RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-M06**

Network Based Threat Hunting: Lessons Learned, Techniques to Share

Tal Darsan

Manager, Managed Cybersecurity Services
Cato Networks

Etay Maor

Sr Director Security Strategy
Cato Networks

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

Agenda & Intro

Agenda

- Quick Intro
- Case Studies
  - Phishing + demo
  - Malware deep dive
  - Ransomware + live demo
- Take-aways

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 Lineage

unpatched

LineageOS source code, O

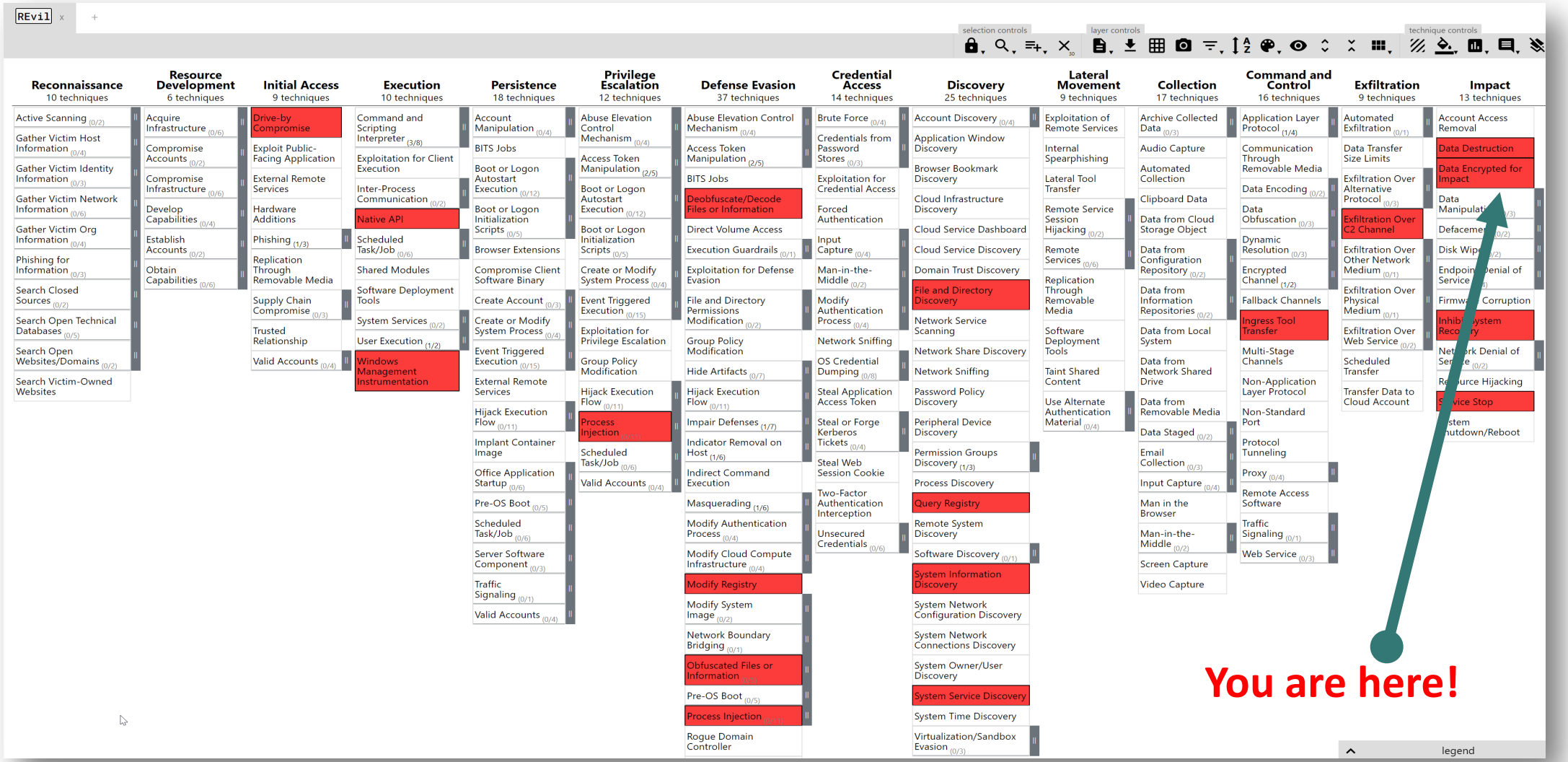
A hacker stole more than $55 million in crypto after a bZx developer fell for a phishing attack

