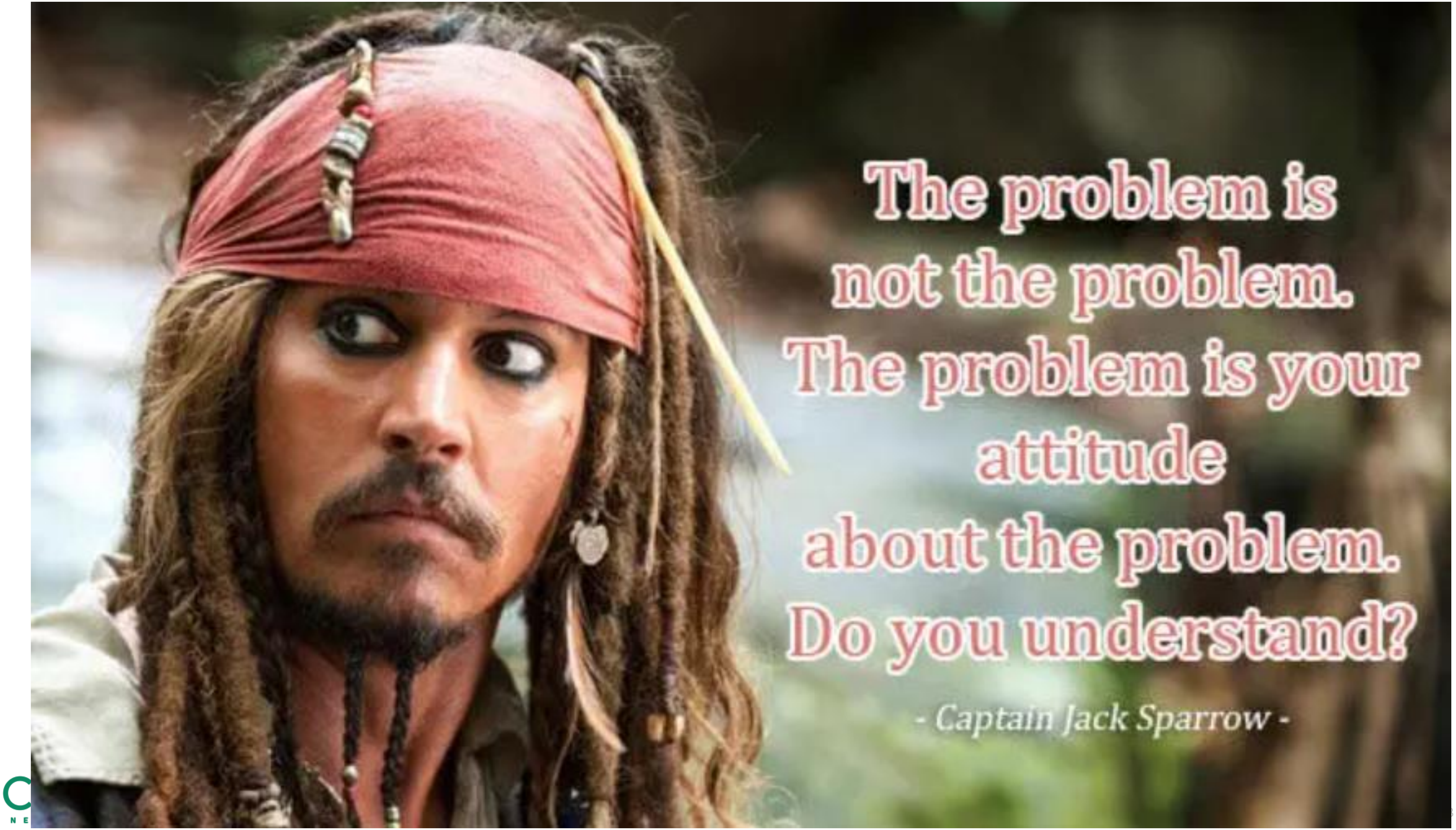
CATO NETWORKS

Busting Cybersecurity Myths

Etay Maor, Sr. Director Security Strategy, Cato Networks

The Attacker Needs To Be Right Just Once, The Defenders Have To Be Right All The Time!

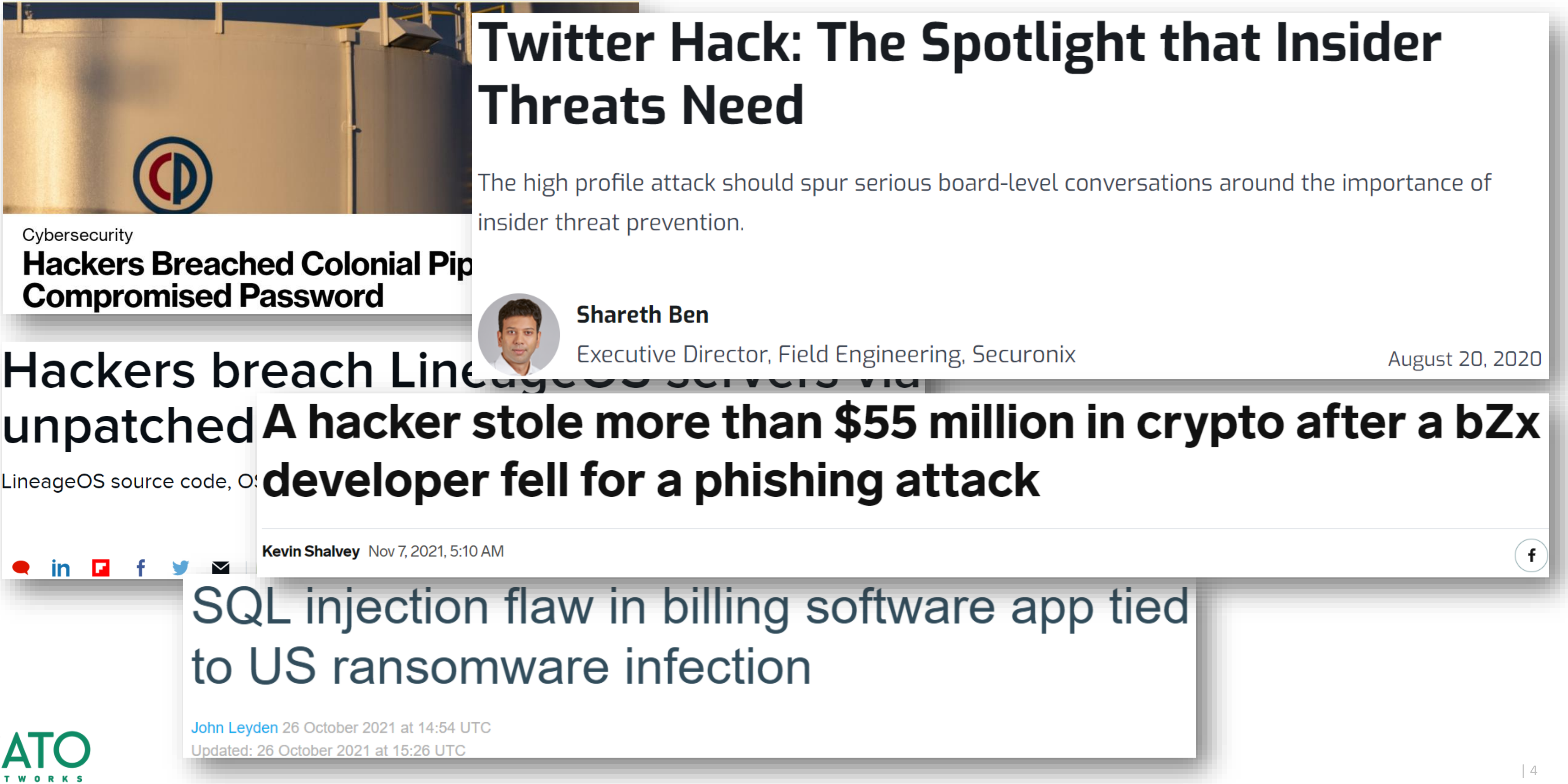
Myth I



The problem is
not the problem.
The problem is your
attitude
about the problem.
Do you understand?

