

RIDGE·IT

GET CYBER READY



@RidgeITCorporation



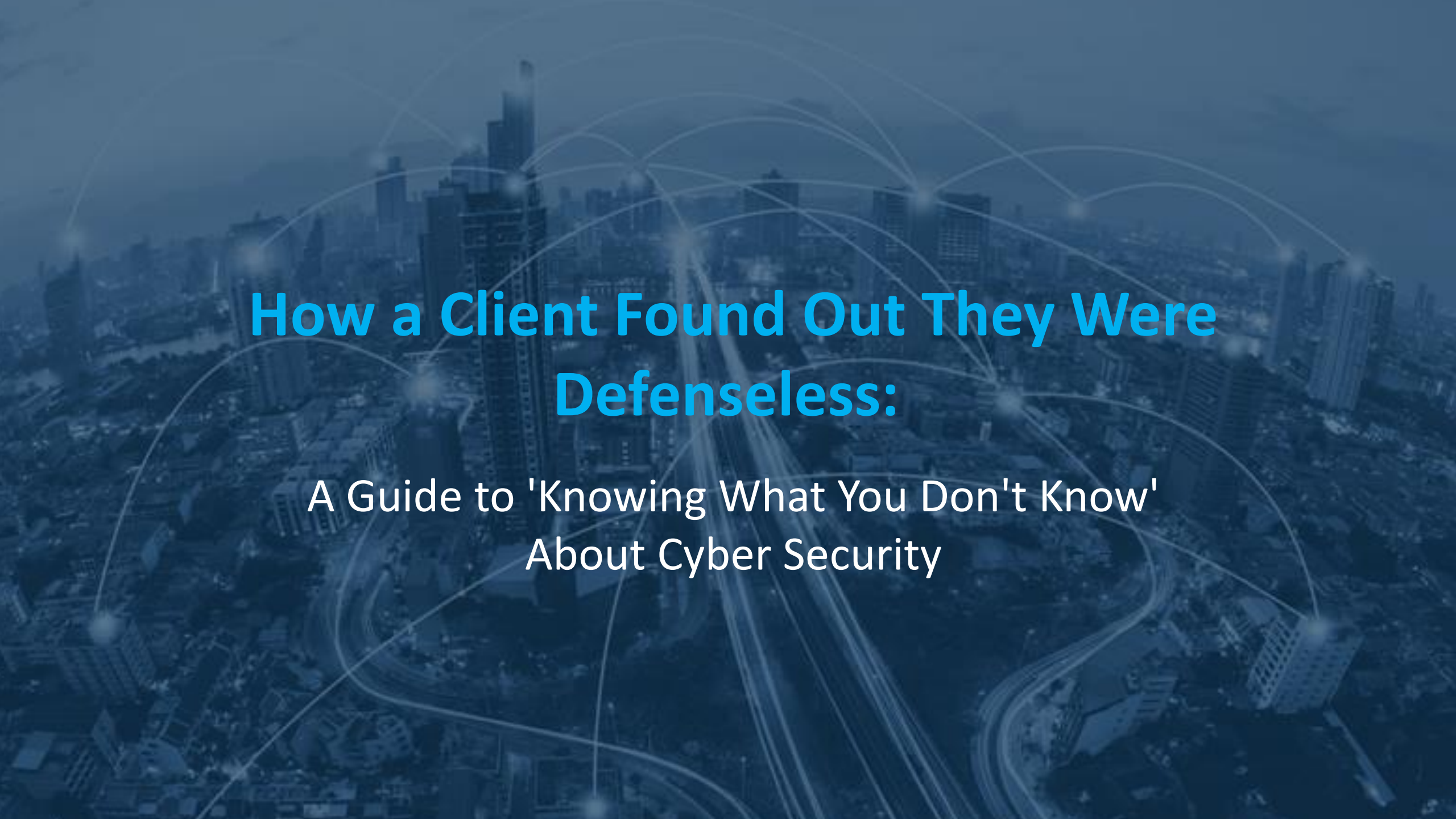
www.RidgeIT.com



Sales@RidgeIT.com



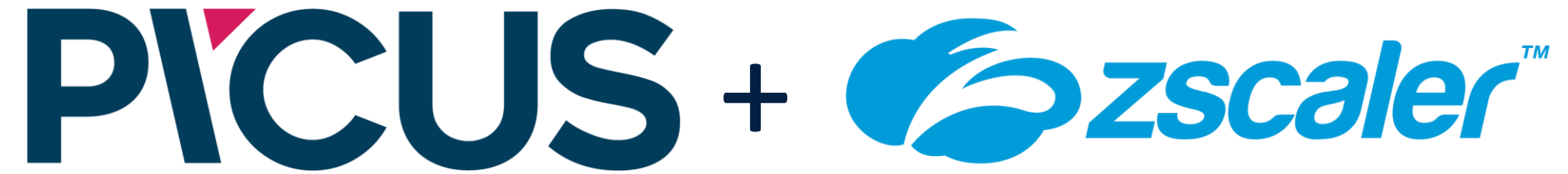
844-743-4348

An aerial view of a city skyline, likely New York City, with a network of glowing white lines and nodes overlaid on the image, suggesting a digital or cyber theme. The lines connect various points across the city, creating a complex web.