Kevin Shalvey Nov 7, 2021, 5:10 AM

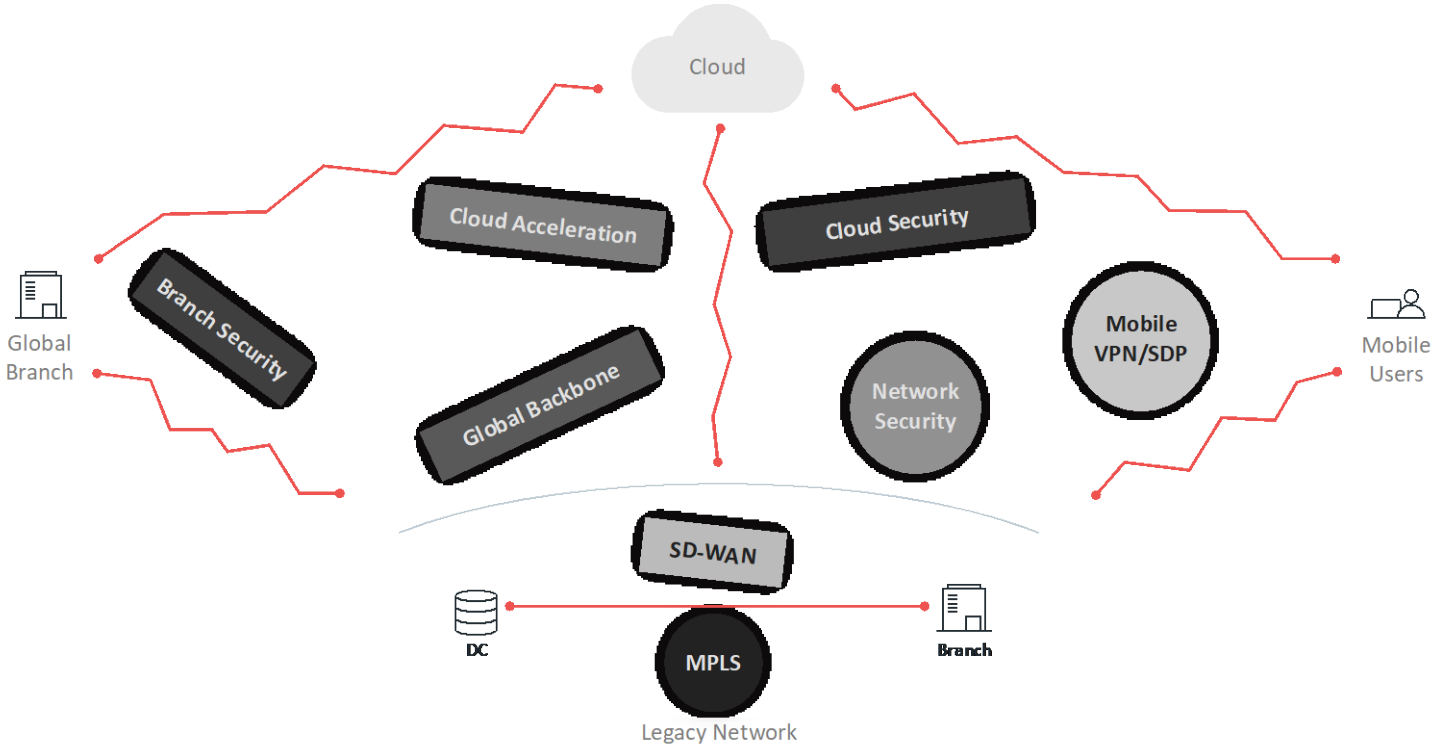
SQL injection flaw in billing software app tied to US ransomware infection

John Leyden 26 October 2021 at 14:54 UTC
Updated: 26 October 2021 at 15:26 UTC

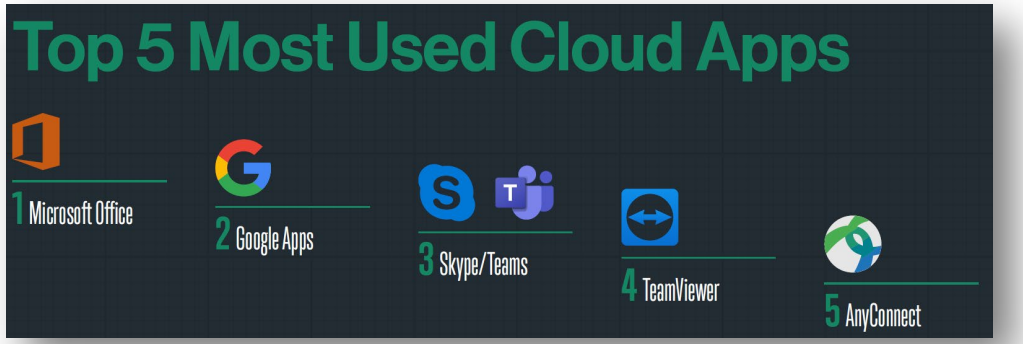
The Attacker Needs To Be Right Just Once, The Defenders Need To Be Right All The Time?



