

Countdown to Crisis: Making Smart Decisions in High Stakes

Ben Jenkins
Director, Cybersecurity

THREATLOCKER

Software



Microsoft Office



Google Chrome



Adobe Reader

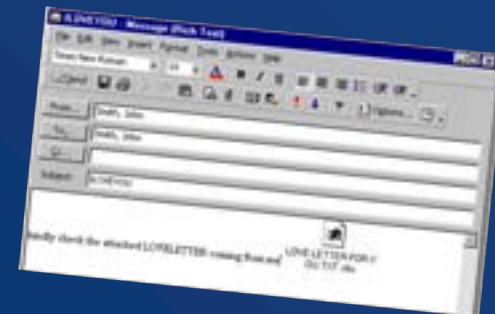
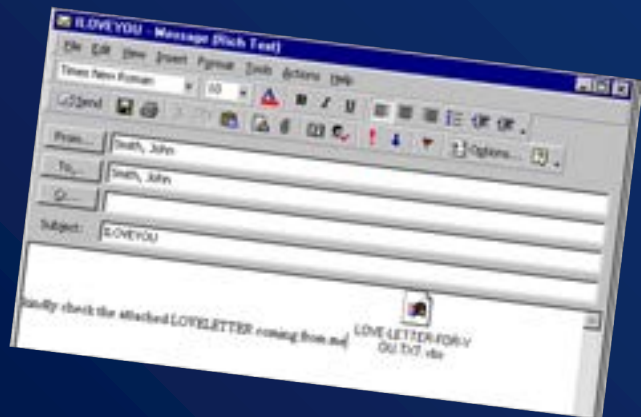


Dropbox

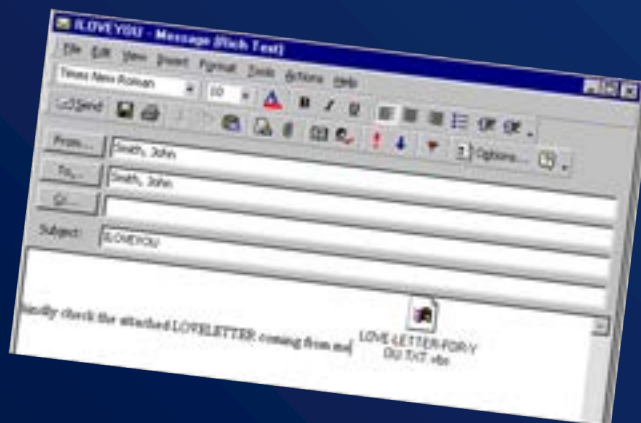


The Possibilities Are Endless

Malware is Software



Malicious Possibilities Are Endless



AIDS Trojan

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

First Ransomware Attack

Pay \$189 to release data

WannaCry Attack



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

Conti V3 Attack

```
All of your files are currently encrypted by CONTI strain.  
  
As you know (if you don't - just "google it"), all of the data that has been encrypted by  
our software cannot be recovered by any means without contacting our team directly.  
If you try to use any additional recovery software - the files might be damaged, so if you  
are willing to try - try it on the data of the lowest value.  
  
To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random  
files completely free of charge.  
  
You can contact our team directly for further instructions through our website :  
  
TOR VERSION :  
(you should download and install TOR browser first https://torproject.org)  
  
http://XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.onion  
  
HTTPS VERSION :  
https://contirecovery.info  
  
YOU SHOULD BE AWARE!  
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and  
are ready to publish it on our news website if you do not respond. So it will be better  
for both sides if you contact us as soon as possible.  
  
---BEGIN ID---  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX|  
---END ID---
```