How a Client Found Out They Were Defenseless:

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

IN PARTNERSHIP WITH:



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:

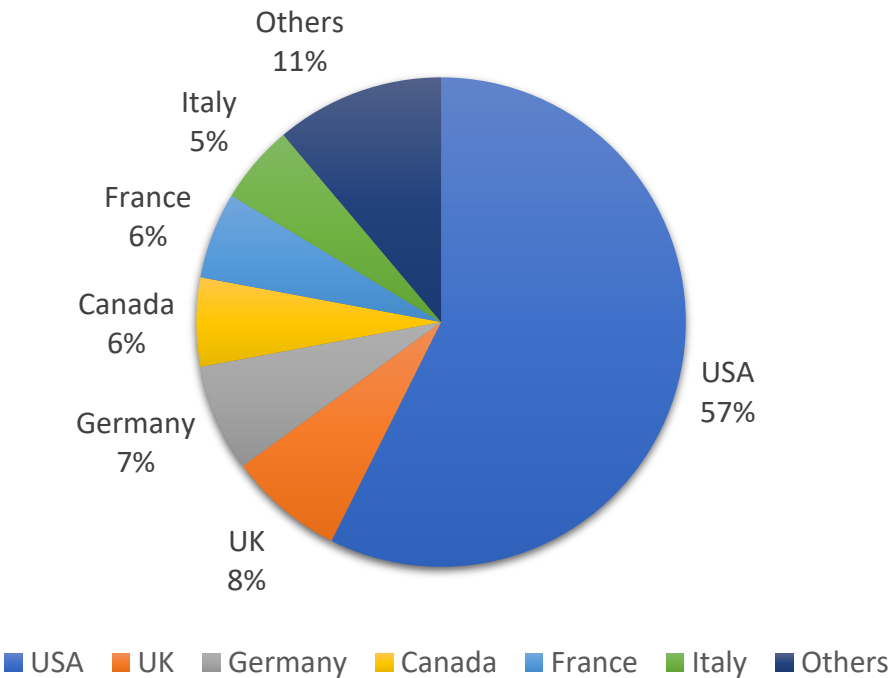
- ✓ 60- minute webinar
 - 45-minute presentation
 - 15-minute Q&A
- ✓ Live Questions in Chat
- ✓ Poll
- ✓ Downloadable Resources
- ✓ Amazon Gift Card – Stay tuned!
 - Winners will be emailed separately post-event.

WHAT WE WILL COVER:

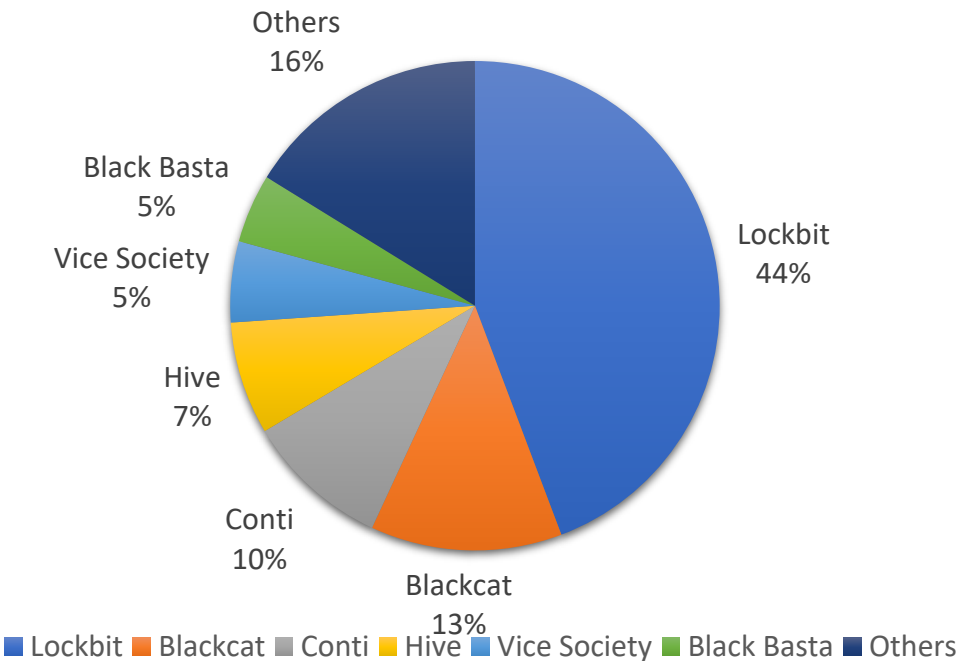
- ✓ 2022 Ransomware and Threat Review.
- ✓ The traditional answer to Cyber Security.
- ✓ Identifying your blind spots.
- ✓ 2023 Cyber Security Action Plan.

