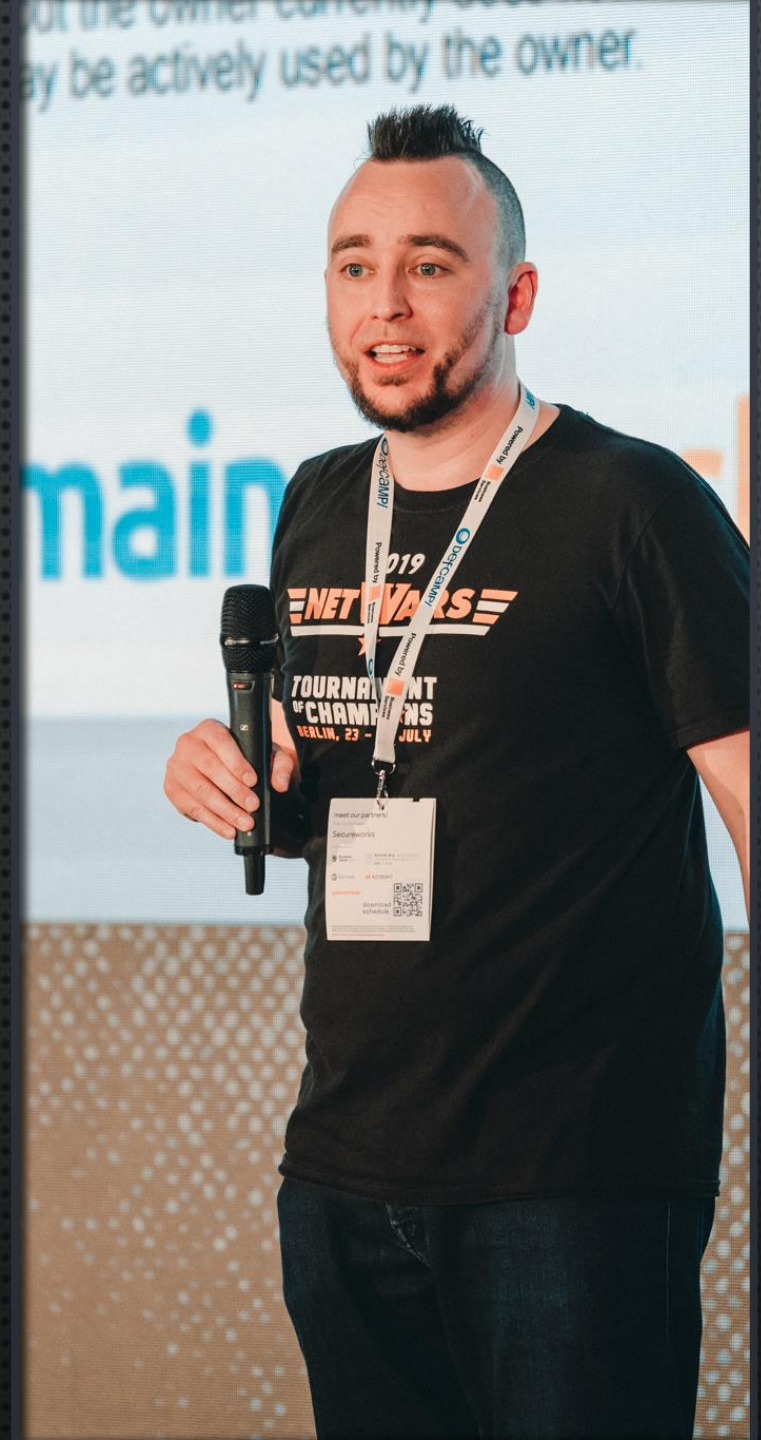
A day in the life as an Incident Responder

By Chris Dale – SANS and River Security



CHRIS DALE

- CHO, Principal and Founder at River Security
- Principal Instructor at SANS

Short WHOAMI:

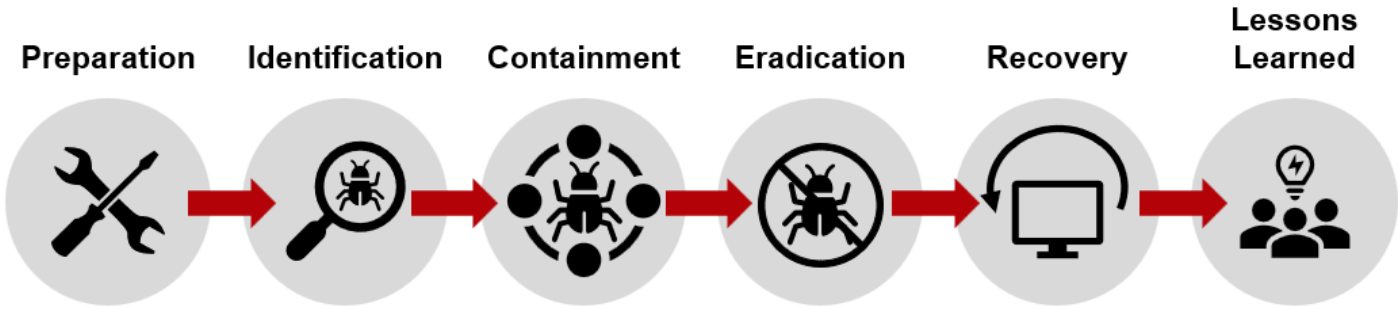
I show how criminals break-in, and I help throw them back out…

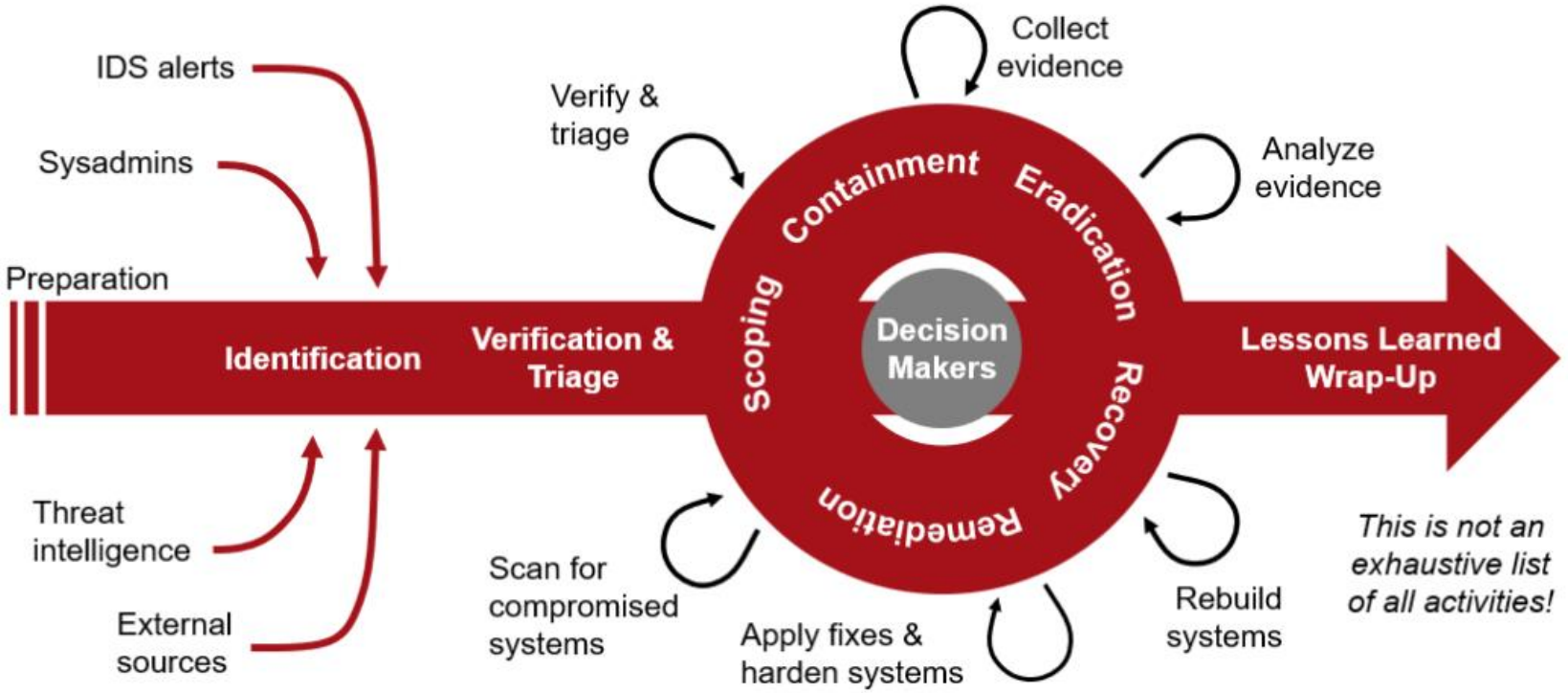
CERTS

GCIH	GIAC Certified Incident Handler
GPEN	GIAC Certified Penetration Tester
GSLC	GIAC Security Leadership
GIAC	GIAC Mobile Device Security Analyst
GDAT	GIAC Defending Advanced Adversaries
GCTI	GIAC Cyber Threat Intelligence
GCFA	GIAC Certified Forensic Analyst
GXIH	GIAC Experienced Incident Handler
GXPT	GIAC Experience Penetration Tester
GSP	GIAC Security Professional