- Over 500m estimated cost
- Still recovering

Smaller Attacks

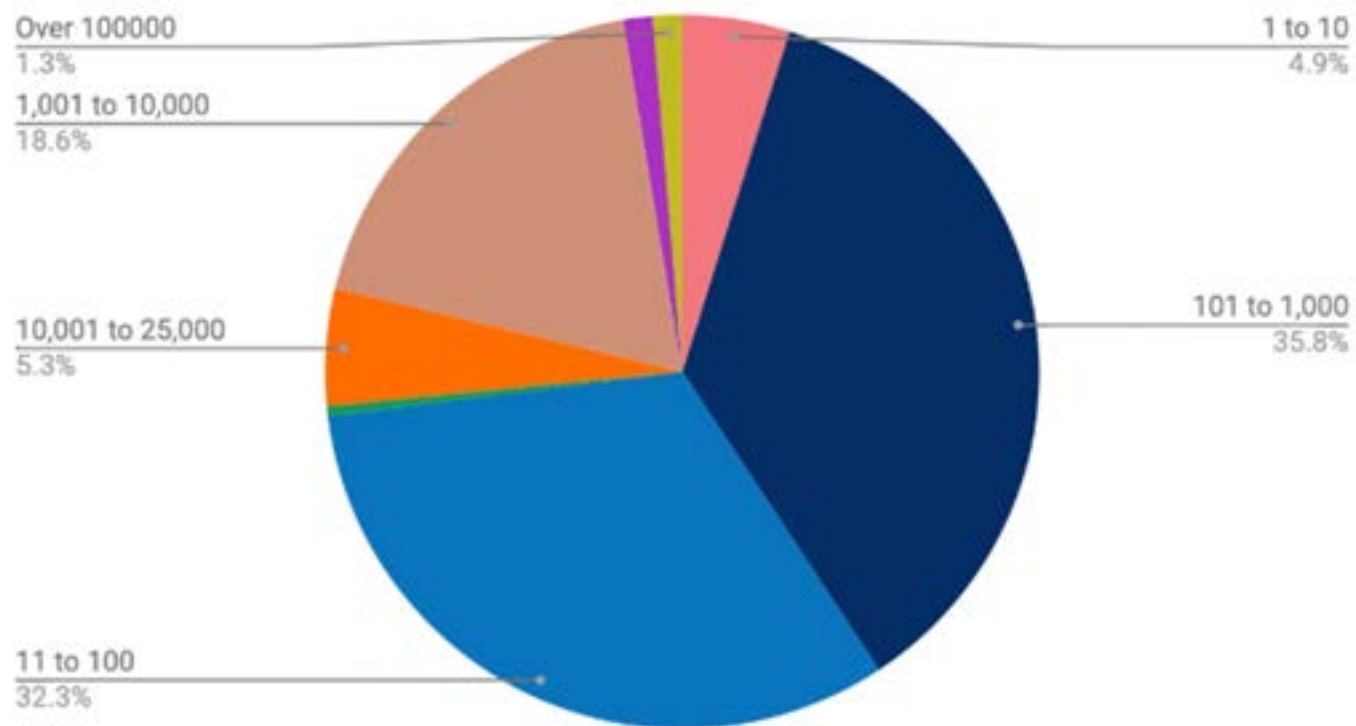


- \$1500 to pay

2021 Attacks

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

Distribution by Company Size (Employee Count)



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 disproportionately affect small businesses

Average 23 days of downtime

Targeting MSPs, SMBs and Enterprise

solarwinds 


Kaseya®

Rubber
Duckies

Vulnerabilities

THREATLOCKER

Threat actors are
innovating how they
deliver malware.

Print Nightmare



PrintNightmare

**Affected Windows 7
and Higher**

**Allows Privilege
Escalation and Remote
Code Execution**

Log4j



- Affects over 3 billion devices
- Allows remote code execution

Living Off The Land



LOLBAS Project

How can we solve this problem?