2022 RANSOMWARE AND THREAT REVIEW:

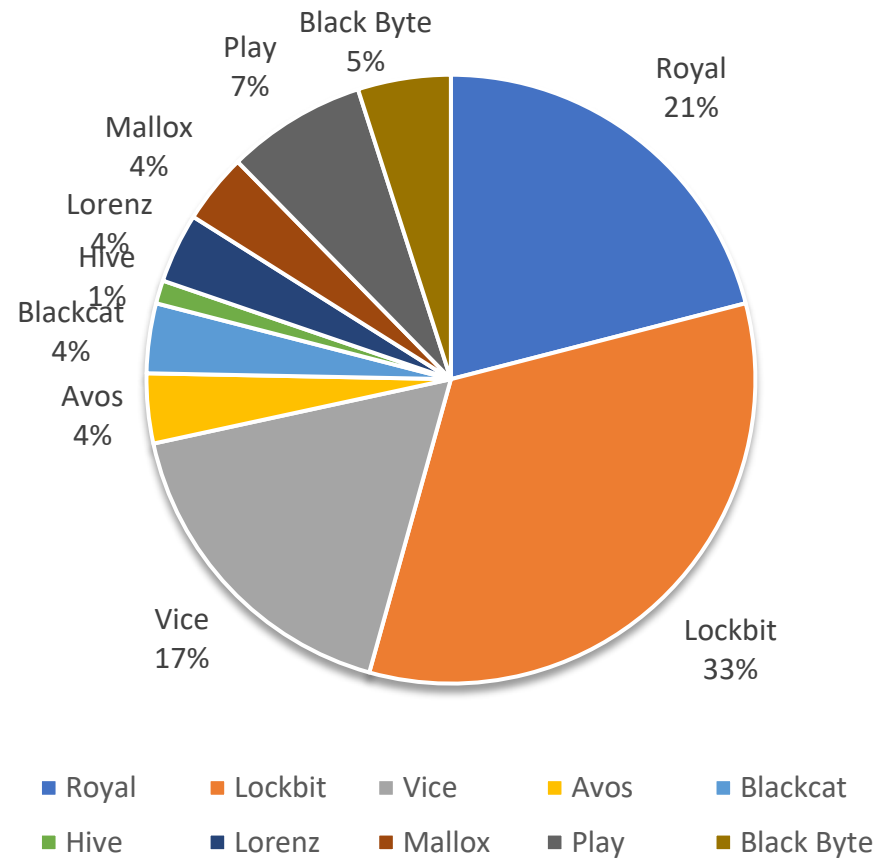
Ransomware By Country



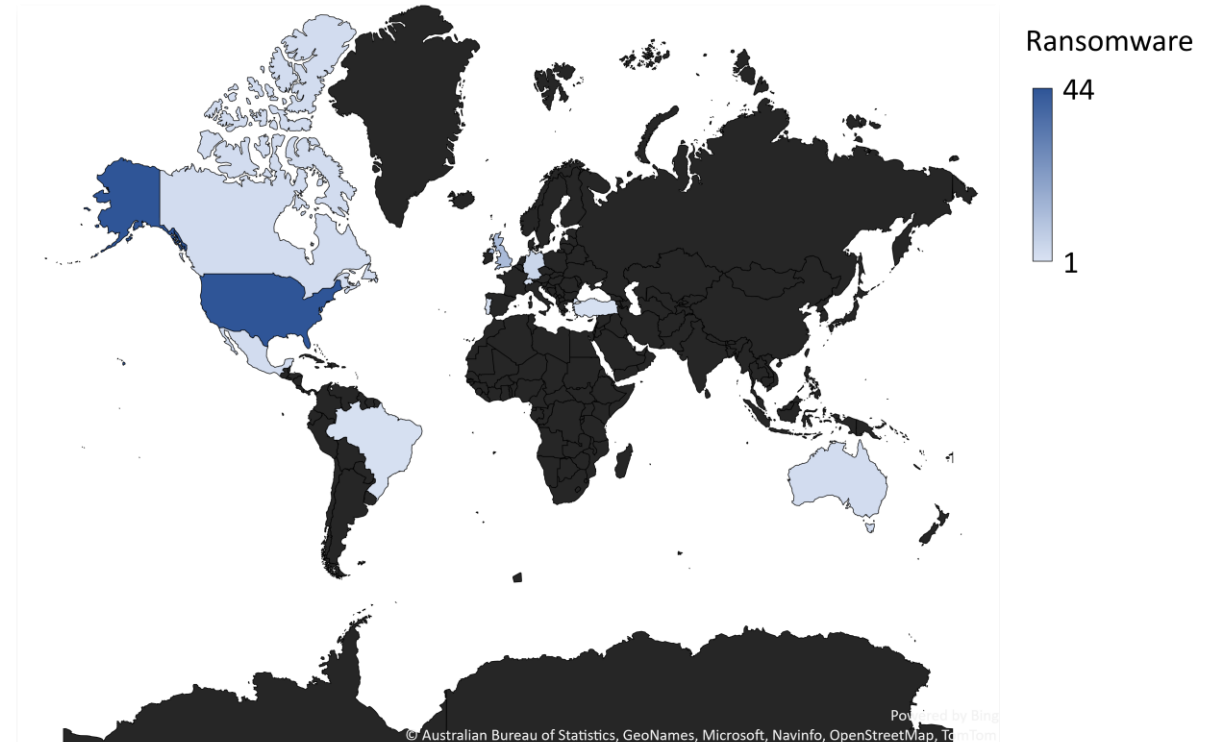
Ransomware By Group



January 2023:



Countries Hit



Ransomware is a business run by businessmen:

**LOCKBIT**
**LockBitSupp**
Premium
Premium

Joined: Mar 8, 2021
Messages: 558
Reaction score: 1,177

Today at 10:24 PM

#96

bigheadguy said: 

this is?

The cyber incident caused major disruption to Royal Mail, which could prevent thousands of letters and parcels from reaching their recipients.

Royal Mail, the UK's international postal service and courier company, announced this week that a cyber incident has caused major disruptions to international export services, preventing the company from sending goods to other countries.

Now the company is working around the clock to eliminate the consequences of a cyber attack. Hundreds of thousands

Click to expand...

Some virtuoso used a leaked incomprehensible builder of one of our lockers, apparently wants to earn a deposit to enter an affiliate program or saves 20% that can be thrown in the negotiation process, if you are reading this, then I am ready to make an exception for you and take it without deposit, because without a reputation, no one will ever pay you, but if you were in an affiliate program, then the desire to pay would be much greater, since for almost 4 years, thousands of pentest clients with post-payment have received the decryptor and there is no reason to believe that after payment the client will be deceived and will be left without a decryptor.

When you write to me in a personal message, do not check the "Encrypt correspondence (AES256 + SHA256)" box, if you are afraid that someone else will read your private messages, then write via secure PRIVATE NOTE and you can send a picture or file via secure FILE

SHARE

NEW YEAR SALE

On this beautiful occasion of the New Year, We wish all of you a very happy New Year. We wish that this year brings a lot of happy moments and joyful events to your life. We also hope that a new start of the year will have a positive on our life. We want to announce, list of companies that their data will be given for free, yes, yes. for free.

CPTM
Hayward
KansasCityHomes

PITMAN FAMILY PA Hurry And download. Happy New Year :) ANDE STEVENS

Ransomware UI:

 LOCKBIT

CHATSSTATSBUILDERLISTINGNEWSFAQPUBLICATIONSBLOGadmin

StealerLockBit REDLockBit BLACKLinux/ESXiChat generation

LockBit BLACK

COMMENT?

COMPANY WEBSITE?

REVENUE?

WHITE FOLDERS?

\$recycle.bin;config.msi;\$windows.*bt;\$windows.*ws;windows.appdata,application data;boot;google.mozilla;program files;program files (x86);programdata;system volume information;tor

WHITE FILES?

autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db

WHITE EXTENSIONS?

