Countdown to Crisis: Making Smart Decisions in High Stakes

Ben Jenkins
Director, Cybersecurity

THREATLOCKER

THREATLOCKER

Software

THREATLOCKER

Microsoft Office

Google Chrome

Adobe Reader

Dropbox

THREATLOCKER

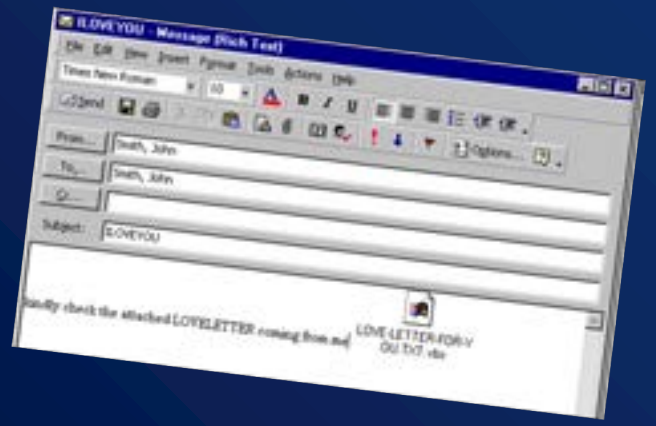
THREATLOCKER

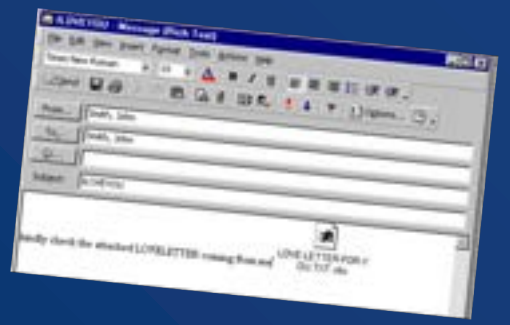
The Possibilities Are Endless

THREATLOCKER

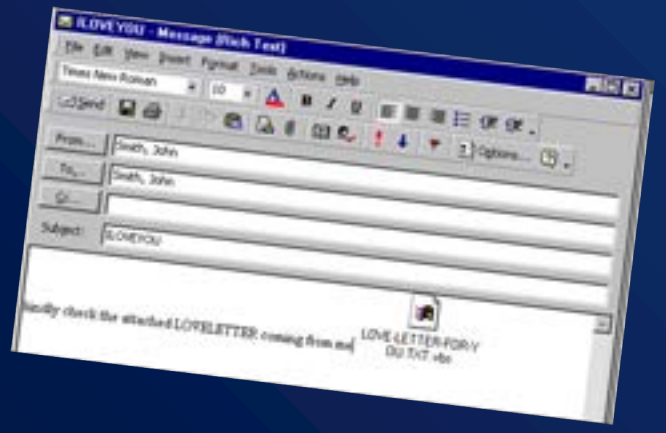
Malware is Software

THREATLOCKER





Malicious Possibilities Are Endless



THREATLOCKER

AIDS Trojan

First Ransomware Attack

Pay $189 to release data

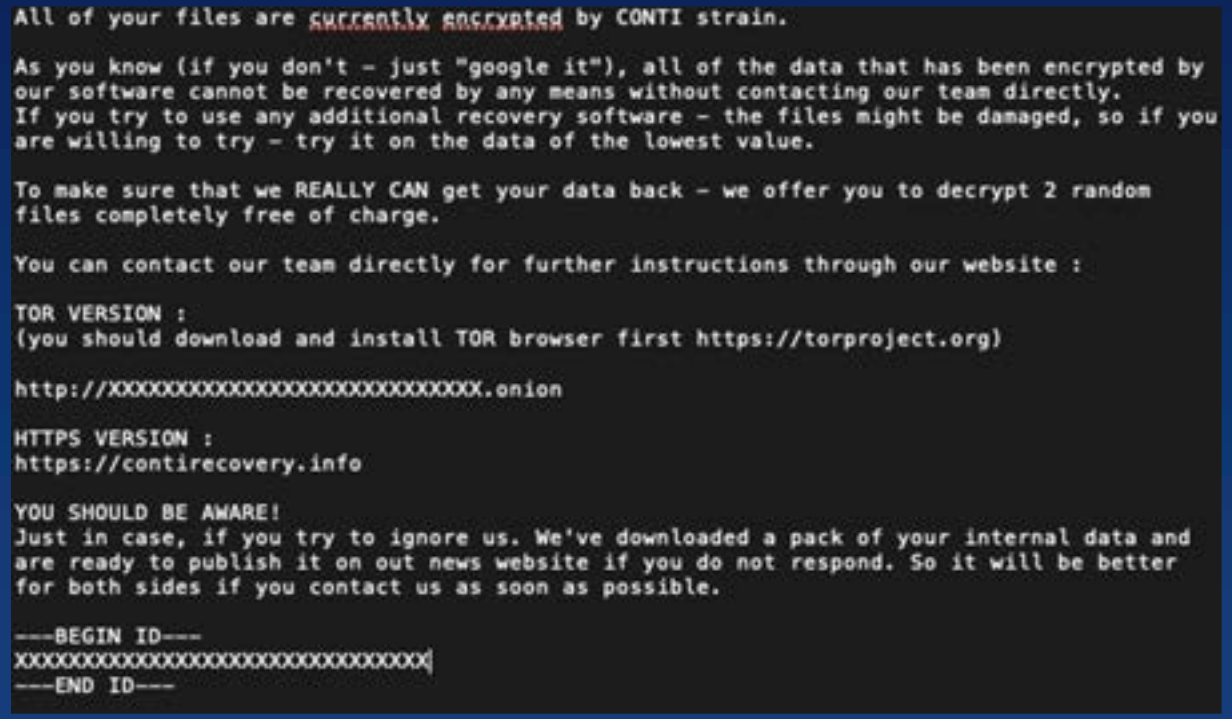
THREATLOCKER

WannaCry Attack

- £92m estimated cost
