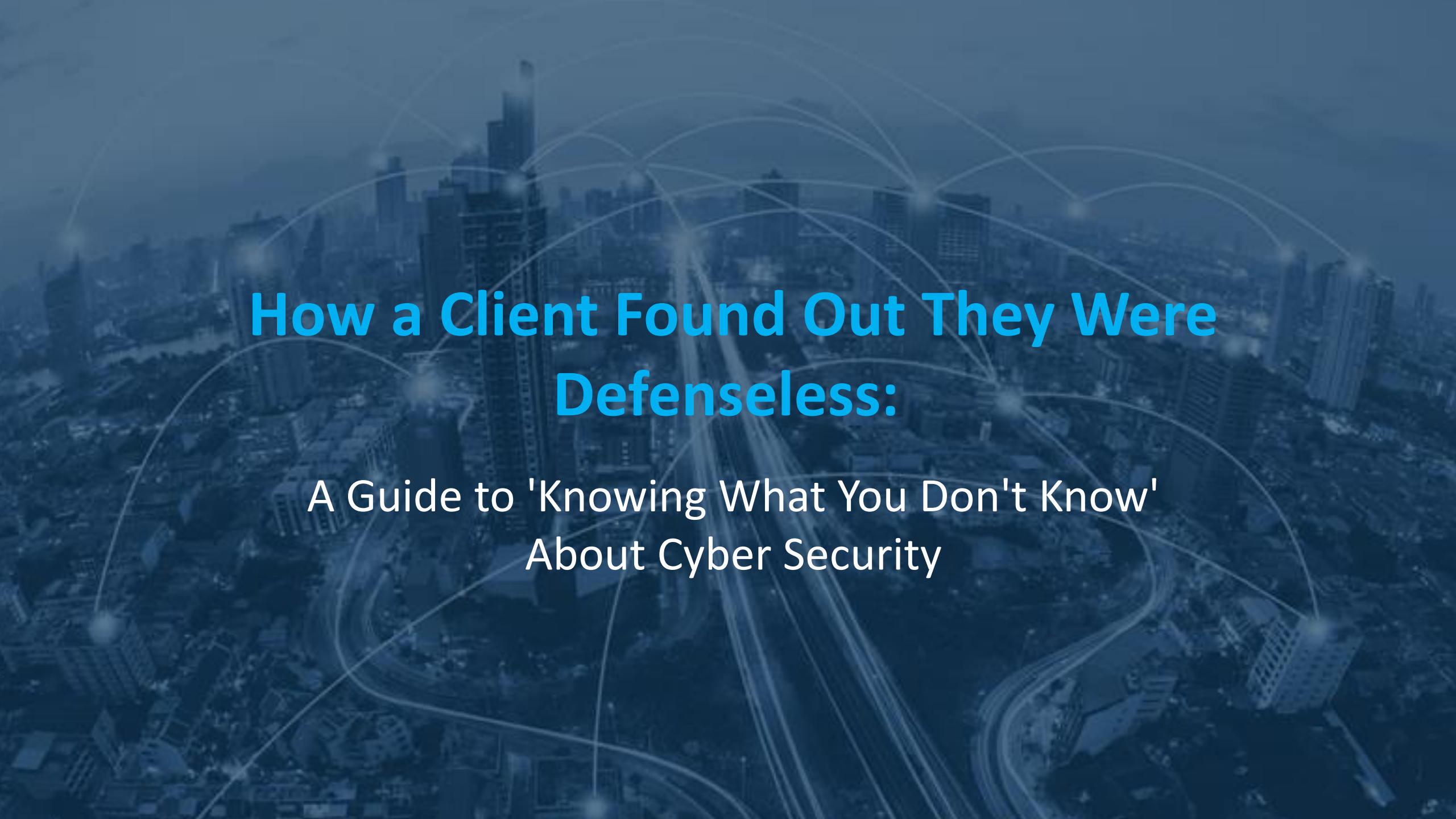

RIDGE·IT
GET CYBER READY
@RidgeITCorporation
www.RidgeIT.com
Sales@RidgeIT.com
844-743-4348



How a Client Found Out They Were Defenseless:

A Guide to 'Knowing What You Don't Know' About Cyber Security

IN PARTNERSHIP WITH:

PICUS + zscaler™

YOUR PANELISTS:

Chad Koslow
CEO
Ridge IT Corporation
@ChadKoslow

Perry Schumacher
CSO
Ridge IT Corporation
@PerrySchumacher

Trace Woodbury
CIO
Ridge IT Corporation
@TraceWoodbury

Volkan Erturk
Co-Founder & CTO
Picus Security
@VolkanErturk

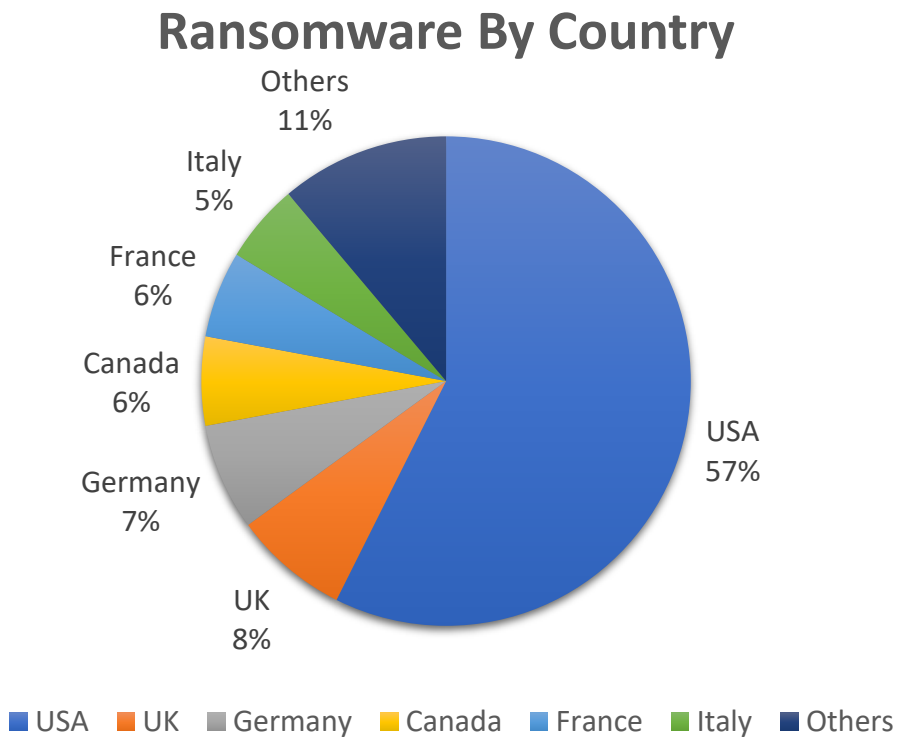
TODAY'S AGENDA:

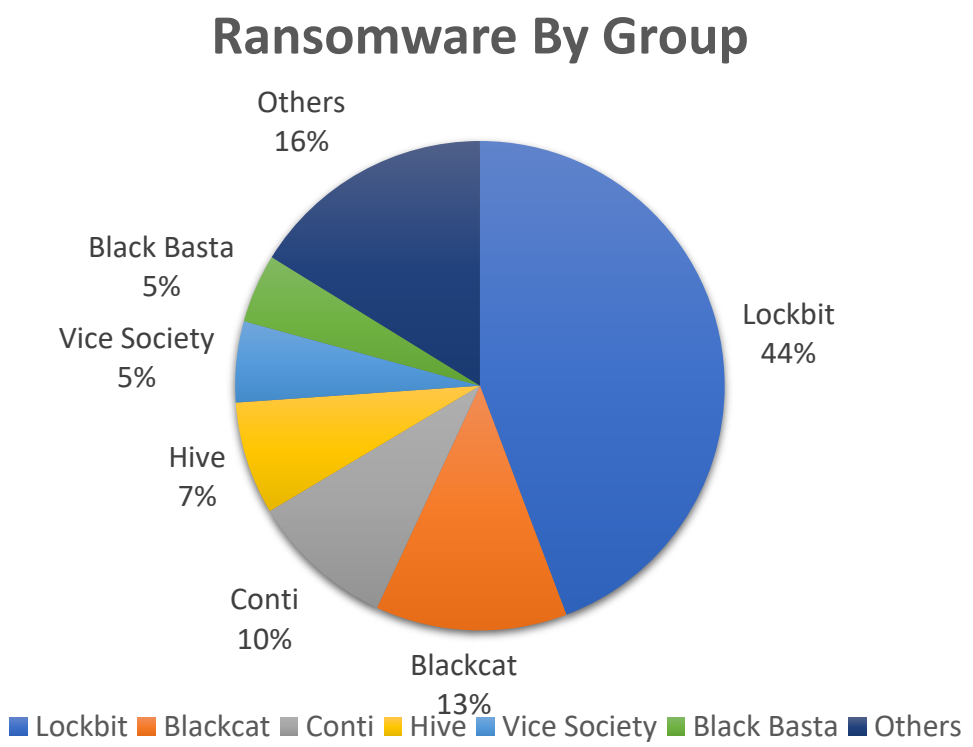
- 60- minute webinar
  - 45-minute presentation
  - 15-minute Q&A
- Live Questions in Chat
- Poll
- Downloadable Resources
- Amazon Gift Card – Stay tuned!
  - Winners will be emailed separately post-event.

WHAT WE WILL COVER:

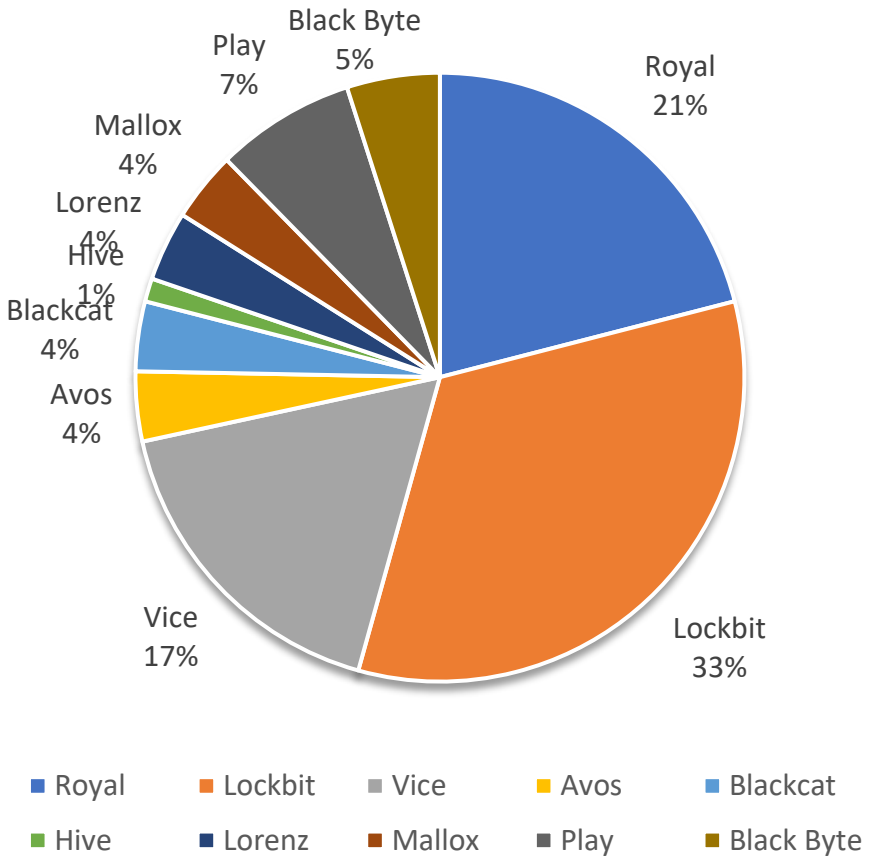
- 2022 Ransomware and Threat Review.
- The traditional answer to Cyber Security.
- Identifying your blind spots.
- 2023 Cyber Security Action Plan.