- Captain Jack Sparrow -

The Single Point Of Failure Fallacy



Cybersecurity

Hackers Breached Colonial Pip

Compromised Password

Twitter Hack: The Spotlight that Insider Threats Need

The high profile attack should spur serious board-level conversations around the importance of insider threat prevention.

Shareth Ben

Executive Director, Field Engineering, Securonix

August 20, 2020

Hackers breach LineageOS servers via unpatched

LineageOS source code, O

A hacker stole more than $55 million in crypto after a bZx developer fell for a phishing attack

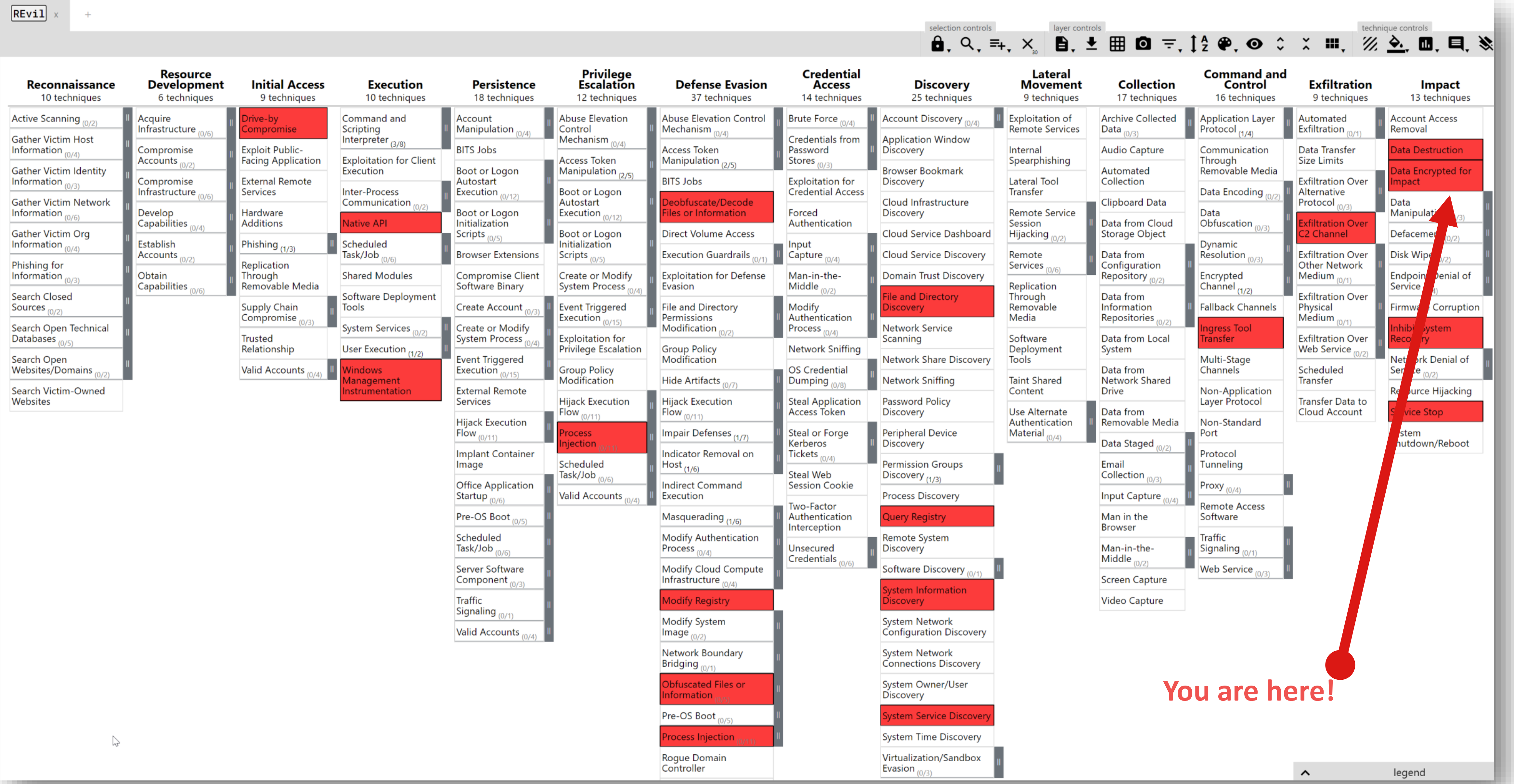
Kevin Shalvey Nov 7, 2021, 5:10 AM

SQL injection flaw in billing software app tied to US ransomware infection

John Leyden 26 October 2021 at 14:54 UTC

Updated: 26 October 2021 at 15:26 UTC

The Attacker Needs To Be Right Just Once, The Defenders Need To Be Right All The Time



Reconnaissance
10 techniques

- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development
6 techniques

- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
10 techniques

- Command and Scripting Interpreter (3/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/6)
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Container Image
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/6)
- Server Software Component (0/3)
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (2/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/6)
- Valid Accounts (0/4)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (2/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (1/7)
- Indicator Removal on Host (1/6)
- Indirect Command Execution
- Masquerading (1/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (0/5)
- Pre-OS Boot (0/5)
- Process Injection (0/11)
- Rogue Domain Controller

Credential Access
14 techniques

- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/6)

Discovery
25 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (1/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (1/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