- 200 Trusts failed one year later

THREATLOCKER

Conti V3 Attack



- Over 500m estimated cost
- Still recovering

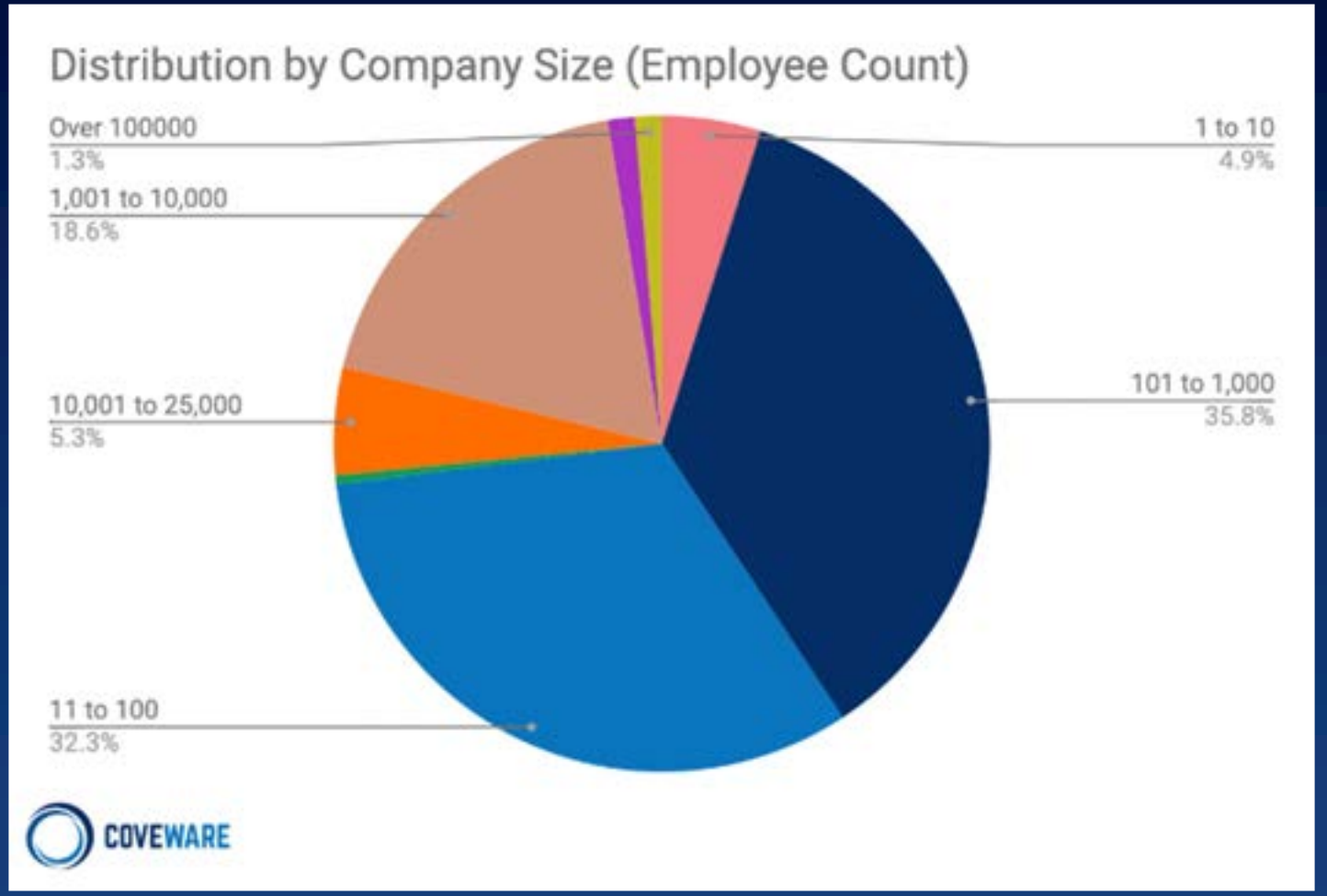
Smaller Attacks

- $1500 to pay

THREATLOCKER

2021 Attacks

- Endpoint management breaches
- MerseyRail
- The National College of Ireland
- Cambridge Meridian Academy Trust
- CD Projekt


Distribution by Company Size (Employee Count)
Over 100000
1.3%
1,001 to 10,000
18.6%
10,001 to 25,000
5.3%
11 to 100
32.3%
1 to 10
4.9%
101 to 1,000
35.8%
COVEWARE

THREATLOCKER

Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

Average Ransom Payout - £170,000

77% of Ransomware Attacks involved the threat to leak exfiltrated data

The data will not be credibly destroyed

Ransomware attacks still disproportionally affect small businesses

Average 23 days of downtime

Source: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound


THREATLOCKER
Targeting MSPs, SMBs and Enterprise

Threat actors are **innovating** how they deliver malware.

THREATLOCKER

Print Nightmare

Affected Windows 7 and Higher

Allows Privilege Escalation and Remote Code Execution

Log4j

- Affects over 3 billion devices
- Allows remote code execution

THREATLOCKER

Living Off The Land

LOLBAS Project

THREATLOCKER

How can we solve this problem?