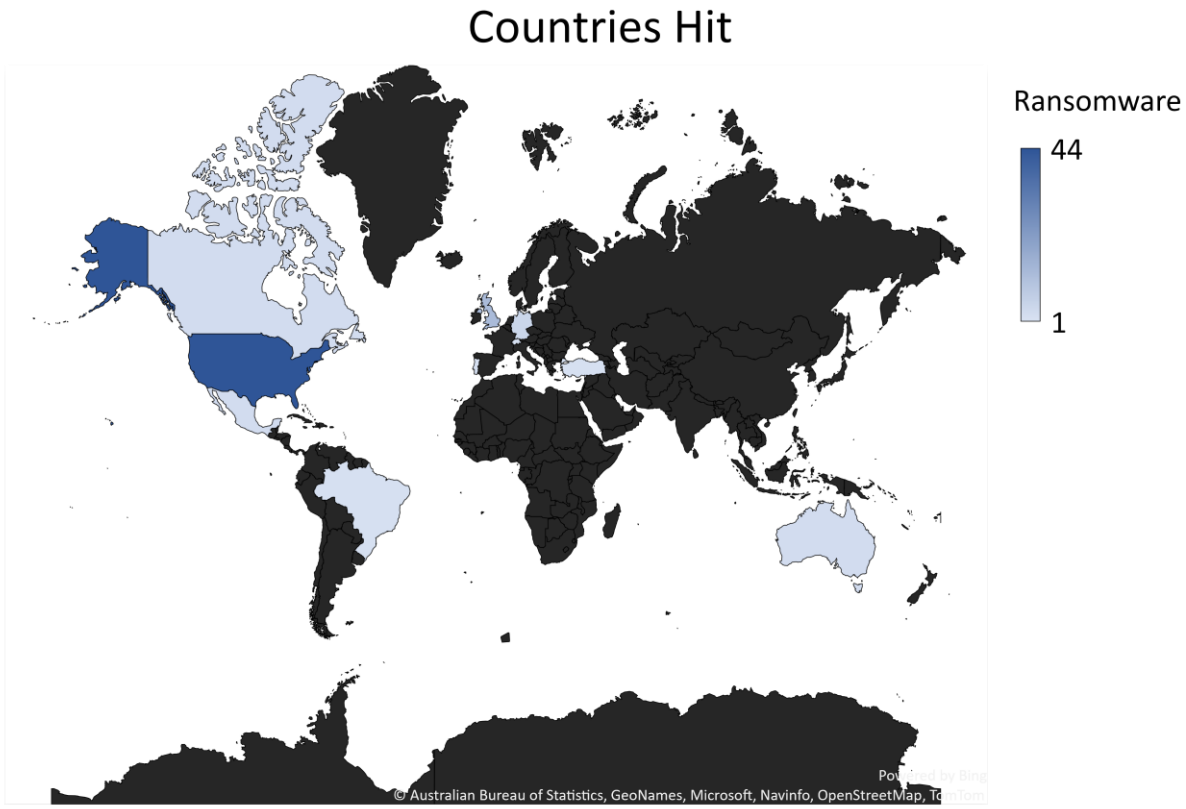
2022 RANSOMWARE AND THREAT REVIEW:



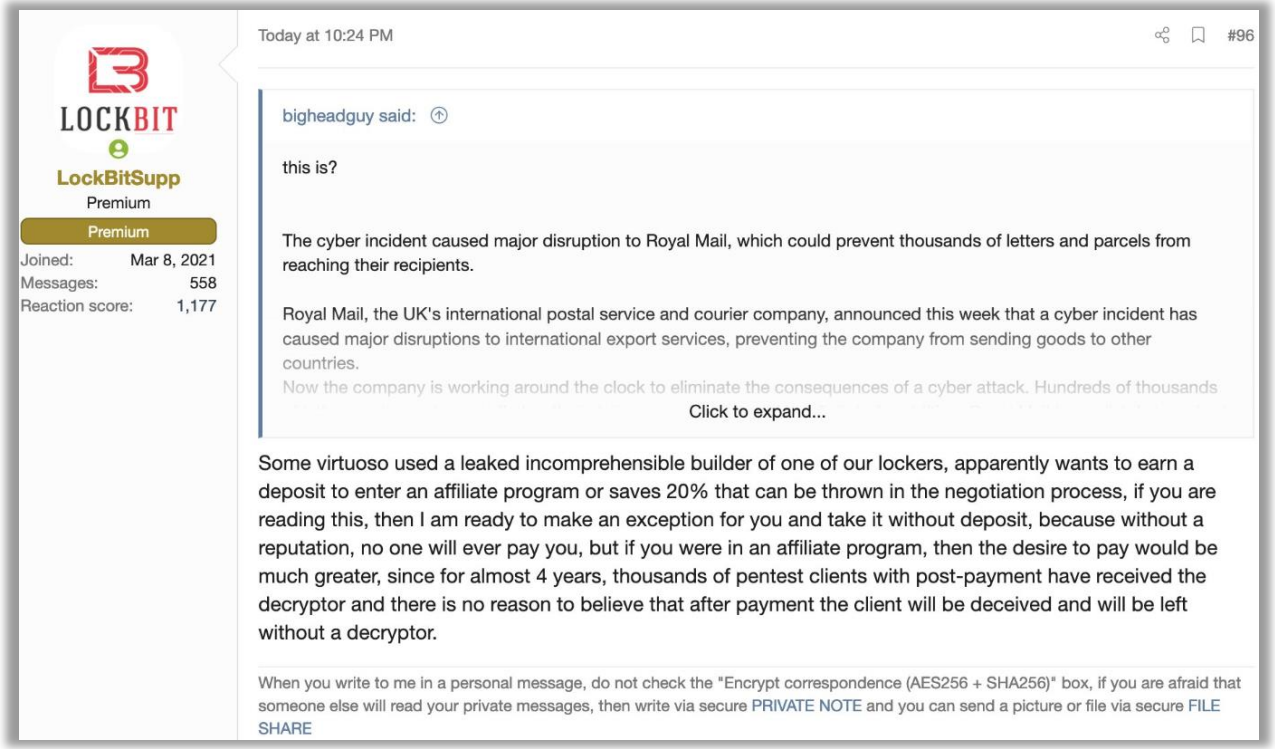


January 2023:

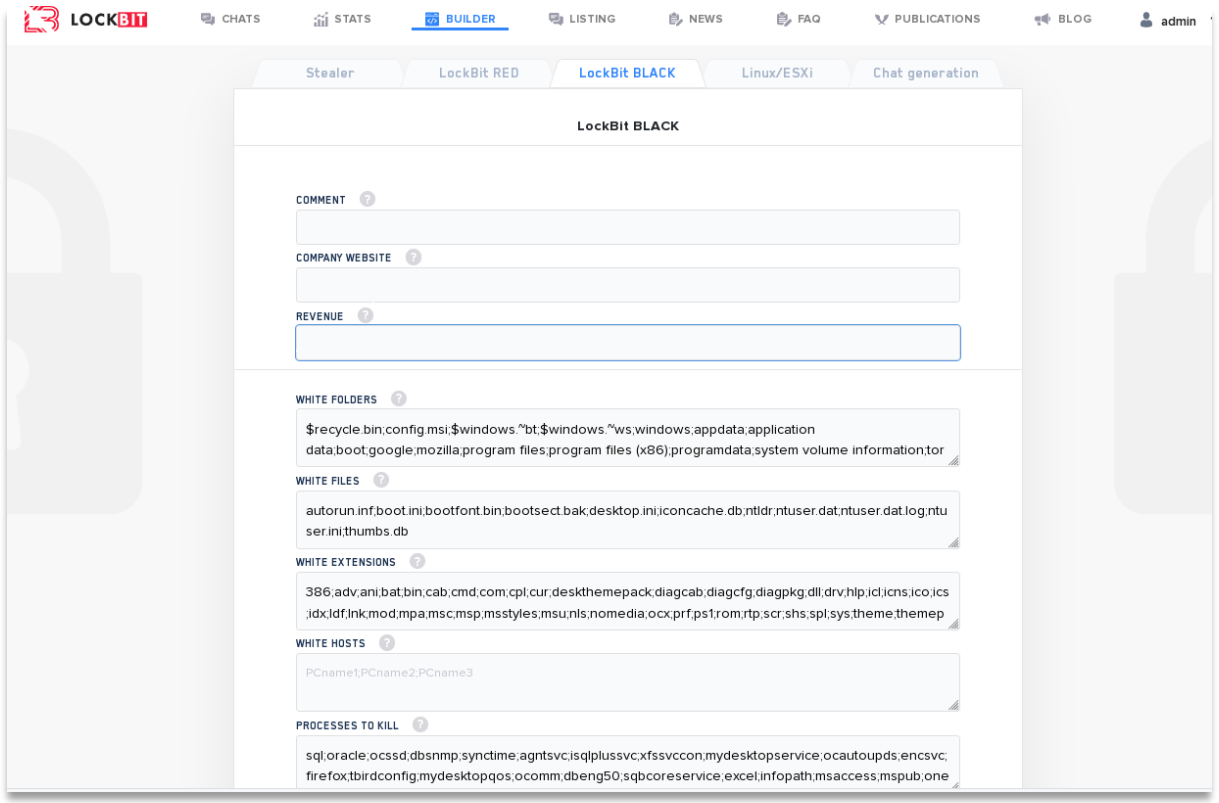


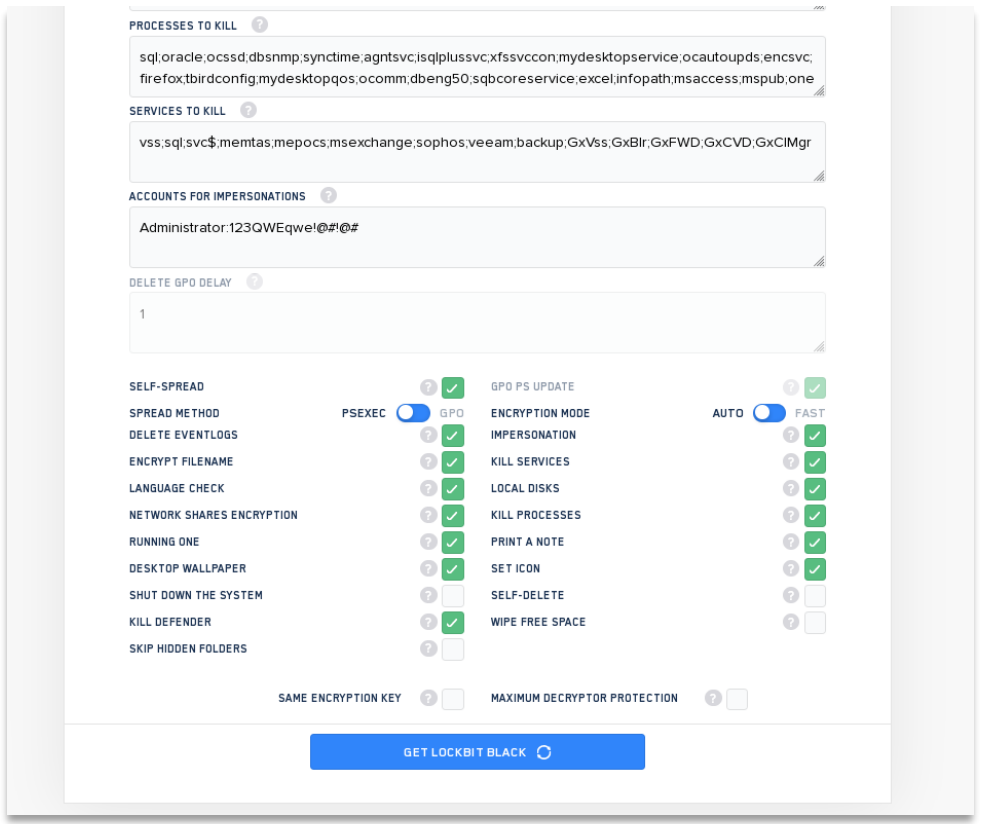


Ransomware is a business run by businessmen:



Ransomware UI:

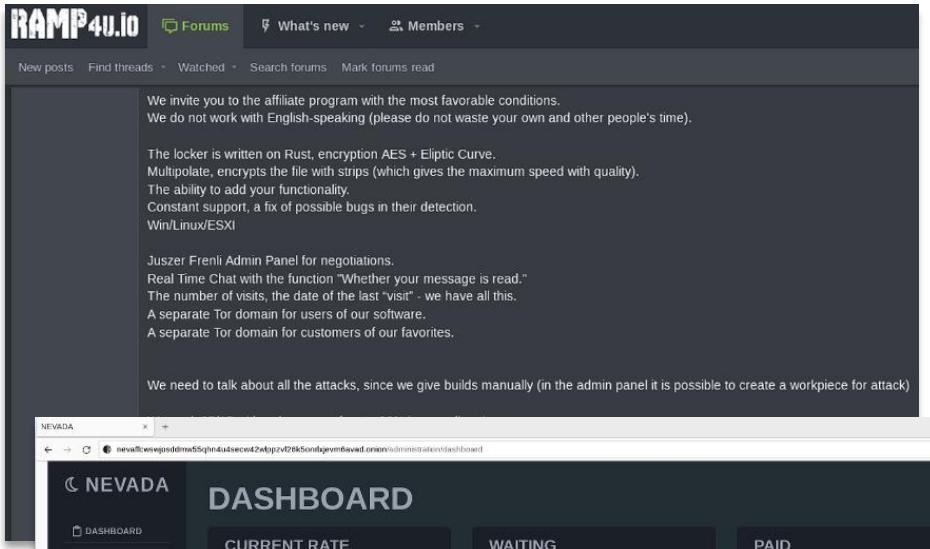


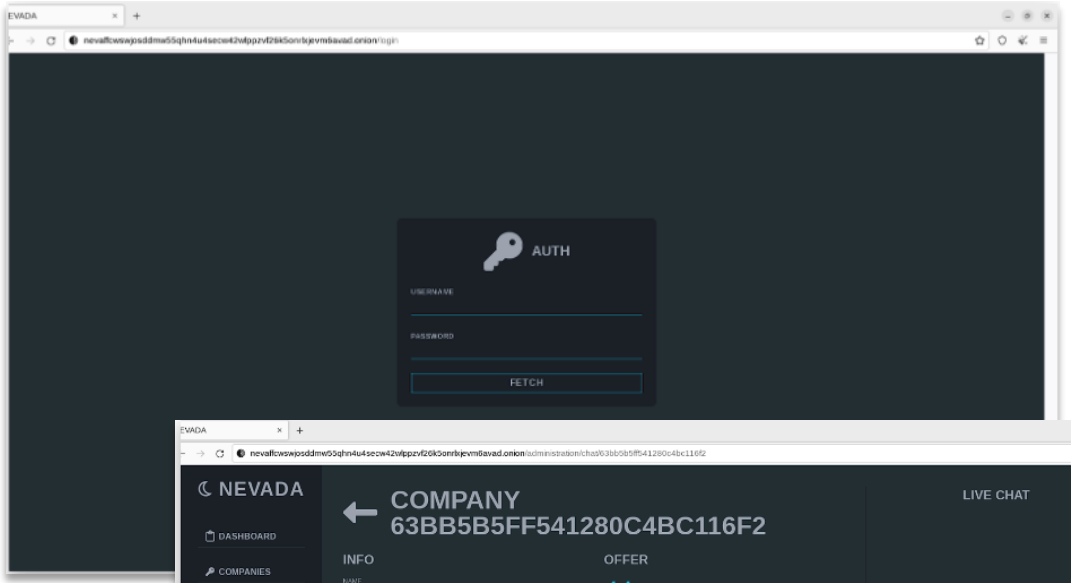


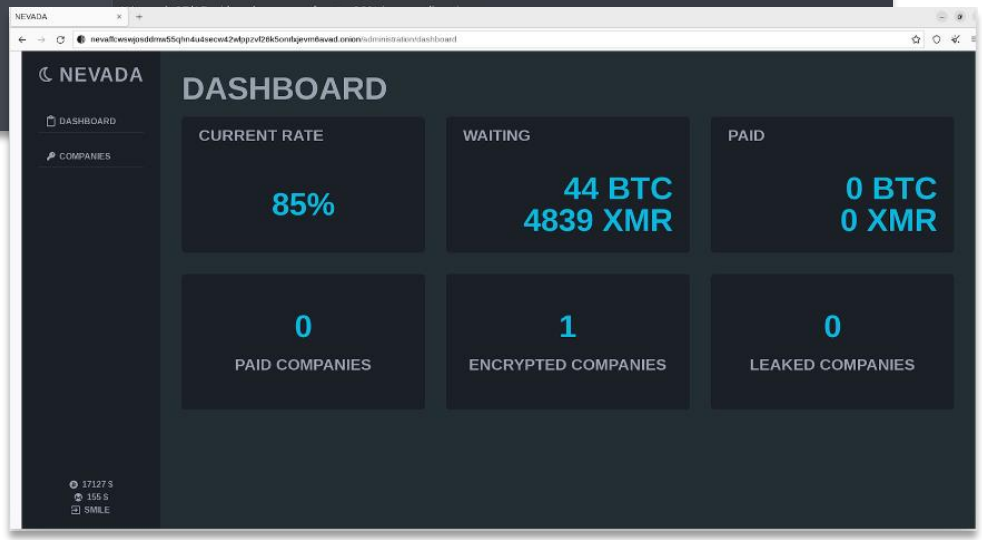
IT CORPORATION

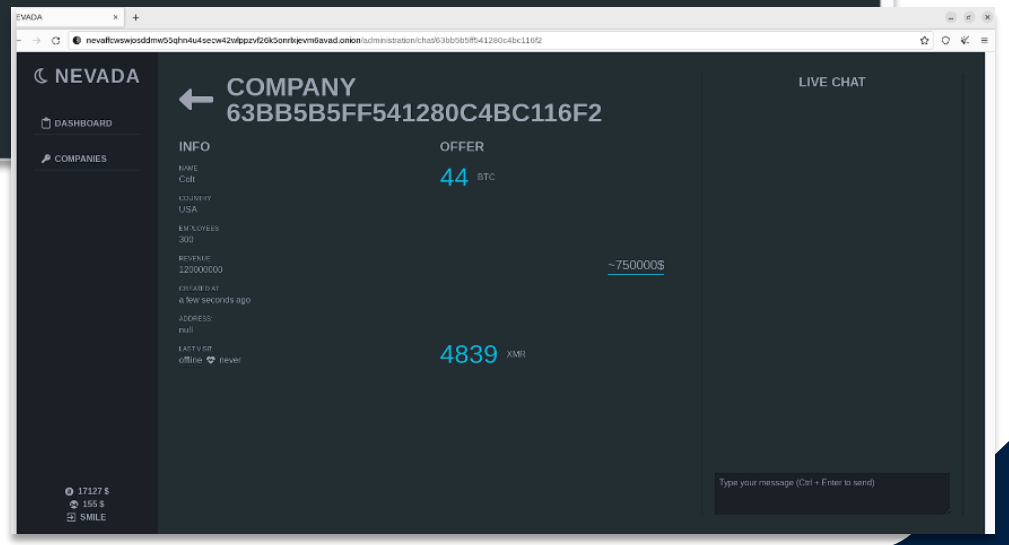
New RaaS - Nevada:

Thanks to Resecurity

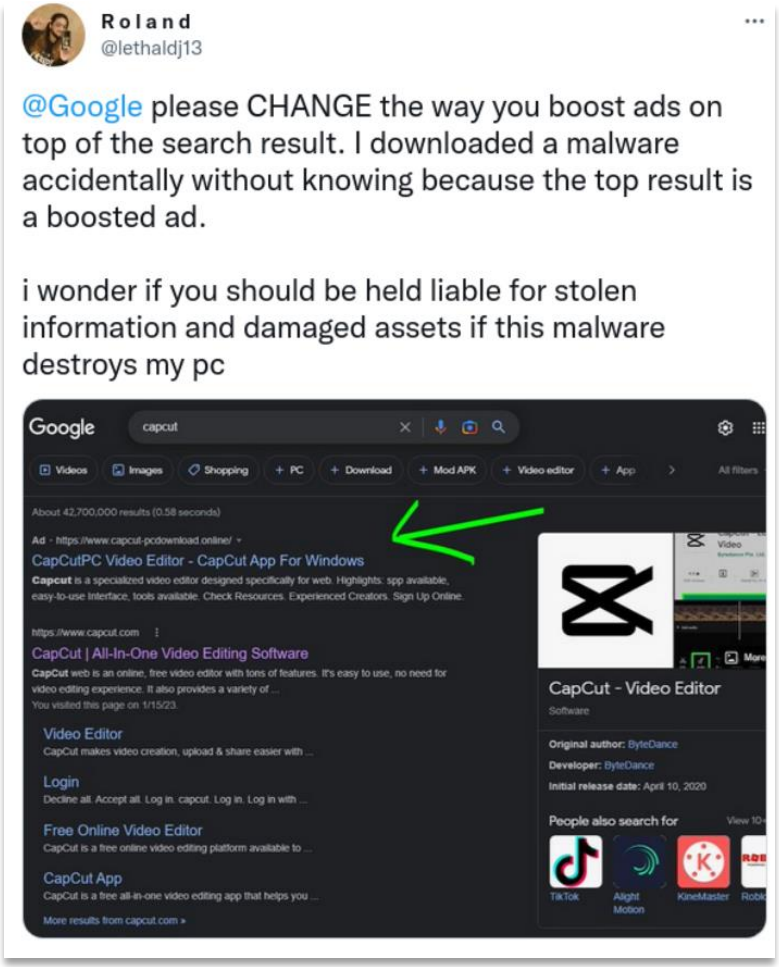


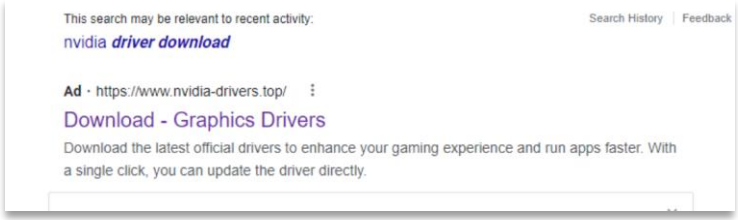


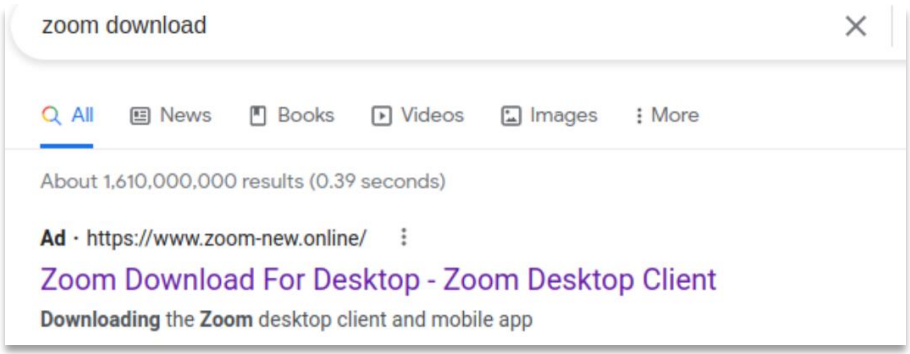


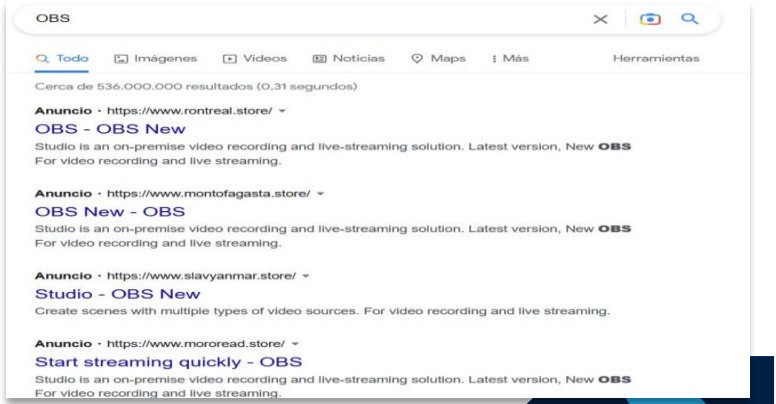


Are you safe at home?
Google ads:





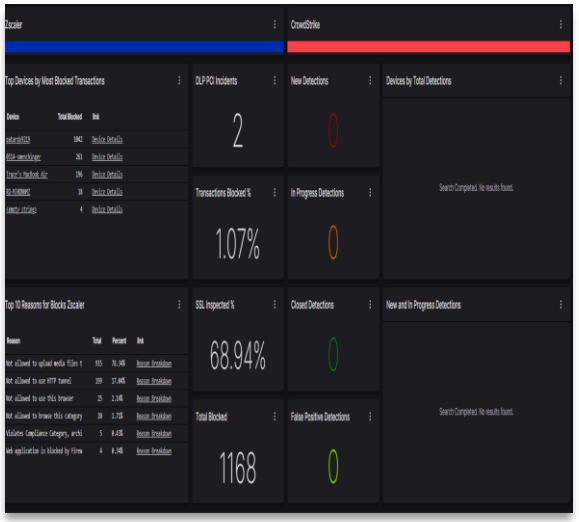




IT CORPORATION

The traditional approach

THE TRADITIONAL ANSWER TO CYBER SECURITY:



January 2023 - Patches

39 Elevation of Privilege Vulnerabilities | 4 Security Feature Bypass Vulnerabilities | 33 Remote Code Execution Vulnerabilities | 10 Information Disclosure Vulnerabilities | 10 Denial of Service Vulnerabilities | 2 Spoofing Vulnerabilities

IT CORPORATION

THE TRADITIONAL ANSWER TO CYBER SECURITY:

John
The lone cyber wolf

For example, the typical IT staffing ratio (the number of employees supported by each IT worker) is 1:27 among all companies included in the survey.

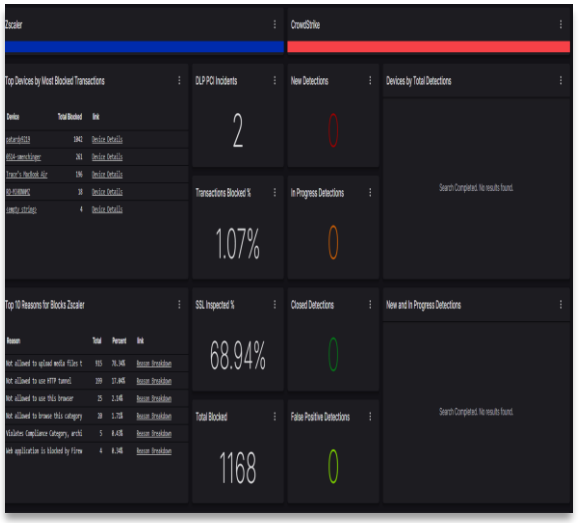
- Workforce.com

From a sample of 250 companies in different industries, a general rule is your security staff should be between 5-10% of your IT staff.