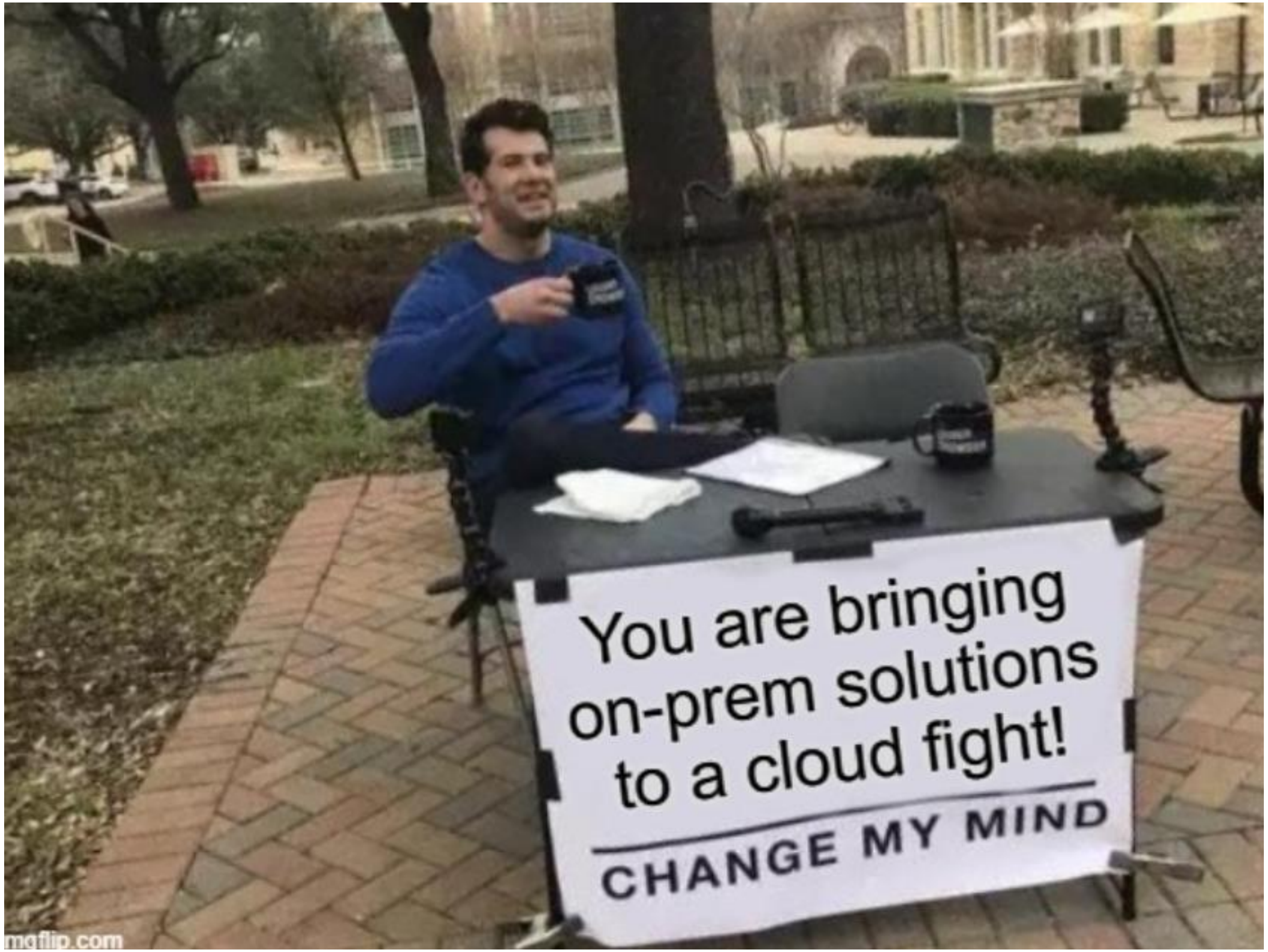
Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

You are here!

CATO
NETWORKS

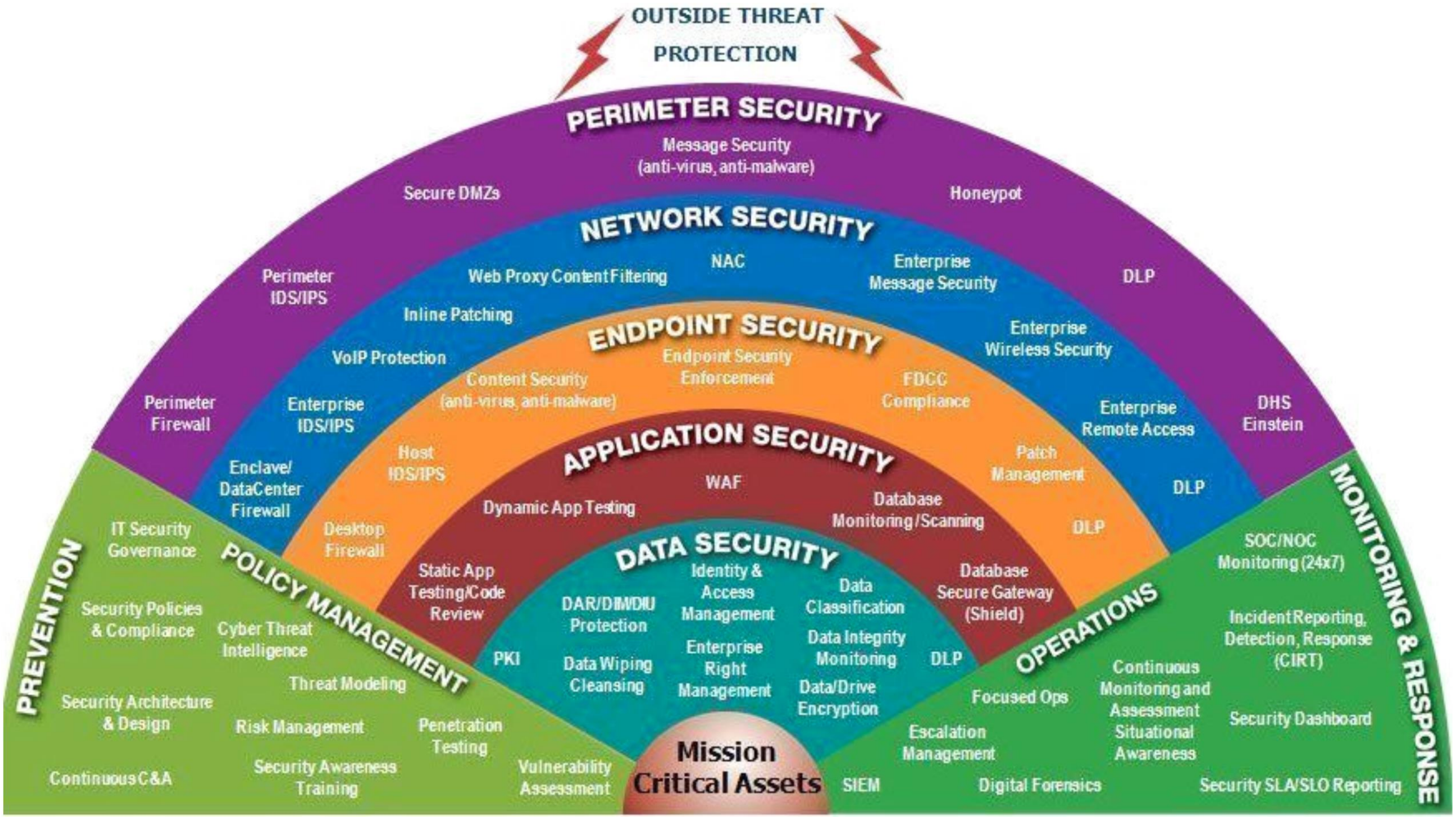
Why Is This Happening?