Incident Resoonse

- Extremely Interesting Field with Lots of Potential





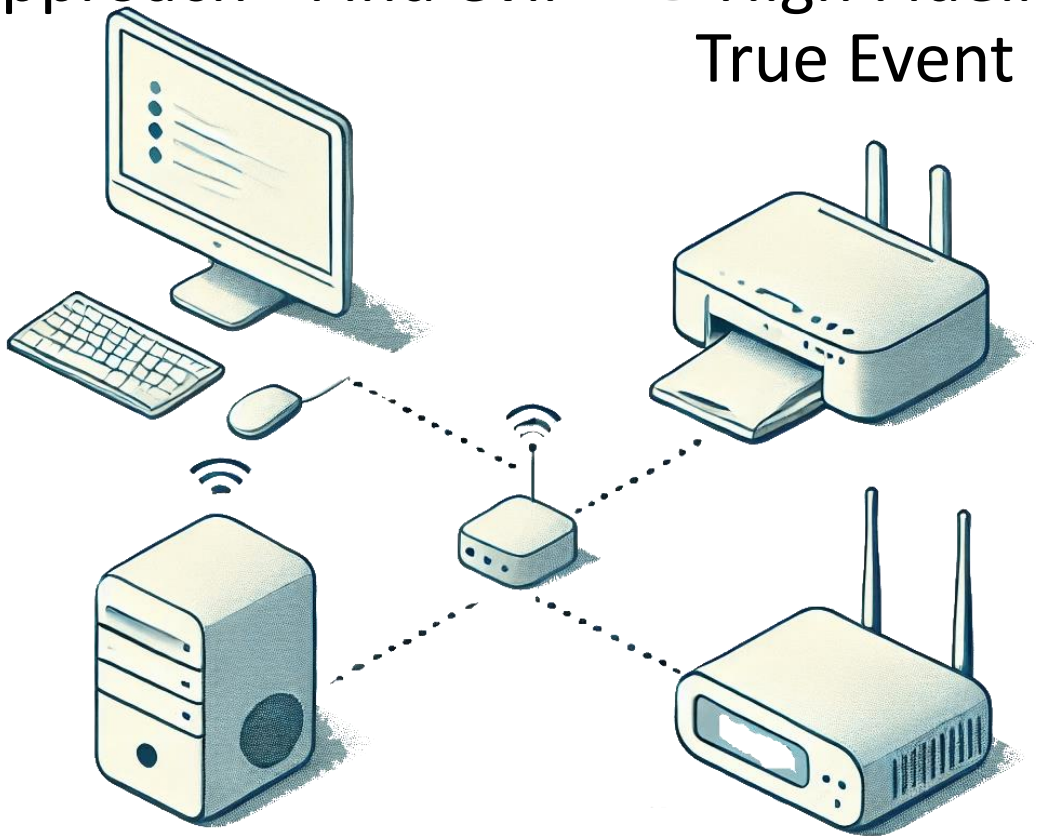
- Lots of Areas to Study and Improve

My Responsibilities in IR

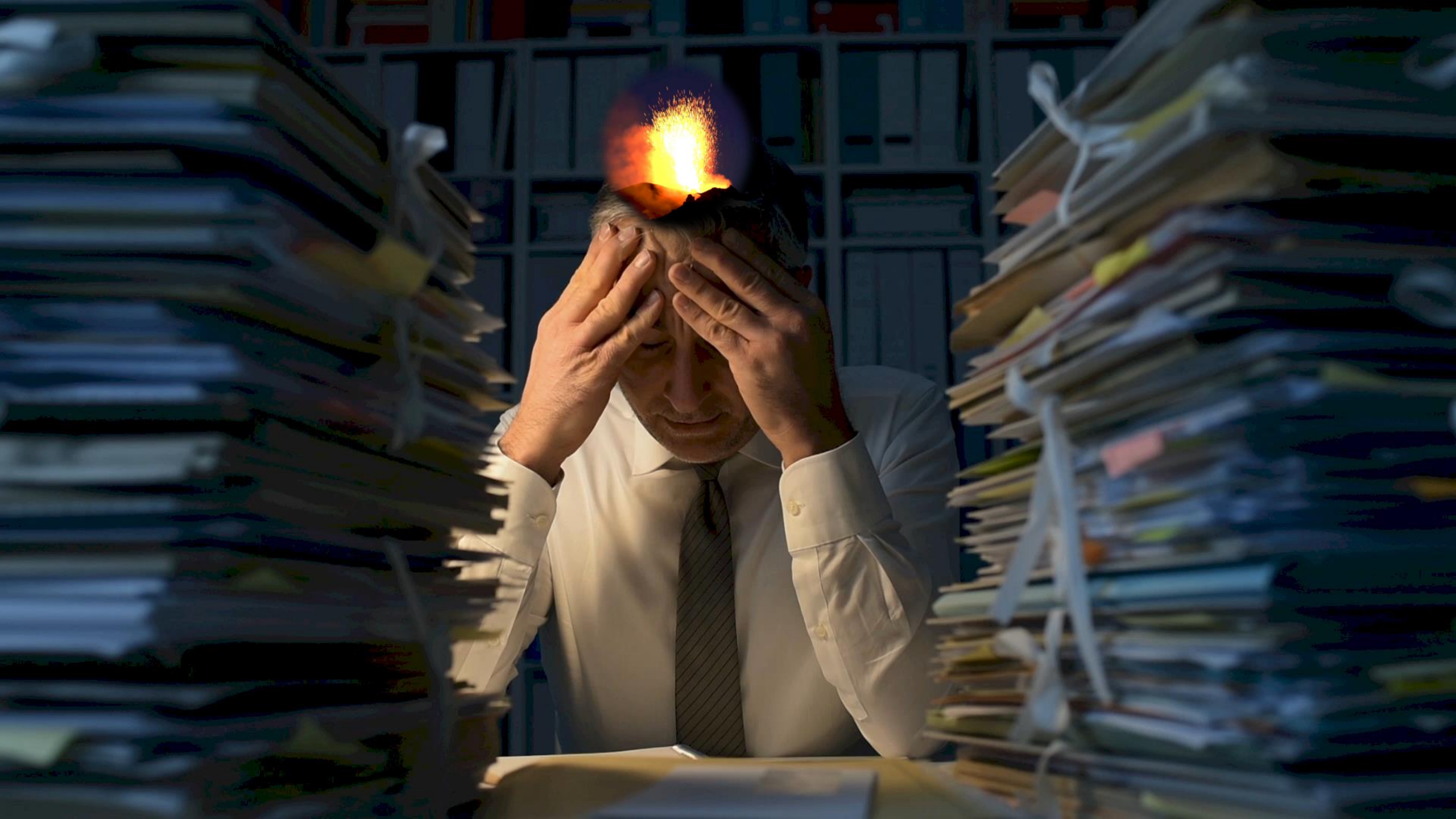
- I belong in the class of “Chaos Pilot”
- When I am called, it is generally “too late” – damage has been done
- Incident Response should ideally be more proactive
- Responding to alerts is generally challenging due to fidelity

Fidelity Example - LLMNR

- Low Fidelity Approach - Find evil LLMNR
- High Fidelity Example – Actual True Event




RIVER
SECURITY
It is not a matter of IF you get hacked
But WHEN you get hacked




"EVERYONE HAS A PLAN UNTILL THEY GET PUNCHED IN THE MOUTH"
MIKE TYSON

Zenmap

Scan Tools Profile Help

Target: [redacted] Profile: Quick scan Scan Cancel

Command: nmap -T[redacted]

Hosts Services

OS Host

[redacted].no

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 [redacted] Details

```
Starting Nmap 5.21 ([redacted]Vest-Europa (sommertid)
Nmap scan report for[redacted]
Host is up (0.014s latency).
Not shown: 96 filtered ports
PORT     STATE  SERVICE
25/tcp   closed smtp
80/tcp   open   http
443/tcp  open   https
3389/tcp open   ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 3.05 seconds
```

Fighting Assumptions

- And asking stupid questions
- 50/50 of my cases, customers had the wrong initial assumptions
  - “Our mobile application is being DDOS’ed”
  - “Our user received an email with an attachment that contained malware”