Antivirus AV 2.0

A.I. **Heuristics**

Threat Hunting SOC

Ransomware Detection

Next Gen Antivirus

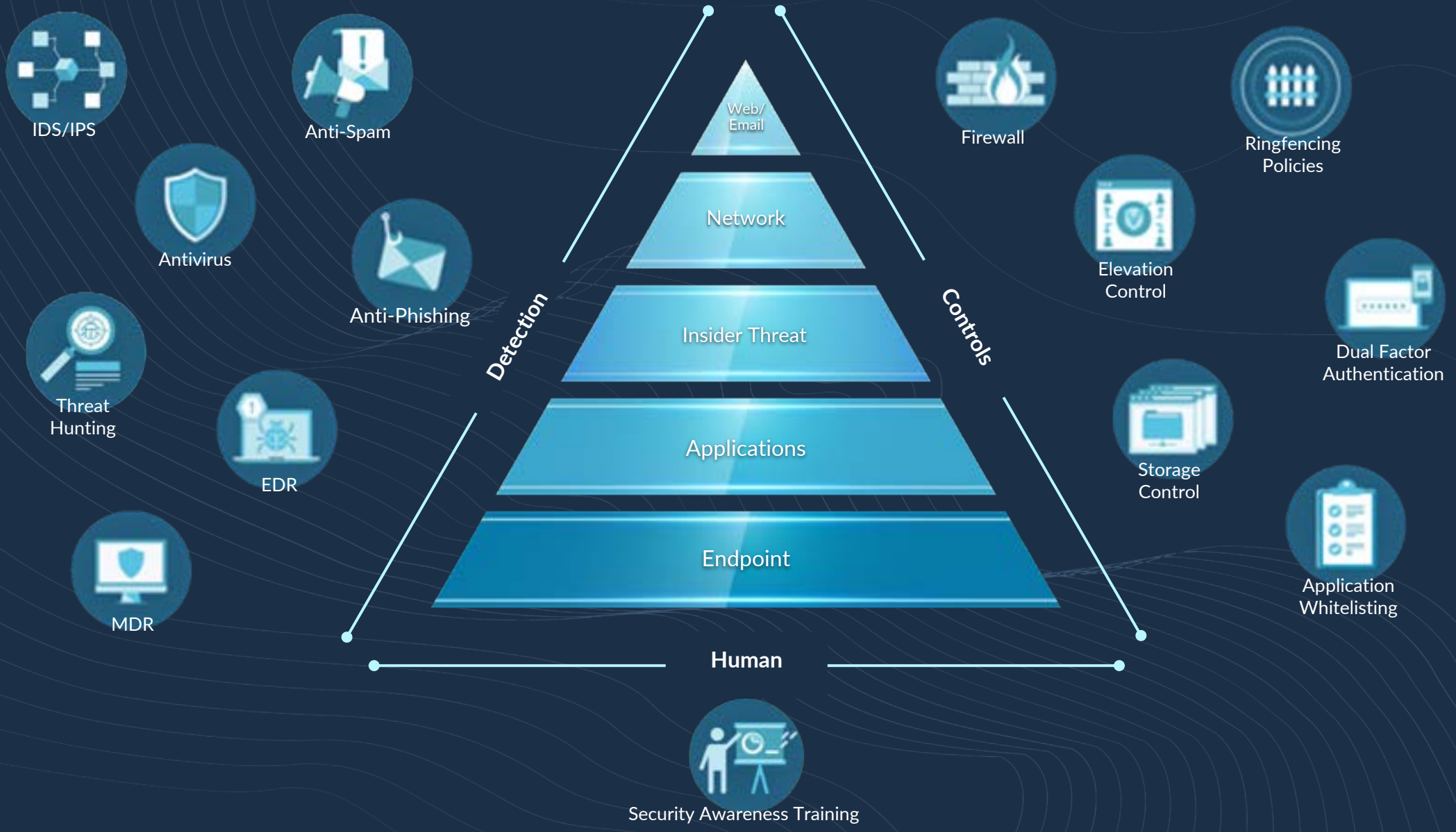
THREATLOCKER

This is Not Working

THREATLOCKER

There Are Solutions

THREATLOCKER



THREATLOCKER

Zero Trust

= Least Privilege

THREATLOCKER

Application Whitelisting

THREATLOCKER

Office

PowerShell

THREATLOCKER

PowerShell

Files and Folders

07/28/2020 00:47:12

Here are the list of recommendations to avoid such a things in future:
- Turn off local passwords
- Force end of administrators sessions
- In group policy set up wdigest value to "0", If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.
- Update passwords every month !
- Check the granted privileges for users, to make them maximum reduced privileges and access only to exact applications.
- In most cases there would enough standard windows software like an Applocker.
- Approve to run only necessaries applications ONLY.
- Don't count on the Anti-Virus, there is no one AV that really helps, they can be useful only in long-term infections, if hackers for some reasons didn't attack in short time.
- Install Endpoint Detection and Response security (EDR) and teach the IT-admin to work with it.
- For huge companies we suggest at least 3 system administrators working 24 hours, maximum 4 admins working 3 shifts for 8 hours per day, that would be enough.

You

07/28/2020 00:51:17

Thank you for all of this in a very timely manner

07/28/2020 00:53:29

Support

You are welcome it's a pleasure to work with professionals. If there will be any questions, please feel free to ask

07/28/2020 01:23:07

Support

Please confirm that you wrote down all important information from this Chat, so we could clear it. However we will keep the chat room and will be here for your support if necessary

THREATLOCKER

Elevation Control

THREATLOCKER

Storage Control

THREATLOCKER

Control Folder Access by Application?

THREATLOCKER

Change the Paradigm of Endpoint Security

Thank You

Book a Demo

THREATLOCKER