More Security Products = Better Security

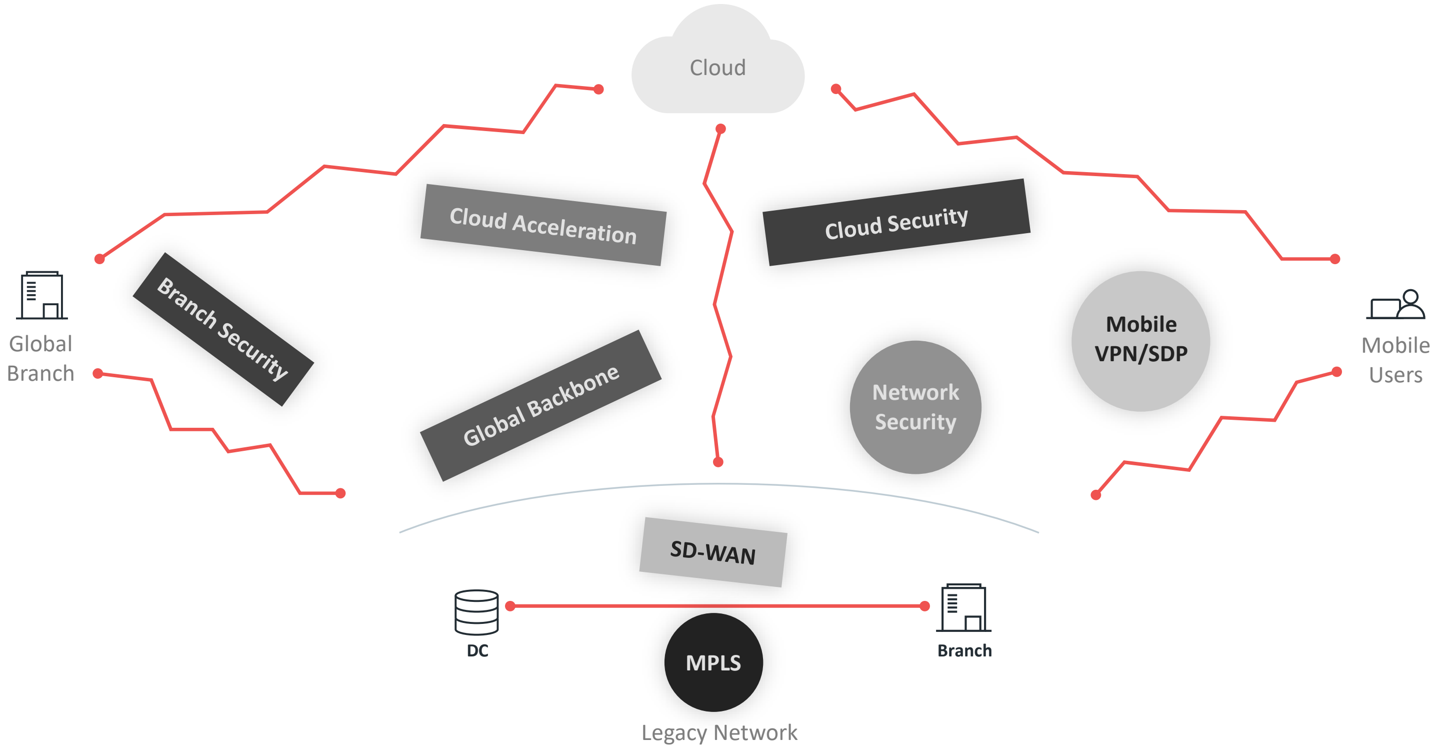
Myth II

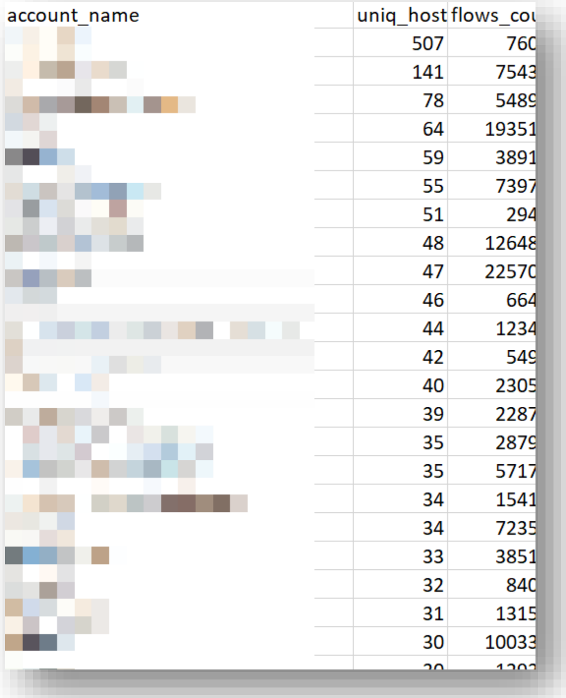
More Security Products Means Better Security



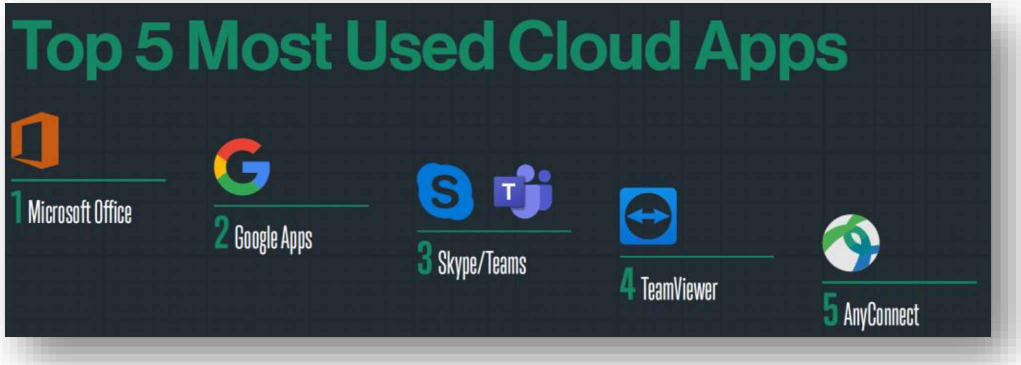
Source: Michael Fisher

So, What Are We Missing?





account_name	uniq_host	flows_cou
[redacted]	507	760
[redacted]	141	7543
[redacted]	78	5489
[redacted]	64	19351
[redacted]	59	3891
[redacted]	55	7397
[redacted]	51	294
[redacted]	48	12648
[redacted]	47	22570
[redacted]	46	664
[redacted]	44	1234
[redacted]	42	549
[redacted]	40	2305
[redacted]	39	2287
[redacted]	35	2879
[redacted]	35	5717
[redacted]	34	1541
[redacted]	34	7235
[redacted]	33	3851
[redacted]	32	840
[redacted]	31	1315
[redacted]	30	10033