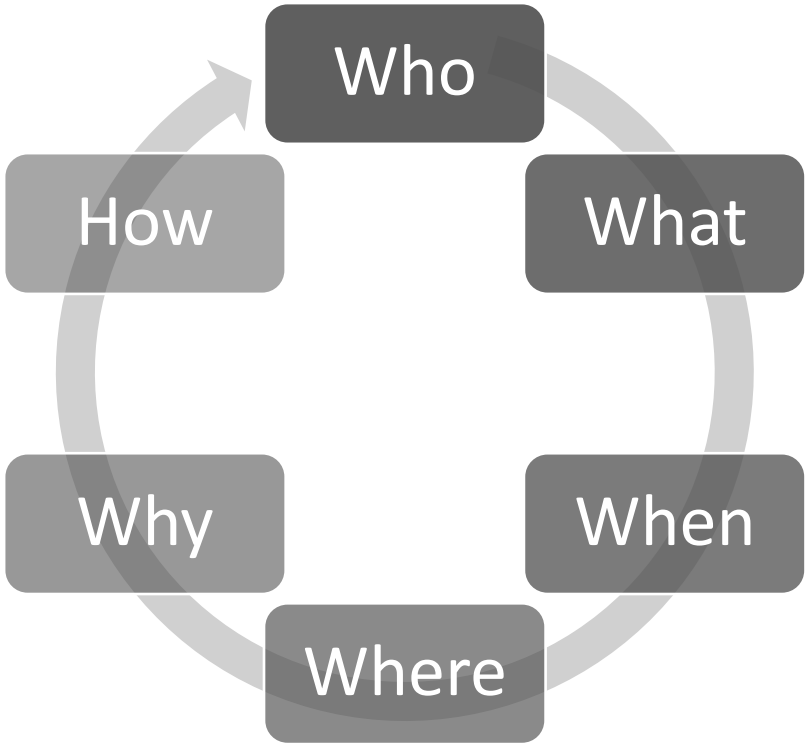
Response Policies

Contain & Clear
vs.
Watch & Learn

Maintain secrecy
vs.
Peer disclosure

Scoping and Triage: The 5 W and 1 H

- Think like a journalist
- Use the 5 W's and 1 H to assess the situation

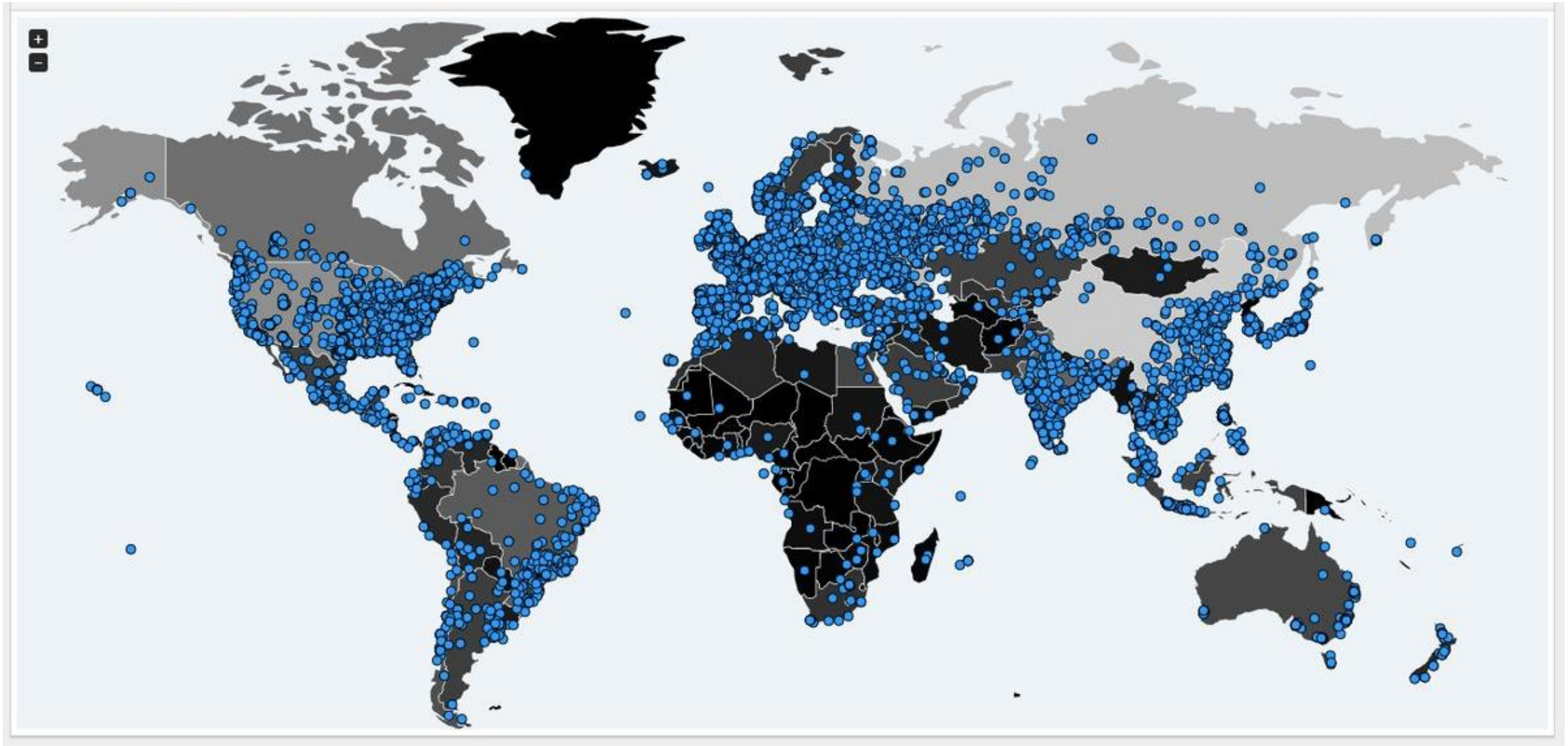


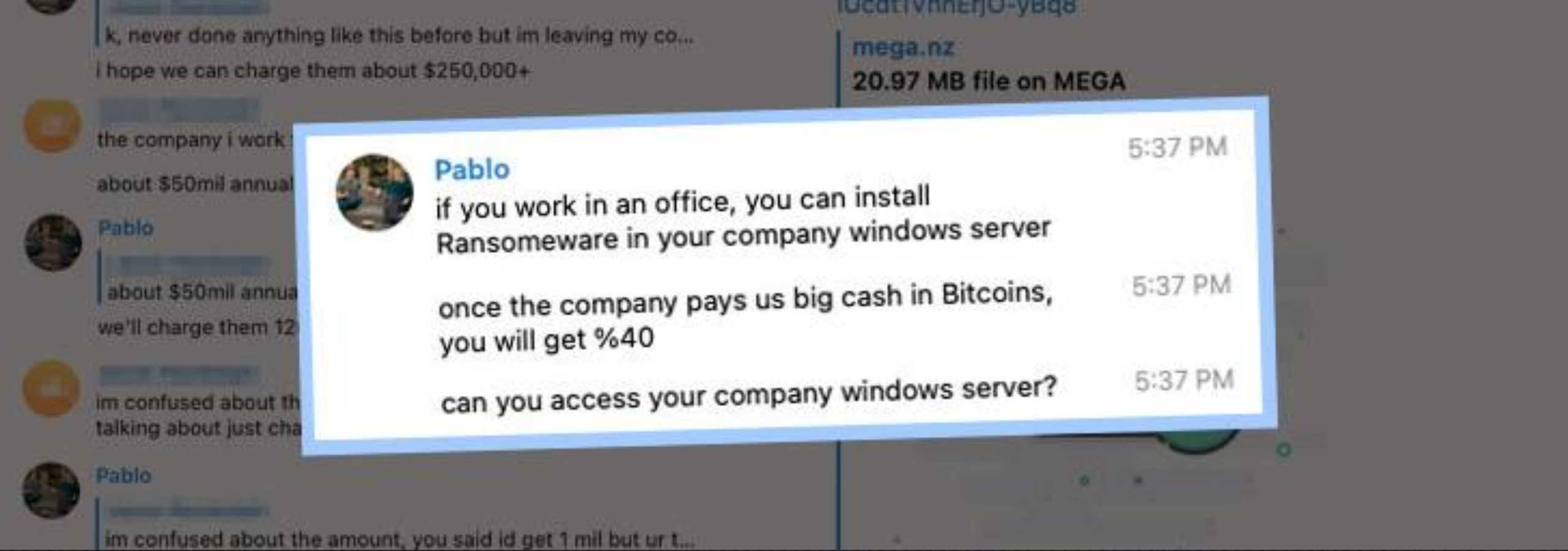
RIVER SECURITY

Ransomware

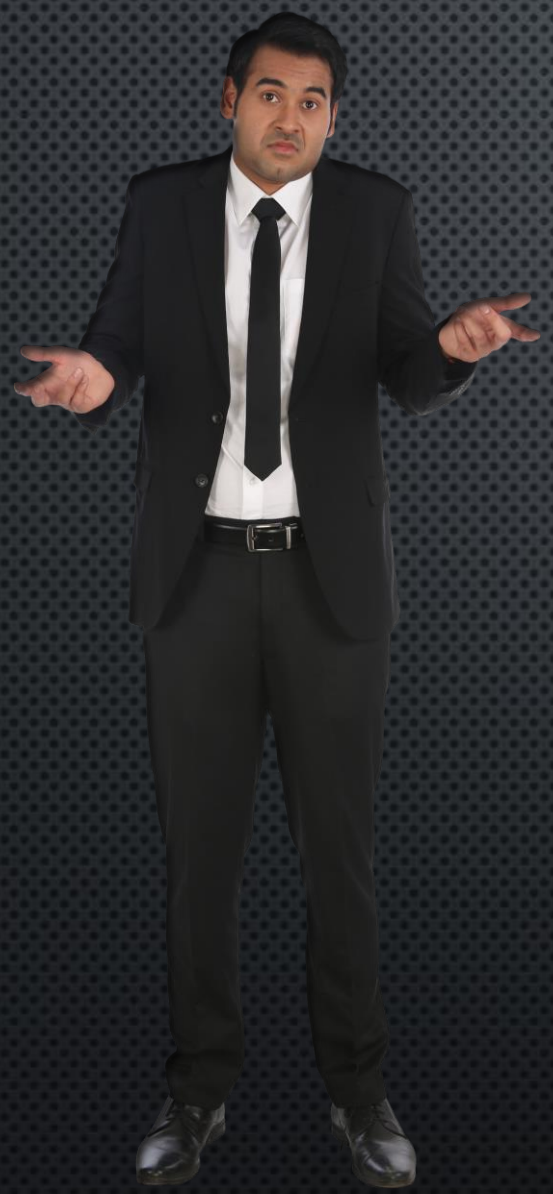
The Never Ending Story

WANNACRY




k, never done anything like this before but im leaving my co...
i hope we can charge them about $250,000+
the company i work
about $50mil annual
Pablo
about $50mil annua
we'll charge them 12
im confused about th
talking about just cha
Pablo
im confused about the amount, you said id get 1 mil but ur t...
mega.nz
20.97 MB file on MEGA
Pablo
5:37 PM
if you work in an office, you can install Ransomeware in your company windows server
once the company pays us big cash in Bitcoins, you will get %40
5:37 PM
can you access your company windows server?
5:37 PM

2021



YET **STILL** TODAY

Business Leaders & Board members prove direct ignorance on Cyber Crime

"Why Would Anyone Want to Hack Me?"

Breachsense Monthly Summary: August 2024

Efron Law Firm	Jangho	Brontoo Technology Solutions	Glazkov	Tiendas Macuto	Findel	Chama Gaucha	Omicron Granite & Tile	Sports and Spine Orthopaedics	Flodraulic Group
EBL Partners	Khandelwal Laboratories	Credible Group	Gauteng Partnership Fund	NR Collecties	KidKraft	Idaho Pacific Lumber	GrandPalaisRmn	Burgess Kilpartik	McPhillips
Pharmaceutics International	LRN	Nilorn	Safefood	Zyxel	Luigi Convertini	Crimson Interactive	TJS	Richmond Auto Mall	Ranger American