- Nuharborsecurity

IT CORPORATION

THE TRADITIONAL ANSWER TO CYBER SECURITY:

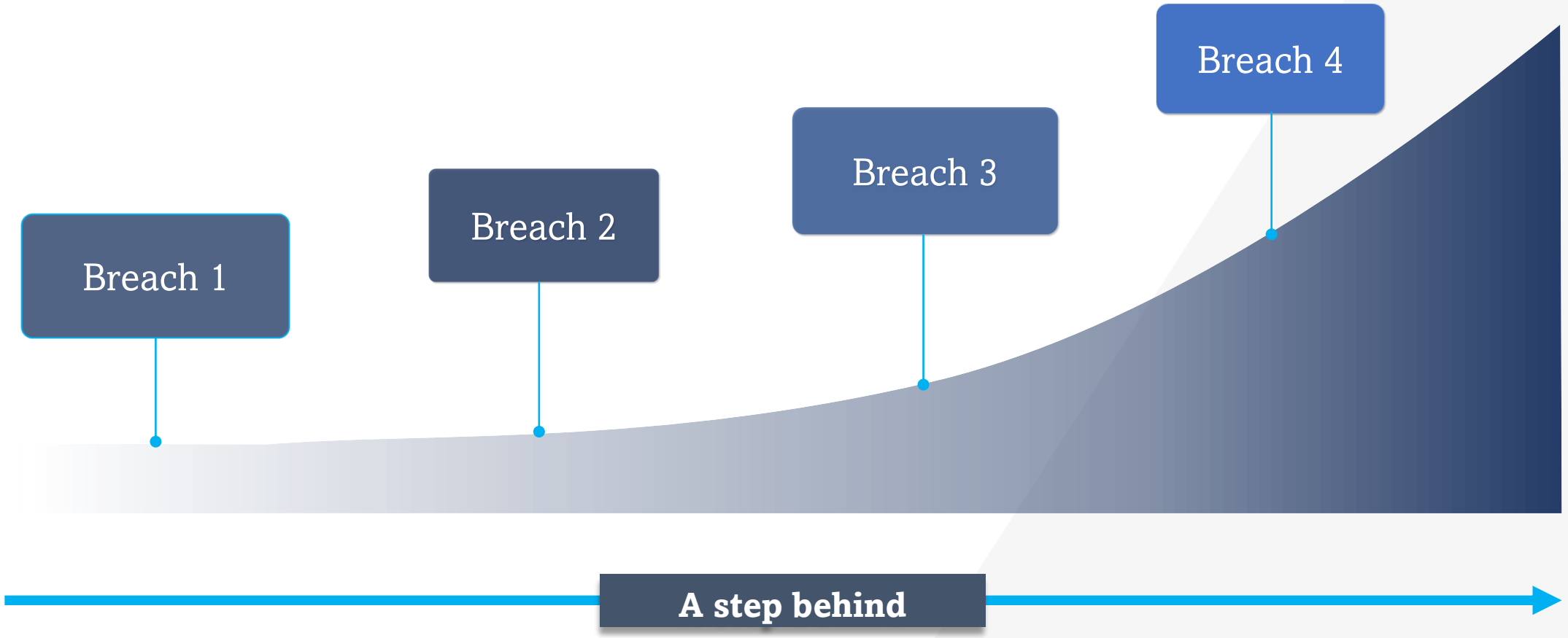


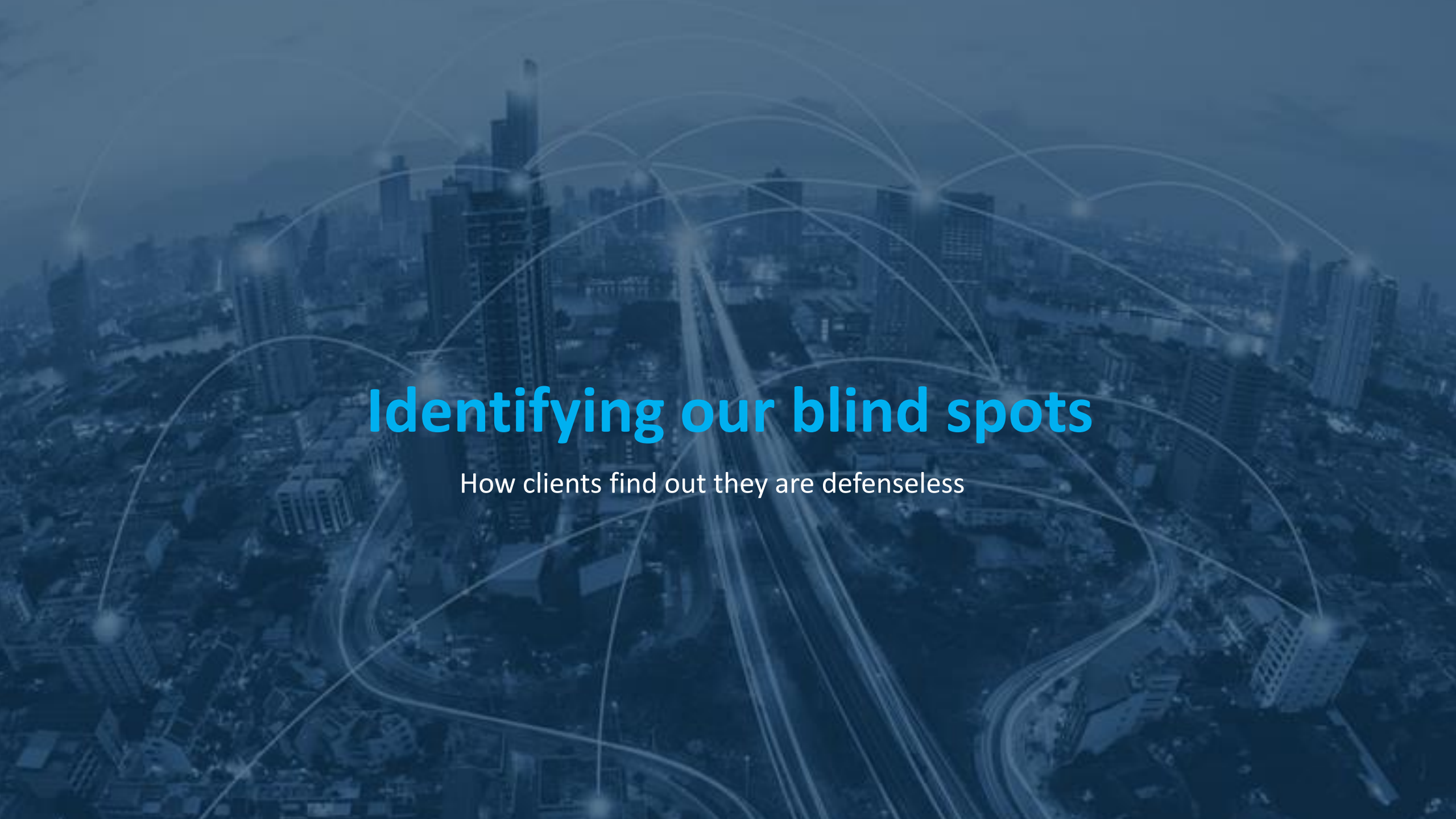
January 2023 - Patches

39 Elevation of Privilege Vulnerabilities | 4 Security Feature Bypass Vulnerabilities | 33 Remote Code Execution Vulnerabilities | 10 Information Disclosure Vulnerabilities | 10 Denial of Service Vulnerabilities | 2 Spoofing Vulnerabilities