386;.adv;.ani;.bat;.bin;.cab;.cmd;.com;.cpl;.cur;.deskthemepack;.diagcab;.diagcfg;.diagpkg;.dll;.drv;.hlp;.icl;.icns;.ico;.ics;.idx;.ldf;.lnk;.mod;.mpa;.msc;.msp;.msstyles;.msu;.nls;.nomedia;.ocx;.prf;.pst;.rom;.rtp;.scr;.shs;.spl;.sys;.theme;.themep

WHITE HOSTS?

PCName1;PCName2;PCName3

PROCESSES TO KILL?

sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;birdconfig;mydesktopqos;ocomm;dbeng50;sqbcoreservice;excel;infopath;msaccess;msspub;one

PROCESSES TO KILL?

sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;birdconfig;mydesktopqos;ocomm;dbeng50;sqbcoreservice;excel;infopath;msaccess;msspub;one

SERVICES TO KILL?

vss;sql;svc;\$memtas;mepocs;msexchange;sophos;veeam;backup;GxVss;GxBir;GxFWD;GxCVD;GxCIMgr

ACCOUNTS FOR IMPERSONATIONS?

Administrator:123QWEqwe!@#@@#

DELETE GPO DELAY?

1

SELF-SPREAD

SPREAD METHOD

DELETE EVENTLOGS

ENCRYPT FILENAME

LANGUAGE CHECK

NETWORK SHARES ENCRYPTION

RUNNING ONE

DESKTOP WALLPAPER

SHUT DOWN THE SYSTEM

KILL DEFENDER

SKIP HIDDEN FOLDERS

PSEXEC

GPO

GPO PS UPDATE

ENCRYPTION MODE

IMPERSONATION

KILL SERVICES

LOCAL DISKS

KILL PROCESSES

PRINT A NOTE

SET ICON

SELF-DELETE

WIPE FREE SPACE

AUTO

FAST

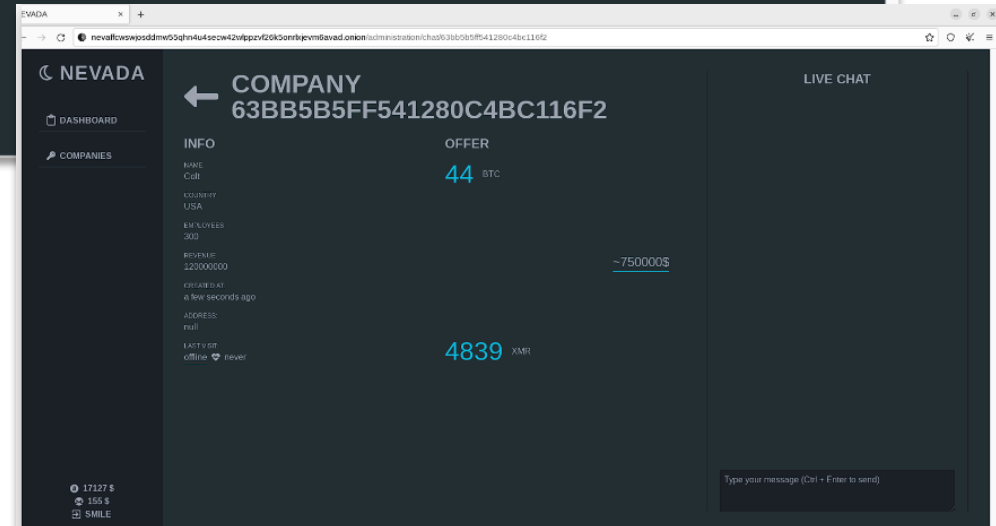
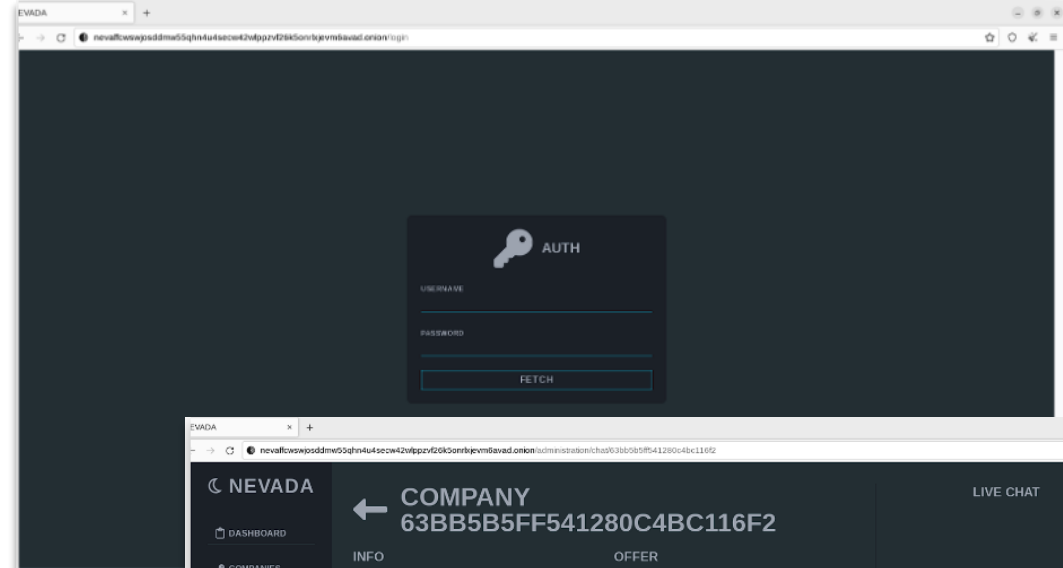
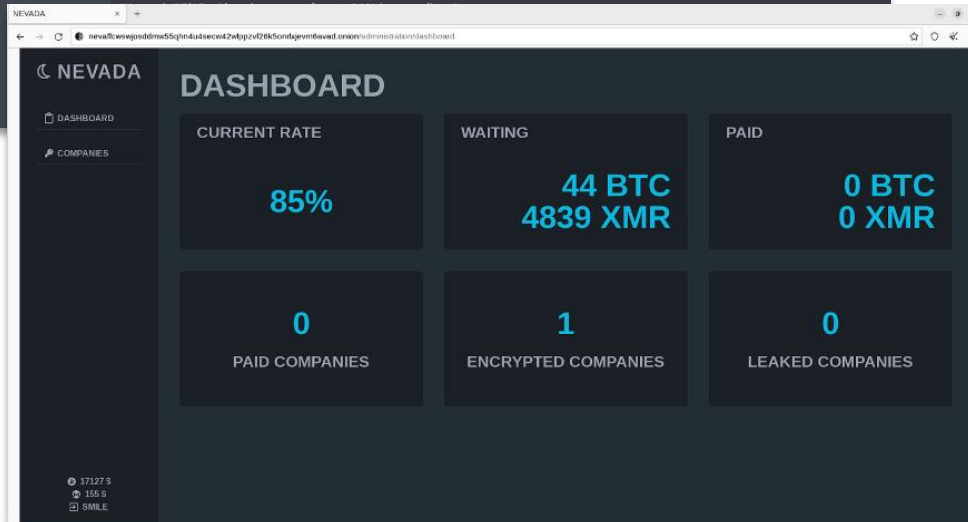
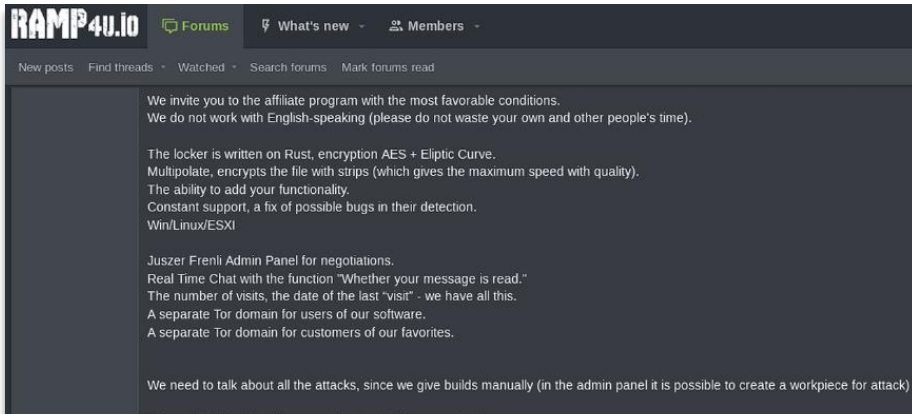
SAME ENCRYPTION KEY?