NYDJ	Eastern Sales	Ark Workplace Risk	Gaston Fence	Wm. W. Meyer & Sons	Burns Industrial	Stahly Engineering & Associates	Agra Services	Seng Tsoi Architect	VOP CZ
Schneider Regional Medical Center	Silipos	Anniversary Holding	American Contract Systems	Vinakom	Saint Peter's Villa	Akkanat Holding	Medisetter	Raeyco Lab Equipment Systems Management	Roberto Verino Difusión
City of Columbus, Ohio	Hi-P Group	Global Cargo Alliance	Element Food Solutions	Keios	Olympus Financial	U.S. Marshals Service	Fish Nelson & Holden	Welding and Fabrication	United Methodist Retirement Homes
Sable International	EXCO	Majestic Metals	Aerotech Solutions	Lennartsfors	Globacap	Anderson Oil & Gas	Klockmetal	Prism Construction	W.A. Richardson Builders
Florence Cement	HP Distribution	Fathom	E-Z UP	Rostance Edwards	Gerald Singleton	Microchip Technology	M.Royo	Cotala Cross-Media	Reward Hospitality
Carlex	Square One Coating Systems	DDM Concut	Adina Design	SuperDrob	The Pyle Group	PreCom	ScottPharma Solutions	Phyton Biotech	DealScoop
Find Great People	Banx	Dynasty Healthcare Group	CinemaTech	Patelco	Percento Technologies	Vans Lumber & Custom Builders	Fresh Aire Franchise	Grant Associates	Heaford
Braspress	KinetX	[illegible]	[illegible] Meats	Hiesmayr H[illegible]technik	Boligforeningen VIBO	Optimize Generator	[illegible]	[illegible]ands	Tur[illegible]
FINGERS	Granit Design	Dunn[illegible]	[illegible]	Promises2K	HVB Ingenieurgesellschaft	Complete [illegible]roll Solutions	Comm[illegible]l Truck Equipm	Ti[illegible] Teleco[illegible]	[illegible] Western [illegible]pplies
Kleven Construction	Alternate Energy	Sumt[illegible]County Sheriff	S[illegible] Taxi	Prefeitura d[illegible]boatão dos Guarara[illegible]	West[illegible]ans	[illegible]	[illegible]	Ministerio Educació[illegible]	Stein Fit