IT CORPORATION

The Results





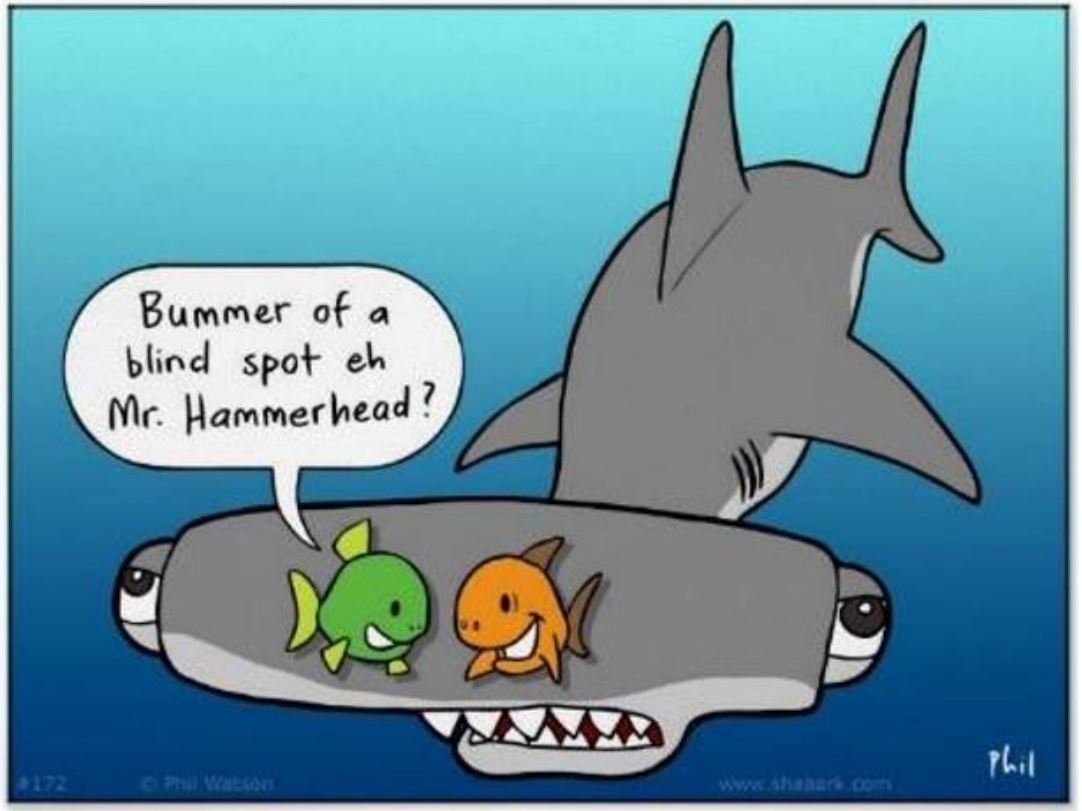
Identifying our blind spots

How clients find out they are defenseless

IDENTIFYING YOUR BLIND SPOTS:

I know that I know

- The security tools are in place
- I have cyber security staff
- I have an MSSP
- I completed a checklist (NIST, audit, etc)
- My cyber security budget



IDENTIFYING YOUR BLIND SPOTS:

I know that I don’t know

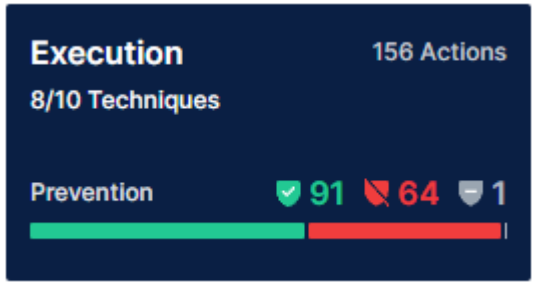
- Can I defend from black cat’s latest variant?
- Do I have the best-in-class tools?
- What are my users home threats when they take the laptop there or work remotely.
- Is my MSSP competent?
- What emerging threats am I not aware of?
- What are all of the ways my sensitive data can be accessed?

IDENTIFYING YOUR BLIND SPOTS:

I don’t know that I don’t know

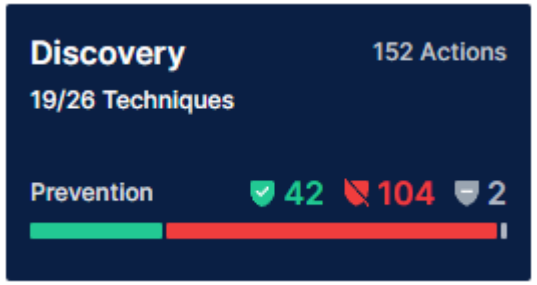
- SSL inspection was turned off on my edge device and 100% of threats made it through.
- My EDR policy was weak and allowed significant attacks to occur in my environment.
- I have an active threat in my environment exfiltrating data.
- I have no logging or alerting for key attacks.

The Weakness:



Weakest:

- WMI
- Scheduled Tasks



Weakest:

- Sysinfo
- Permission Discovery (Net utility)
- File Discovery

Weakest:

- Scheduled tasks
- Boot or logon autostart

2023 Cyber Security action plan

Identify where you are?

Stage 1 - Hygiene	Stage 2 - Limiting breaches	Stage 3 - Proactive
• EDR • Edge / Firewalls • Identity Management with MFA for Apps • Disaster recovery • Incident response plan • Vulnerability and Patch Management • Email flagging, filtering, and encryption.	• Privilege access management • Application segmentation • SIEM / SOAR • XDR Capabilities • MSSP / SOC • MFA at Desktop and Server Login • Configuration Management	• Continuous validation • Cyber engineer training • Table top exercises

IT CORPORATION

RIDGE
IT CORPORATION

Take Away

What does it mean to become Cyber Ready?

- Don't hide behind logos
- Continuously validate your security tools
- Look for continuous improvement-your adversaries are an organized business, not (just) teenagers in a basement

Remember

- Posture Matters.. Know what you don't know
- Staying ahead of attackers is a constant battle
- Cost of breaches are increasing faster than budget
- Best of breed tools 5 years ago, are no longer the best of today. Continuously evaluate your tools and their implementations

POSTURE MATTERS


QUESTIONS?


THANK YOU FOR ATTENDING!