Top 5 Most Used Cloud Apps

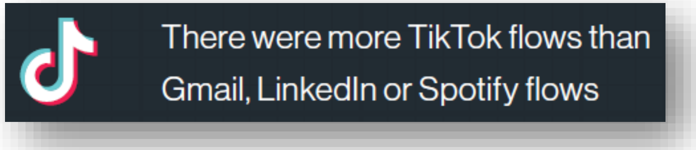
1 Microsoft Office

2 Google Apps

3 Skype/Teams

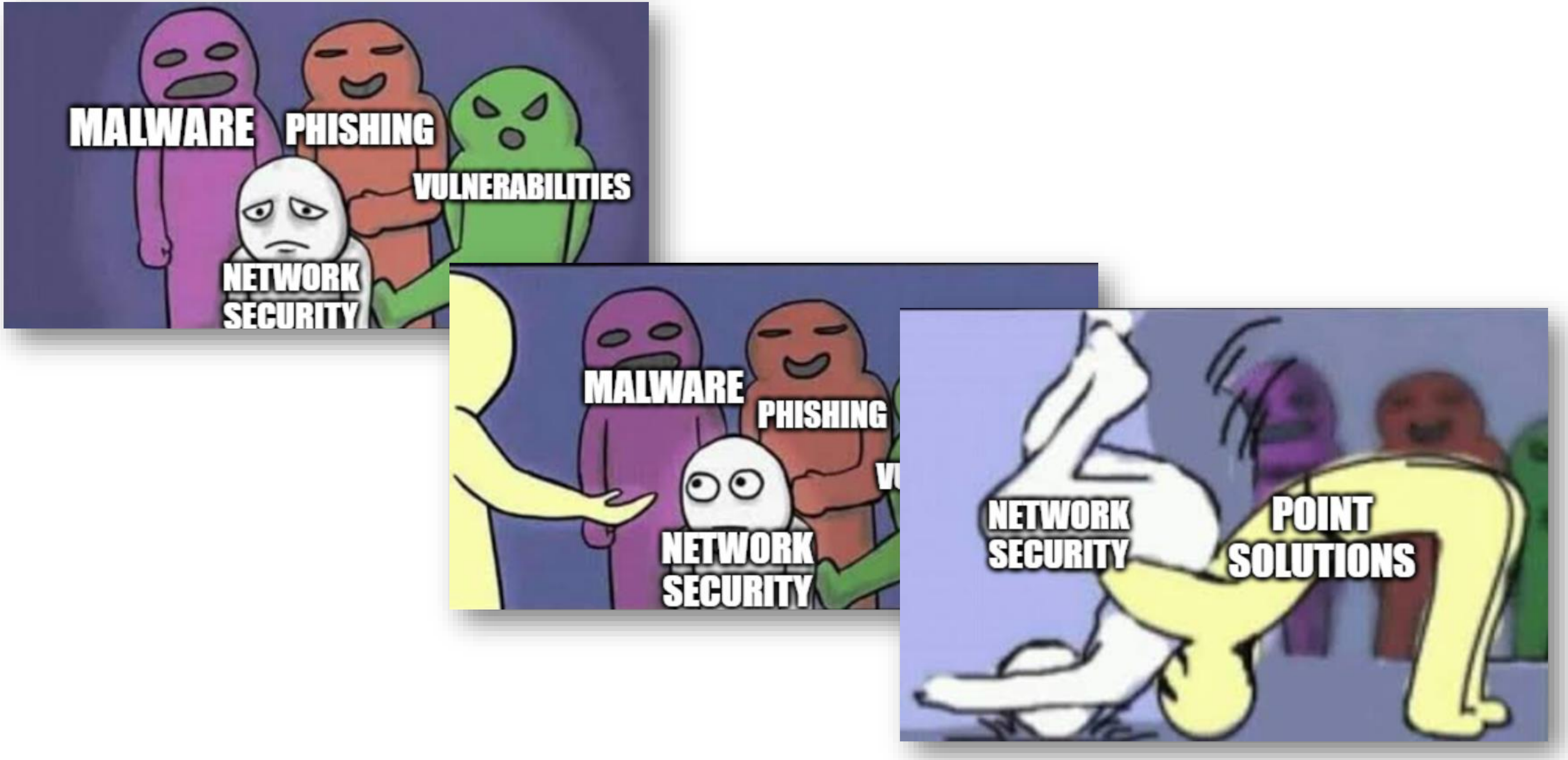
4 TeamViewer

5 AnyConnect



There were more TikTok flows than Gmail, LinkedIn or Spotify flows

Why Is This Happening?



Why Is This Happening?

I GOT TONS OF MALWARE SIGNATURES
YOU ARE NOT GOING TO JUST PREDICT THE PAST, RIGHT?
RIGHT???

Everything, Everywhere, Anytime

THE POLICY MUST FOLLOW THE USER

Ransomware Attack Stages

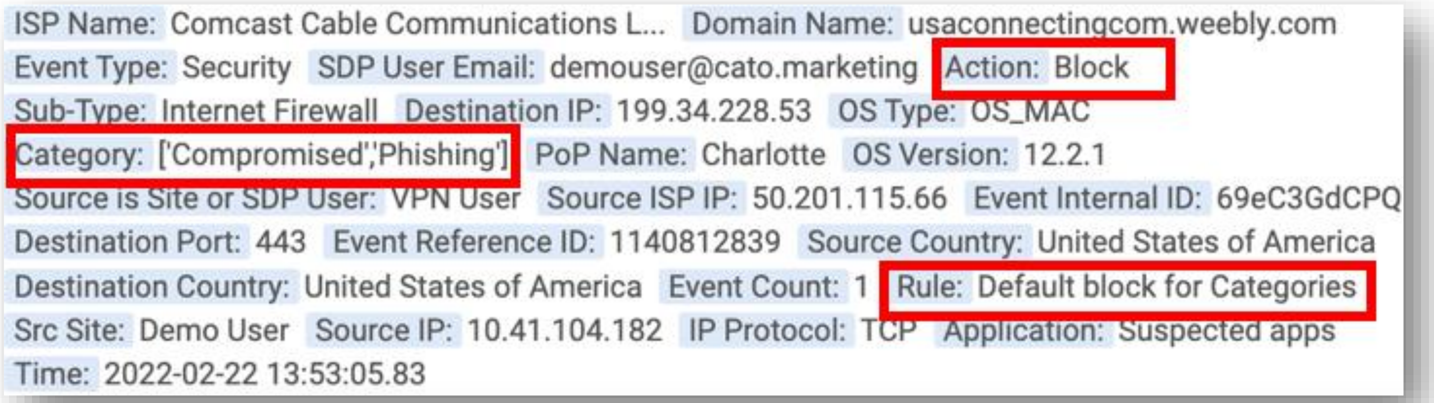
Case Study (and disclaimer)

- Phase 1 – Infiltration
  - Phishing
  - Connection to external site
  - Download of payload
- Phase 2 – Network activity
  - Admin password collection
  - In memory (fileless) malware
  - 2 Weeks of network lateral movement
  - SMB pushing encryption (guess when!?)
- Phase 3 – Exfiltration
  - Upload