MAXIMUM DECRYPTOR PROTECTION?

GET LOCKBIT BLACK

New RaaS - Nevada:

Thanks to Resecurity



Are you safe at home?

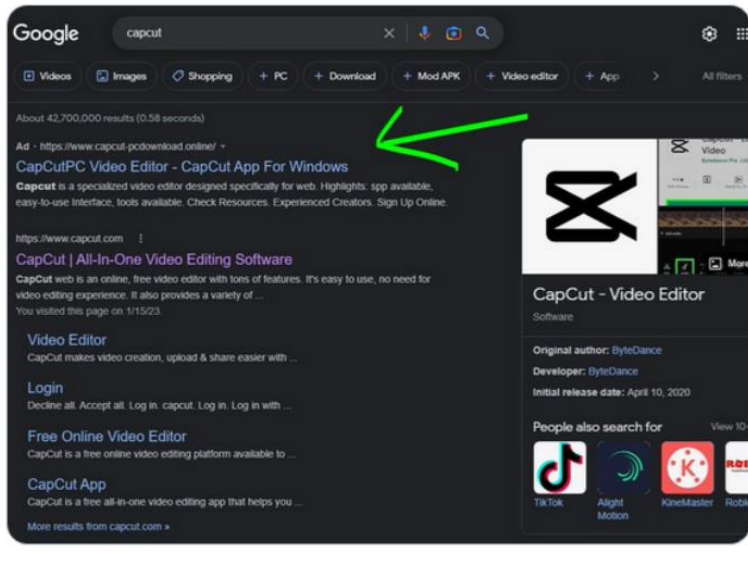
Google ads:



Roland
@lethaldj13

@Google please CHANGE the way you boost ads on top of the search result. I downloaded a malware accidentally without knowing because the top result is a boosted ad.

i wonder if you should be held liable for stolen information and damaged assets if this malware destroys my pc



This search may be relevant to recent activity: [nvidia driver download](#)

Ad · <https://www.nvidia-drivers.top/>

Download - Graphics Drivers

Download the latest official drivers to enhance your gaming experience and run apps faster. With a single click, you can update the driver directly.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

December 21, 2022

Alert Number
I-122122-PSA

Questions regarding this PSA should be directed to your local
FBI Field Office.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users

The FBI is warning the public that cyber criminals are using search engine advertisement services to impersonate brands and direct users to malicious sites that host ransomware and steal login credentials and other financial information.

METHODOLOGY

Cyber criminals purchase advertisements that appear within internet search results using a domain that is similar to an actual business or service. When a user searches for that business or service, these advertisements appear at the very top of search results with minimum distinction between an advertisement and an actual search result.

zoom download

[All](#) [News](#) [Books](#) [Videos](#) [Images](#) [More](#)

About 1,610,000,000 results (0.39 seconds)

Ad · <https://www.zoom-new.online/>

Zoom Download For Desktop - Zoom Desktop Client

Downloading the Zoom desktop client and mobile app

OBS

[Todo](#) [Imágenes](#) [Videos](#) [Noticias](#) [Maps](#) [Más](#) [Herramientas](#)

Cerca de 536.000.000 resultados (0,31 segundos)

Anuncio · <https://www.rontreal.store/>

OBS - OBS New

Studio is an on-premise video recording and live-streaming solution. Latest version, New **OBS** For video recording and live streaming.

Anuncio · <https://www.montofagasta.store/>

OBS New - OBS

Studio is an on-premise video recording and live-streaming solution. Latest version, New **OBS** For video recording and live streaming.

Anuncio · <https://www.slavyanmar.store/>

Studio - OBS New

Create scenes with multiple types of video sources. For video recording and live streaming.