Priefert	Burger Industriewerk	Pierre Diamonds	Boni	on365	Dunlop Aircraft Tyres	Brookshire Dental	Success Microbank	Suva City Council	TCIDA
Durham	SOBHA	Golfoy.com	Washington Times	Central College Jounieh	SchoolRush	UAE Government	Tranter	IPH Ingénierie	Parrish
Dometic	Ziba Design	Moser Wealth Advisors	Benson Kearley IFG	BTS Biogas	Life University	Criminal Psychology	Risser Oil	John Kellys London	Farmers' Rice Cooperative
PeoplesHR	IOI Group	Netcomms	Texas Centers for Infectious Disease Associates	Yang Enterprises	Instadriver	Pryx Fanbase	Clatronic	The Fence Authority	The Bakersfield Californian
National Beverage	Fatboy	Amco	Thompson Davis	Carver Companies	Cincinnati Pain Physicians	Saudi Government	Hollywood Burbank Airport	Gruyeria	Crain Group
Valley Bulk	Casco Antiguo	Ayurcann	Riley Pope & Laney	J&J Network Engineering	Level Supermind	Widex	Oceanside Glasstile	Viña Luis Felipe Edwards	Seirus
Effingham County Schools	Omni Family Health	The Link Group	praca.gov.pl	Per4mance	UFCW Local 135	Harris Technology Services	Stiller Aesthetics	Riverside Resort Hotel and Casino	Sunrise Erectors
McDowall Affleck	Fractalia	DM Merchandising	M&M Transport	SMK	EBA	SPIE TEC	Corbally Gartland and Rappleyea	La Cité Internationale de la Bande Dessinée et de l'Image	Galgorm
dahl Valve	UnitedHealthcare	Luis Oliveras	Southwest Family Medicine Associates	AER Worldwide	Kronick Moskovitz Tiedemann & Girard	PocketRisk	Malone Toyota	Ramón Corripio	Performance Controls
Association of Christian Schools International	Landal GreenParks	All Weather Architectural Aluminum	Sterling Rope	Zydus	Don't Waste Services	Smart ERP Solutions	Gortemoller	Indraprastha Institute of Information Technology Delhi	Akanea