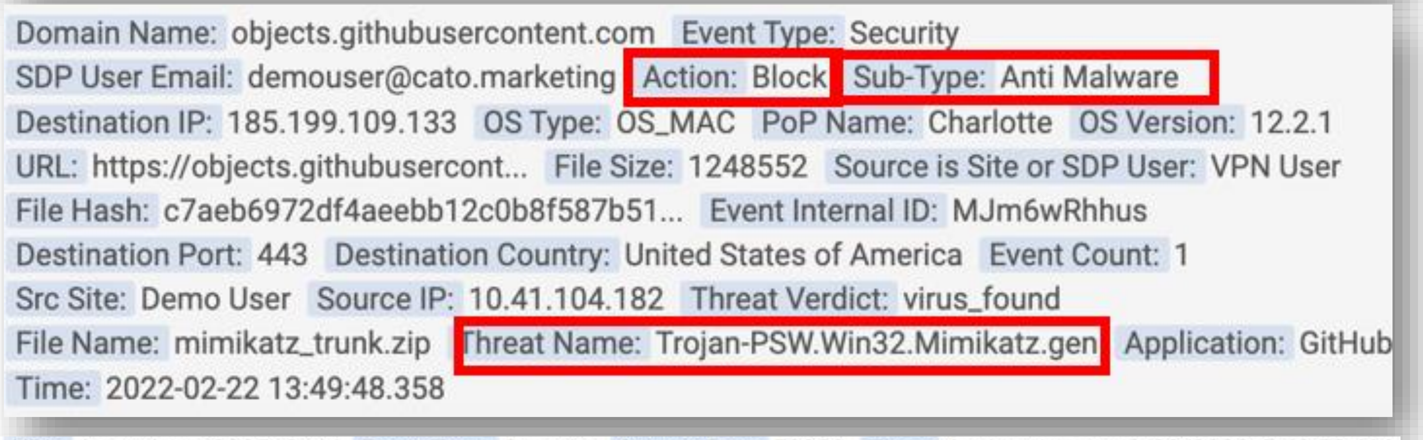
Ransomware Attack Stages

Choke Points

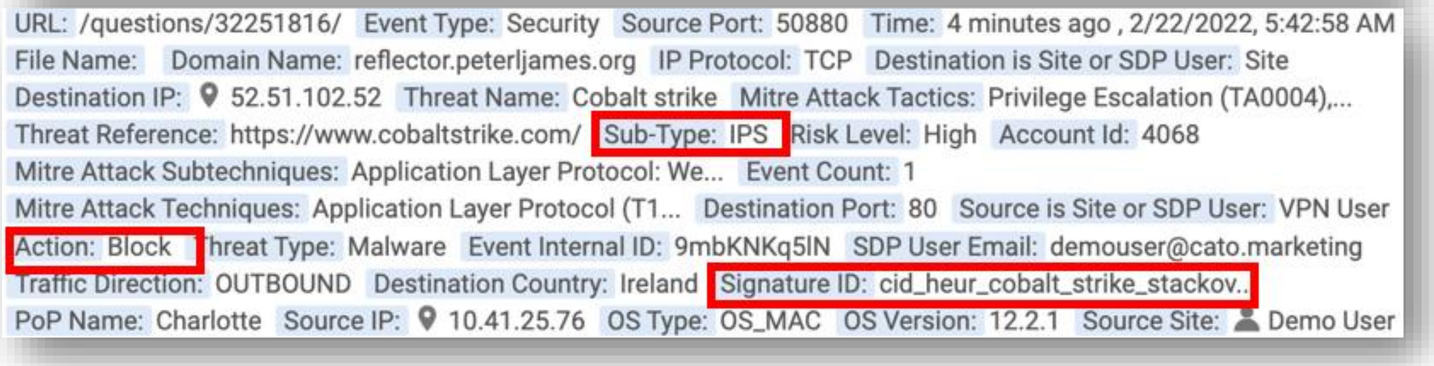
- Phase 1 – Infiltration
  - Phishing
  - Connection to external site
  - Download of payload
- Phase 2 – Network activity
  - Admin password collection
  - In memory (fileless) malware
  - 2 Weeks of network lateral movement
  - SMB pushing encryption (guess when!?)
- Phase 3 – Exfiltration
  - Upload



```
ISP Name: Comcast Cable Communications L...  Domain Name: usaconnectingcom.weebly.com
Event Type: Security  SDP User Email: demouser@cato.marketing  Action: Block
Sub-Type: Internet Firewall  Destination IP: 199.34.228.53  OS Type: OS_MAC
Category: ['Compromised','Phishing']  PoP Name: Charlotte  OS Version: 12.2.1
Source is Site or SDP User: VPN User  Source ISP IP: 50.201.115.66  Event Internal ID: 69eC3GdCPQ
Destination Port: 443  Event Reference ID: 1140812839  Source Country: United States of America
Destination Country: United States of America  Event Count: 1  Rule: Default block for Categories
Src Site: Demo User  Source IP: 10.41.104.182  IP Protocol: TCP  Application: Suspected apps
Time: 2022-02-22 13:53:05.83
```



```
Domain Name: objects.githubusercontent.com  Event Type: Security
SDP User Email: demouser@cato.marketing  Action: Block  Sub-Type: Anti Malware
Destination IP: 185.199.109.133  OS Type: OS_MAC  PoP Name: Charlotte  OS Version: 12.2.1
URL: https://objects.githubusercont...  File Size: 1248552  Source is Site or SDP User: VPN User
File Hash: c7aeb6972df4aeebb12c0b8f587b51...  Event Internal ID: MJm6wRhhus
Destination Port: 443  Destination Country: United States of America  Event Count: 1
Src Site: Demo User  Source IP: 10.41.104.182  Threat Verdict: virus_found
File Name: mimikatz_trunk.zip  Threat Name: Trojan-PSW.Win32.Mimikatz.gen  Application: GitHub
Time: 2022-02-22 13:49:48.358
```

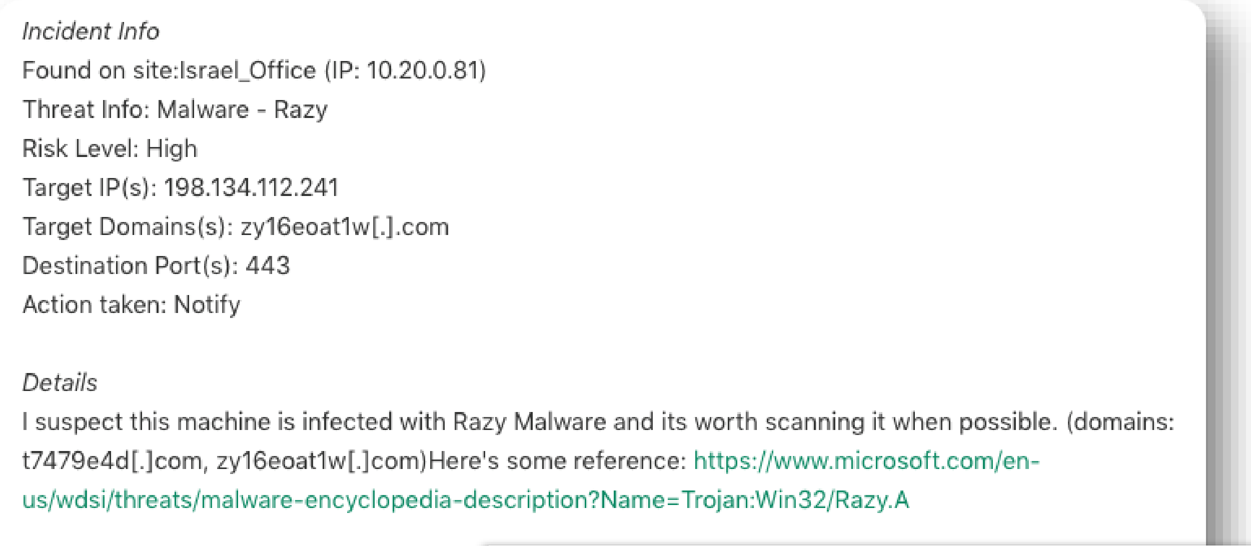


```
URL: /questions/32251816/  Event Type: Security  Source Port: 50880  Time: 4 minutes ago , 2/22/2022, 5:42:58 AM
File Name:  Domain Name: reflector.peterljames.org  IP Protocol: TCP  Destination is Site or SDP User: Site
Destination IP: 52.51.102.52  Threat Name: Cobalt strike  Mitre Attack Tactics: Privilege Escalation (TA0004),...
Threat Reference: https://www.cobaltstrike.com/  Sub-Type: IPS  Risk Level: High  Account Id: 4068
Mitre Attack Subtechniques: Application Layer Protocol: We...  Event Count: 1
Mitre Attack Techniques: Application Layer Protocol (T1...  Destination Port: 80  Source is Site or SDP User: VPN User
Action: Block  Threat Type: Malware  Event Internal ID: 9mbKNKq5lN  SDP User Email: demouser@cato.marketing
Traffic Direction: OUTBOUND  Destination Country: Ireland  Signature ID: cid_heur_cobalt_strike_stackov..
PoP Name: Charlotte  Source IP: 10.41.25.76  OS Type: OS_MAC  OS Version: 12.2.1  Source Site: Demo User
```