Anuncio · <https://www.mororead.store/>

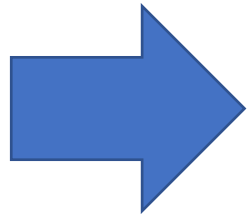
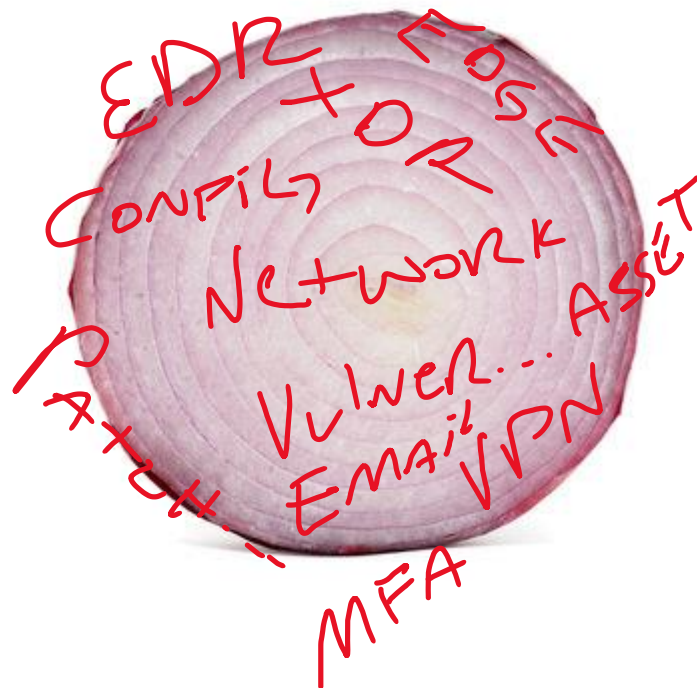
Start streaming quickly - OBS

Studio is an on-premise video recording and live-streaming solution. Latest version, New **OBS** For video recording and live streaming.

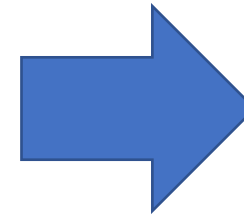
An aerial view of a city at night, with a blue tint. Overlaid on the city are numerous glowing white lines that form a complex network, connecting various points across the urban landscape. The lines are curved and intersect, creating a sense of connectivity and data flow. The city's skyline, including several tall skyscrapers, is visible in the background.

The traditional approach

THE TRADITIONAL ANSWER TO CYBER SECURITY:



Zscaler				CrowdStrike	
Top Devices by Most Blocked Transactions				OLP/PO Incidents	New Detections
Device	Total Blocked	Hit		2	0
Device 1	1000	Device Details			
Device 2	500	Device Details			
Device 3	100	Device Details			
Device 4	50	Device Details			
Device 5	10	Device Details			
Device 6	5	Device Details			
				Transactions Blocked %	In Progress Detections
				1.07%	0
Top 10 Reasons for Blocks Zscaler				SSL Inspected %	Crowd Detections
Reason	Total	Percent	Hit	68.94%	0
Not allowed to upload with file t	100	78.46%	Reason Breakdown		
Not allowed to use HTTP method	50	39.23%	Reason Breakdown		
Not allowed to use this browser	25	19.61%	Reason Breakdown		
Not allowed to browse this category	10	7.85%	Reason Breakdown		
Violates Compliance Category, etc	5	3.92%	Reason Breakdown		
Web application is blocked by firm	4	3.14%	Reason Breakdown		
				Total Blocked	False Positive Detections
				1168	0



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

THE TRADITIONAL ANSWER TO CYBER SECURITY:



John
The lone cyber wolf

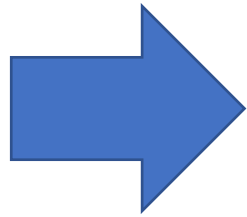
For example, the typical IT staffing ratio (the number of employees supported by each IT worker) is 1:27 among all companies included in the survey.

- Workforce.com

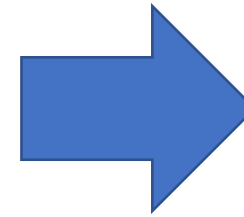
From a sample of 250 companies in different industries, a general rule is your security staff should be between 5-10% of your IT staff.

- Nuharborsecurity

THE TRADITIONAL ANSWER TO CYBER SECURITY:



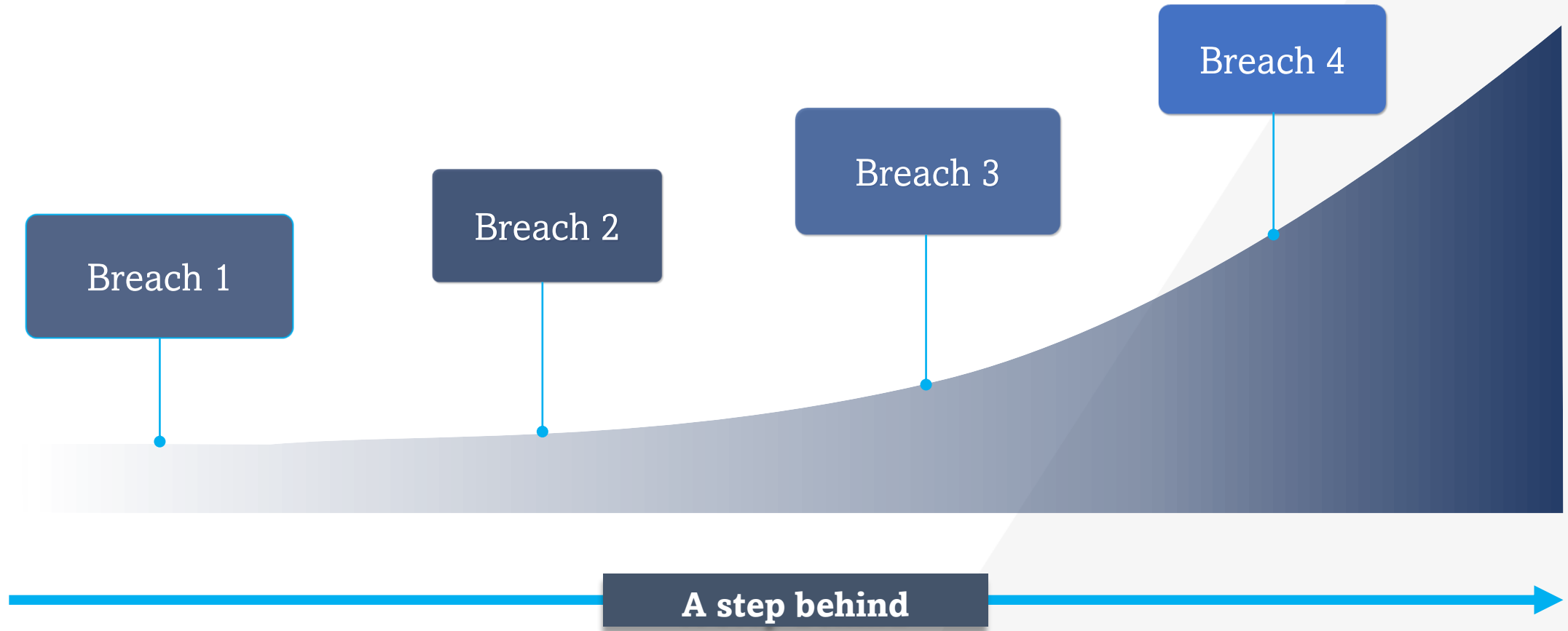
Zscaler				CrowdStrike	
Top Devices by Most Blocked Transactions				DLP PCI Incidents	New Detections
Device	Total Blocked	Hit		2	0
Device 1	1000	Device Details			
Device 2	500	Device Details			
Device 3	100	Device Details			
Device 4	50	Device Details			
Device 5	4	Device Details			
				Transactions Blocked %	In Progress Detections
				1.07%	0
Top 10 Reasons for Blocks Zscaler				SSL Inspected %	Crowd Detections
Reason	Total	Percent	Hit	68.94%	0
Not allowed to upload with file t	100	78.46%	Reason Breakdown		
Not allowed to use HTTP method	100	21.46%	Reason Breakdown		
Not allowed to use this browser	10	2.14%	Reason Breakdown		
Not allowed to browse this category	10	2.14%	Reason Breakdown		
Violates Compliance Category, etc	5	0.43%	Reason Breakdown		
Not application is blocked by firm	4	0.43%	Reason Breakdown		
				Total Blocked	False Positive Detections
				1168	0

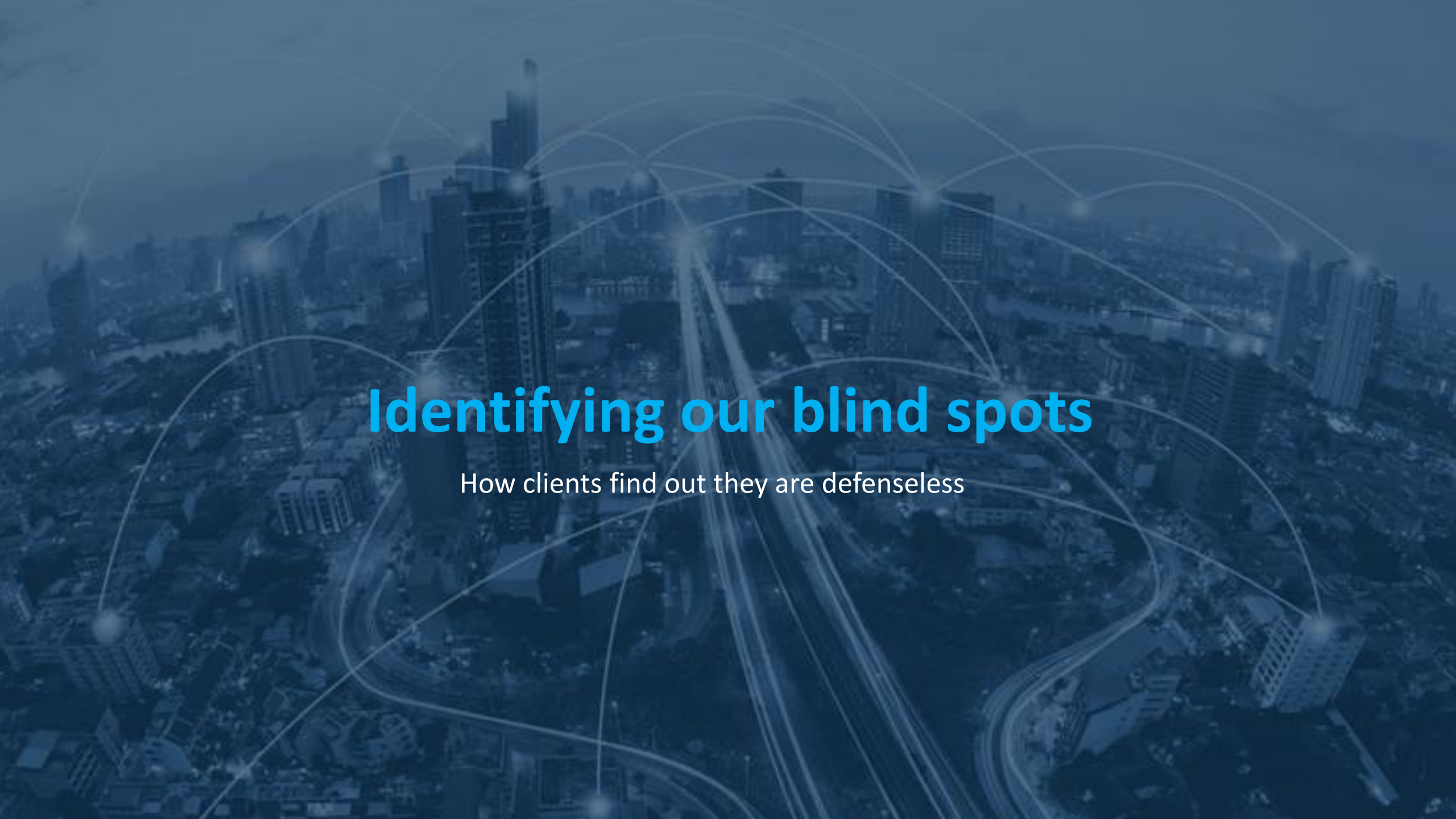


January 2023 - Patches

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

The Results



An aerial view of a city skyline, likely New York City, with a network of glowing white lines and nodes overlaid on the image, suggesting a global or digital network. The lines connect various points across the city, creating a complex web of connections. The overall color scheme is a deep blue, giving it a technological and futuristic feel.