WITH THE HISTORY OF RANSOMWARE BEHIND US

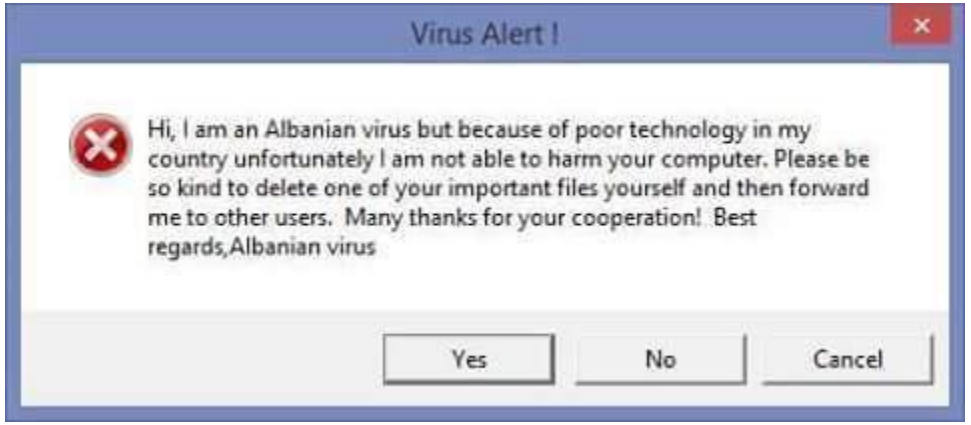
ASK YOURSELF:
WHEN WAS YOUR BACKUP DESIGNED, AND WHAT WAS IT DESIGNED FOR?

STORY TIME & THE ELEPHANT IN THE ROOM

- First Ransom: Unlock data
- Second ransom: Data theft
- Triple Ransom: Individuals pressured

My Experience

- Can be extremely stressful and taxing
  - Taxing on both family and business
- IR requires people to answer questions, not just ask them
- Technically stimulating work
- In general rewarding work if you can “save the day”
- There is a lot of potential in IR, but not always willingness to invest



RIVER SECURITY

THANK YOU!

Fight Cyber Crime! – https://riversecurity.eu

https://into.bio/chrisdale & https://into.bio/rivsec

Download slides here!

Twitter – https://twitter.com/ChrisADale

LinkedIn – https://www.linkedin.com/in/chrisad/