Ransomware Attack Stages

Choke Points

- Phase 1 – Infiltration
  - Phishing
  - Connection to external site
  - Download of payload
- Phase 2 – Network activity
  - Admin password collection
  - In memory (fileless) malware
  - 2 Weeks of network lateral movement
  - SMB pushing encryption (guess when!?)
- Phase 3 – Exfiltration
  - Upload



Incident Info

Found on site:Israel_Office (IP: 10.20.0.81)

Threat Info: Malware - Razy

Risk Level: High

Target IP(s): 198.134.112.241

Target Domains(s): zy16eoat1w[.].com

Destination Port(s): 443

Action taken: Notify

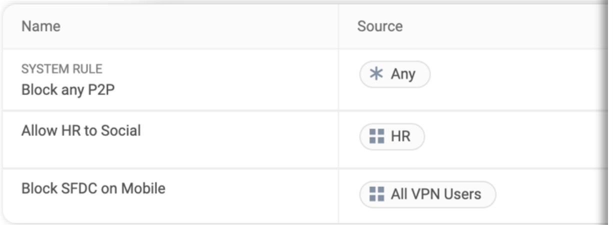
Details

I suspect this machine is infected with Razy Malware and its worth scanning it when possible. (domains: t7479e4d[.]com, zy16eoat1w[.]com)Here's some reference: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Razy.A

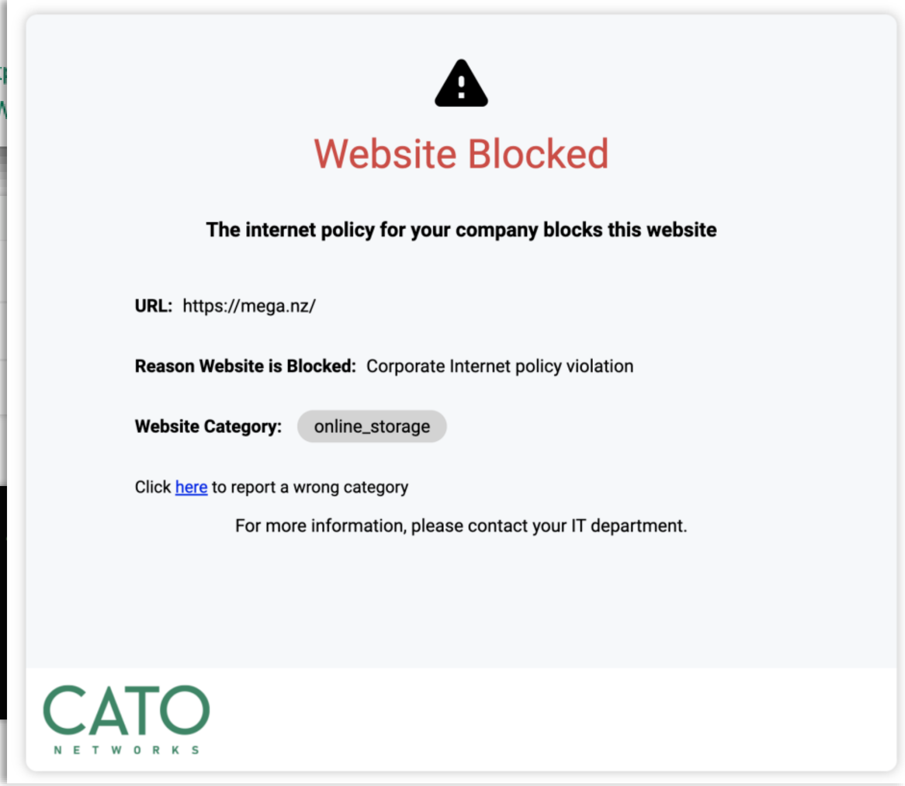
Recommended Action

Remove this threat using the following:htt

encyclopedia-description?Name=Trojan:W



Name	Source
SYSTEM RULE Block any P2P	✳ Any
Allow HR to Social	HR
Block SFDC on Mobile	All VPN Users