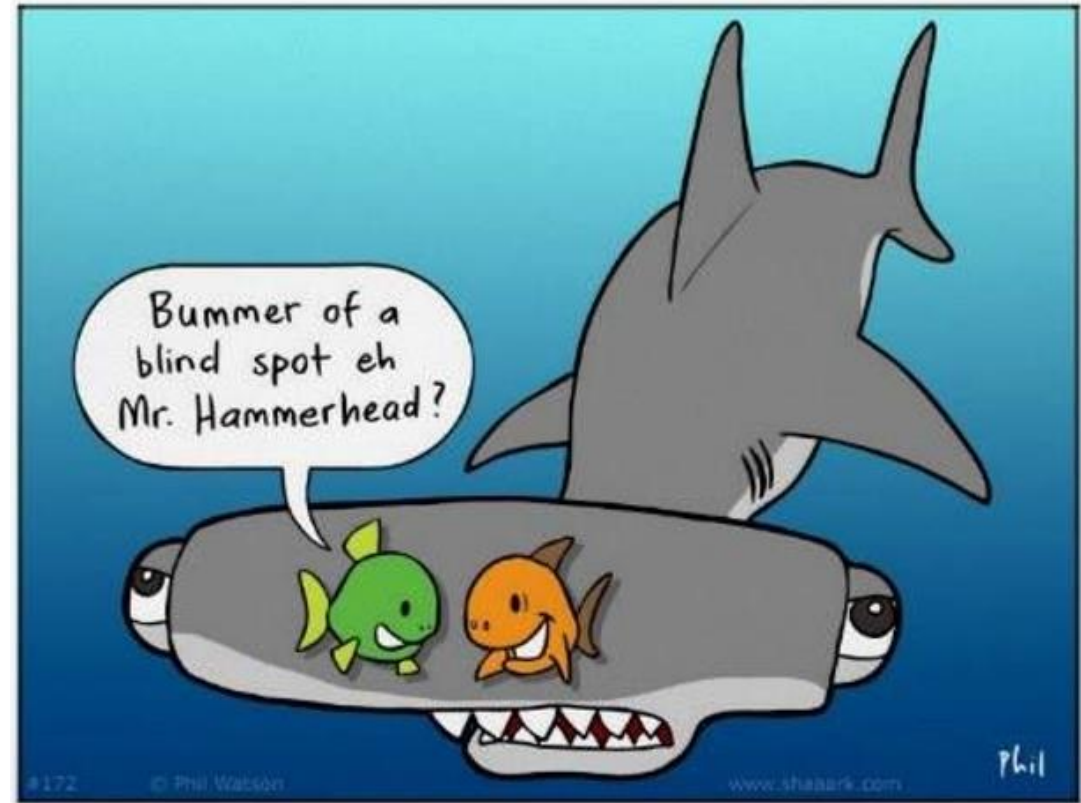
Identifying our blind spots

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?



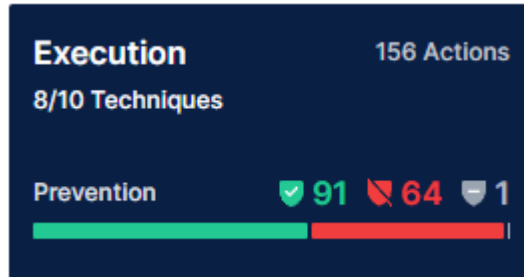
IDENTIFYING YOUR BLIND SPOTS:

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.

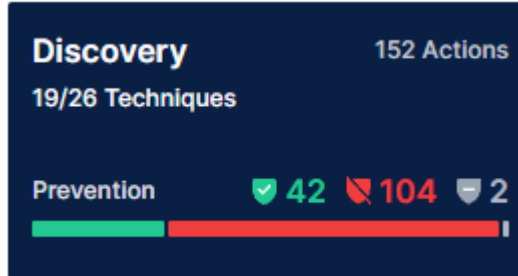


The Weakness:



Weakest:

- WMI
- Scheduled Tasks



Weakest:

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



Weakest:

- Scheduled tasks
- Boot or logon autostart

An aerial view of a city skyline at dusk or dawn, with a blue color overlay. A network of white lines and glowing nodes is superimposed over the city, representing a digital or cyber network. The lines connect various points across the city, with some lines being thicker and more prominent than others. The overall image has a futuristic and technological feel.

2023 Cyber Security action plan

Identify where you are?

Stage 1 - Hygiene

- EDR
- Edge / Firewalls
- Identity Management with MFA for Apps
- Disaster recovery
- Incident response plan
- Vulnerability and Patch Management
- Email flagging, filtering, and encryption.

Stage 2 - Limiting breaches

- Privilege access management
- Application segmentation
- SIEM / SOAR
- XDR Capabilities
- MSSP / SOC
- MFA at Desktop and Server Login
- Configuration Management

Stage 3 - Proactive

- Continuous validation
- Cyber engineer training
- Table top exercises

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



An aerial photograph of a city at night, with a blue color overlay. A network of white lines and glowing nodes is superimposed on the image, connecting various points across the cityscape. The lines are curved and intersect, creating a web-like pattern. The nodes are small, bright white circles. The city below shows a dense urban environment with many buildings and a prominent highway with multiple lanes.

QUESTIONS?

An aerial view of a city at night, with a blue tint. Overlaid on the city are white, glowing lines that form a network of arcs and straight paths, connecting various points across the urban landscape. The lines are thicker in some areas, suggesting a central hub or a major thoroughfare.

THANK YOU FOR ATTENDING!