Antivirus AV 2.0

A.I. Heuristics

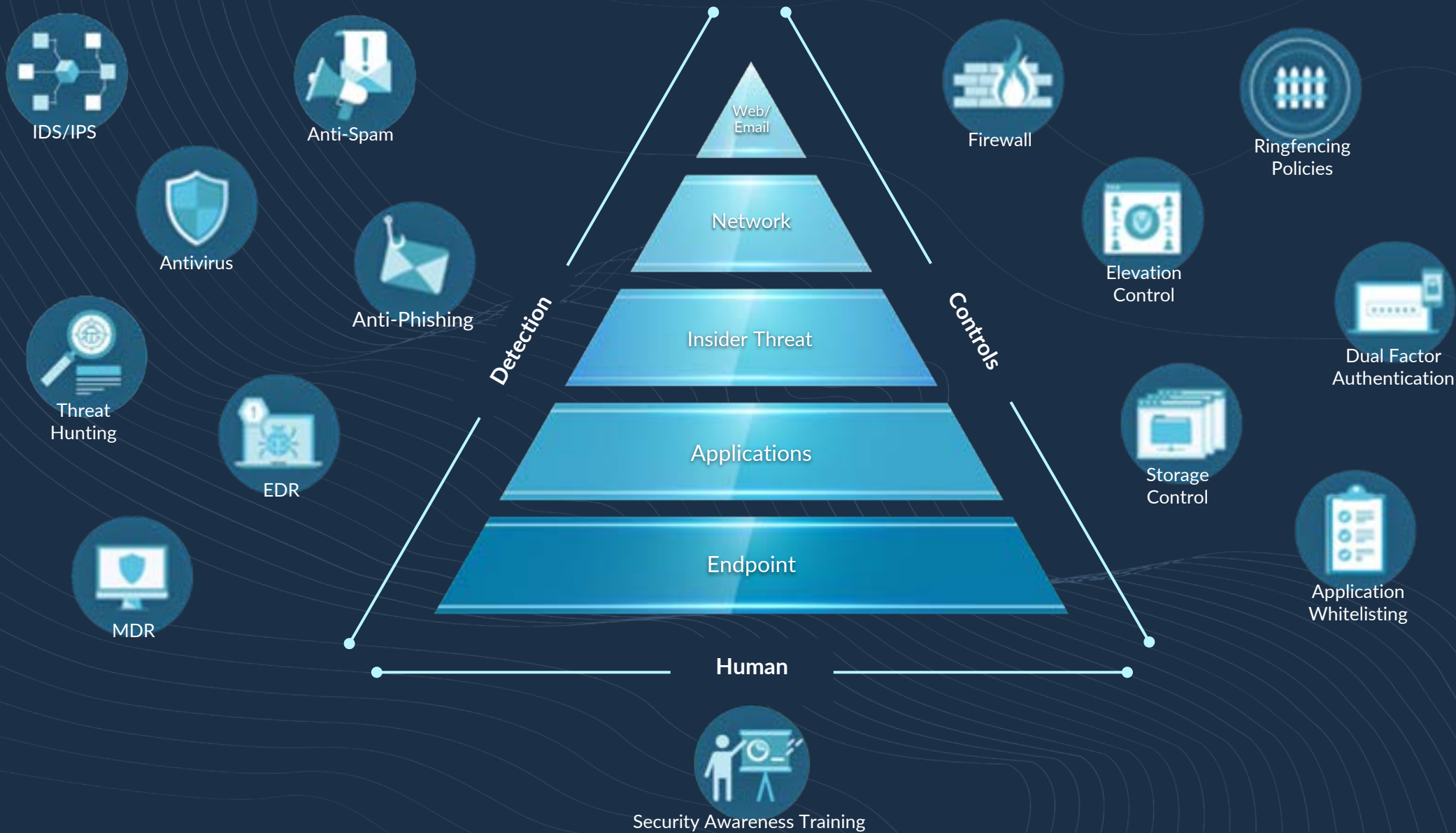
Threat Hunting SOC

Ransomware Detection

Next Gen Antivirus

This is Not Working

There Are Solutions



Zero Trust

= Least Privilege

Application Whitelisting



Office



PowerShell



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 necessities 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

Thank you for all of this in a very timely manner

07/28/2020 00:51:17

07/28/2020 00:53:28

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



Elevation Control

Storage Control

Control Folder Access by Application?



Change the Paradigm of Endpoint Security

Thank You
Book a Demo
THREATLOCKER