⚠

Website Blocked

The internet policy for your company blocks this website

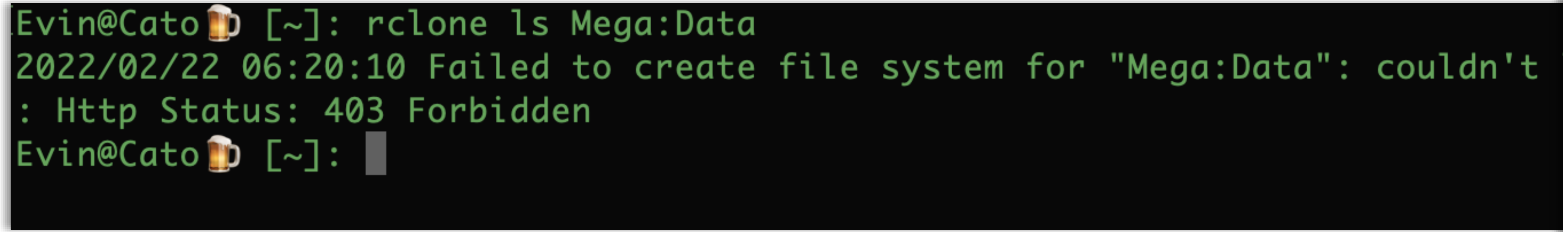
URL: https://mega.nz/

Reason Website is Blocked: Corporate Internet policy violation

Website Category: online_storage

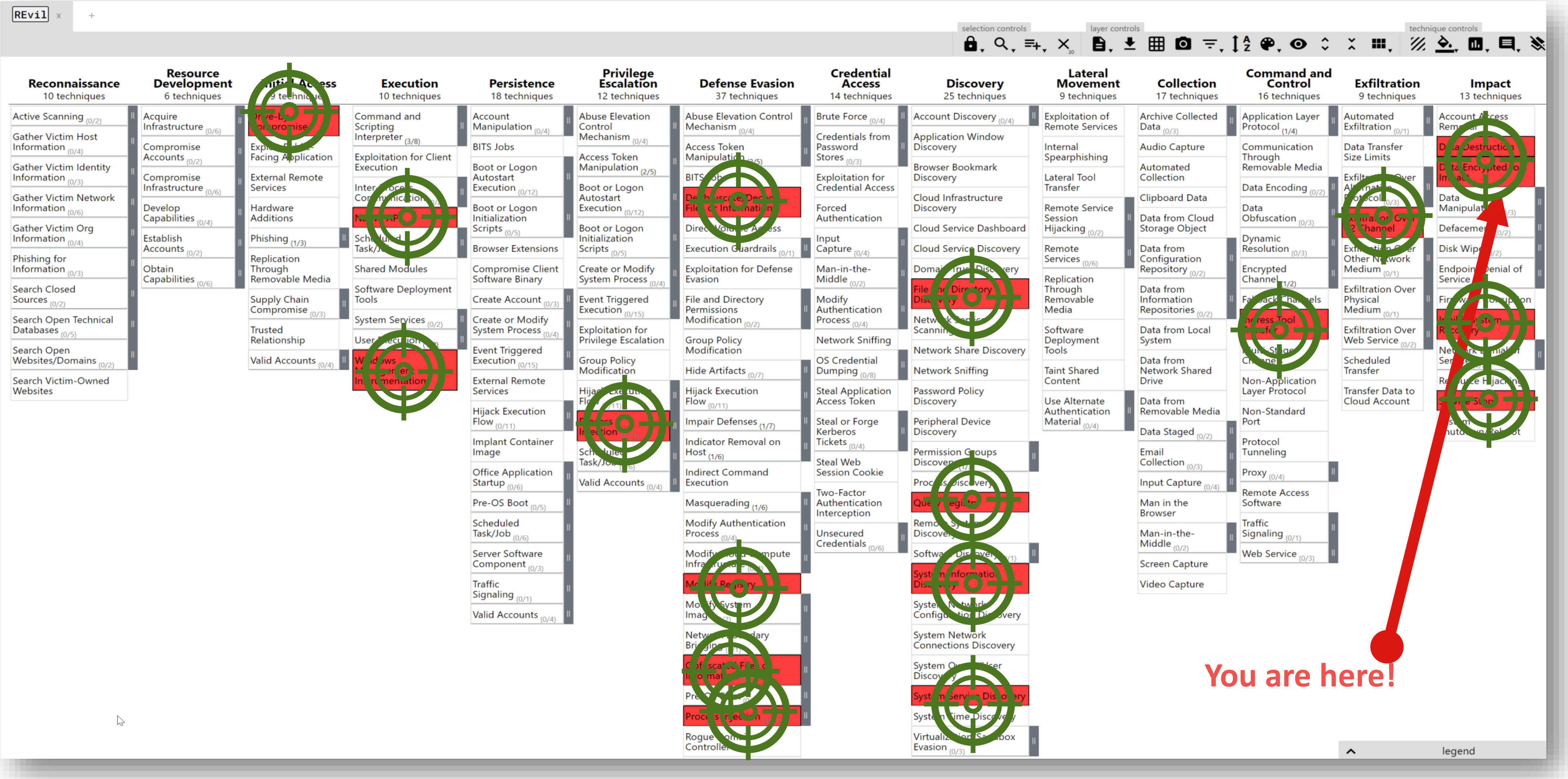
Click here to report a wrong category

For more information, please contact your IT department.



```
Evin@Cato🍺 [~]: rclone ls Mega:Data
2022/02/22 06:20:10 Failed to create file system for "Mega:Data": couldn't
: Http Status: 403 Forbidden
Evin@Cato🍺 [~]: █
```

Single Point of Failure VS Multiple Choke Points Approach



Reconnaissance 10 techniques
- Active Scanning (0/2)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/2)
- Search Victim-Owned Websites

Resource Development 6 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution 10 techniques
- Command and Scripting Interpreter (3/8)
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution
- Windows Management Instrumentation

Persistence 18 techniques
- Account Manipulation (0/4)
- BITS Jobs
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- External Remote Services
- Hijack Execution Flow (0/11)
- Implant Container Image
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/6)
- Server Software Component (0/3)
- Traffic Signaling (0/1)
- Valid Accounts (0/4)

Privilege Escalation 12 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (2/5)
- Boot or Logon Autostart Execution (0/12)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/15)
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow (0/11)
- Process Injection (0/11)
- Scheduled Task/Job (0/6)
- Valid Accounts (0/4)

Defense Evasion 37 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (2/5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Group Policy Modification
- Hide Artifacts (0/7)
- Hijack Execution Flow (0/11)
- Impair Defenses (1/7)
- Indicator Removal on Host (1/6)
- Indirect Command Execution
- Masquerading (1/6)
- Modify Authentication Process (0/4)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information
- Pre-OS Boot
- Process Injection
- Rogue Domain Controller

Credential Access 14 techniques
- Brute Force (0/4)
- Credentials from Password Stores (0/3)
- Exploitation for Credential Access
- Forced Authentication
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify Authentication Process (0/4)
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (0/6)

Discovery 25 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (1/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection 17 techniques
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Man in the Browser
- Man-in-the-Middle (0/2)
- Screen Capture
- Video Capture

Command and Control 16 techniques
- Application Layer Protocol (1/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (1/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration 9 techniques
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

You are here!

CATO NETWORKS

A Converged Solution

Policy

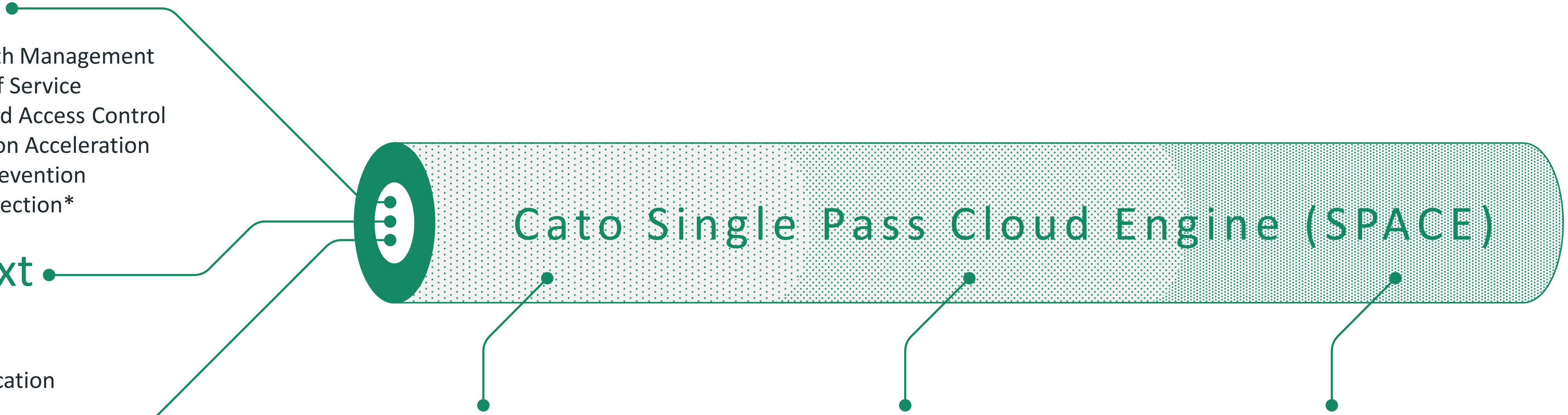
- Bandwidth Management
- Quality of Service
- Risk-based Access Control
- Application Acceleration
- Threat Prevention
- Data Protection*

Context

- Account
- Device
- Authentication
- Identity
- Network
- Application
- Data

Flows

- Branches
- Users
- Applications
- Clouds
- Systems
- IoT



Cato Single Pass Cloud Engine (SPACE)

Access

- Zero Trust Network Access
- Single Sign-On
- Multi Factor Authentication
- Risk-Based Application Access

Network

- Traffic shaping
- Global Route Optimization
- WAN & SaaS Acceleration
- Multi-Cloud Networking

Security

- Next Generation Firewall
- Secure Web Gateway
- Next Generation Anti Malware
- Intrusion Prevention System
- Cloud Access Security Broker*
- Data Loss Prevention*
- Remote Browser Isolation*

Bonus Myth – Attackers Use Their Own Servers

Aka – LOL? LOC!

CATO NETWORKS

The Network for Whatever's Next

Thank You!