So, What Are We Missing?



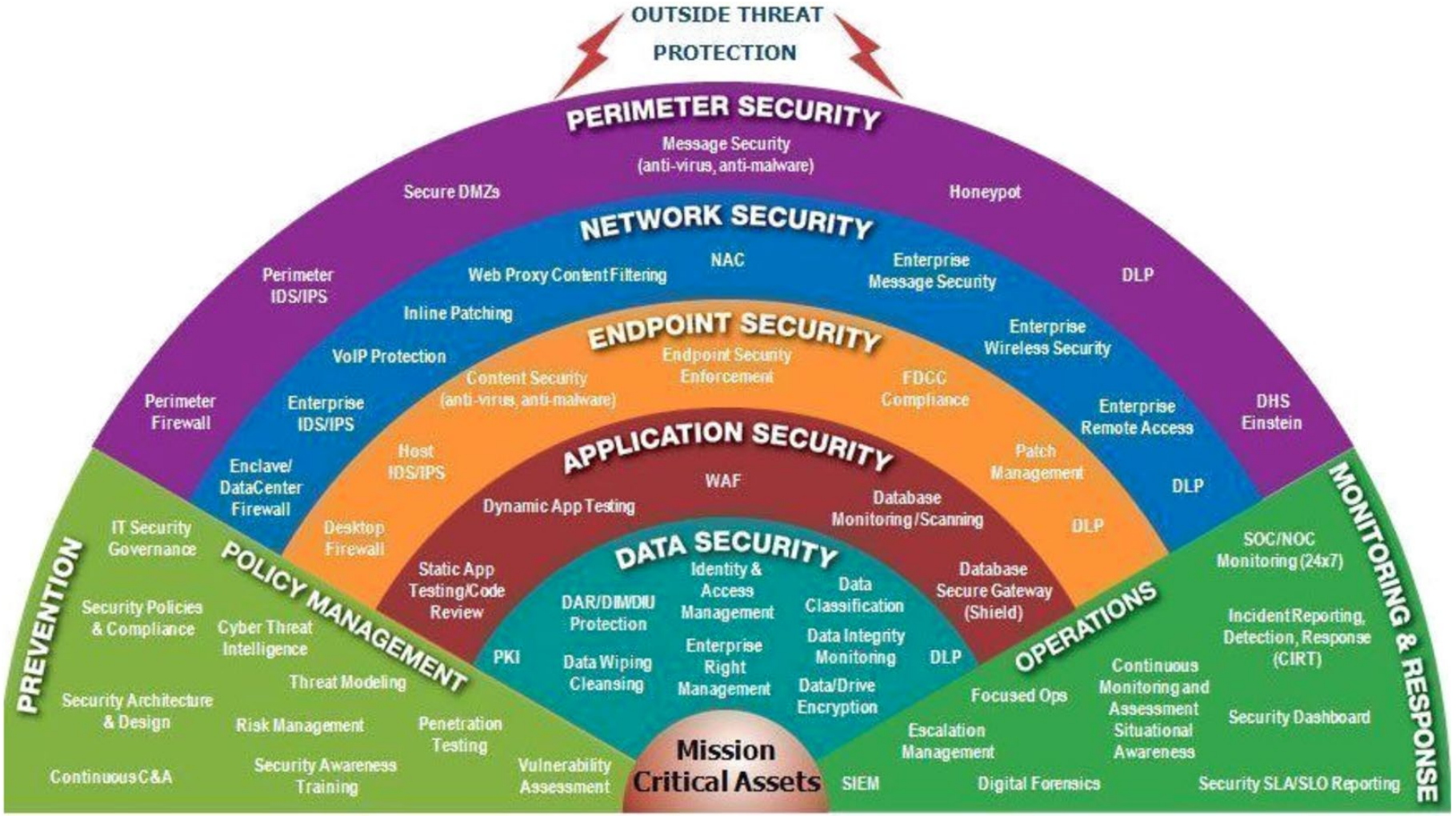
account_name	uniq_host	flows_cou
	507	760
	141	7543
	78	5489
	64	19351
	59	3891
	55	7397
	51	294
	48	12648
	47	22570
	46	664
	44	1234
	42	549
	40	2305
	39	2287
	35	2879
	35	5717
	34	1541
	34	7235
	33	3851
	32	840
	31	1315
	30	10033



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

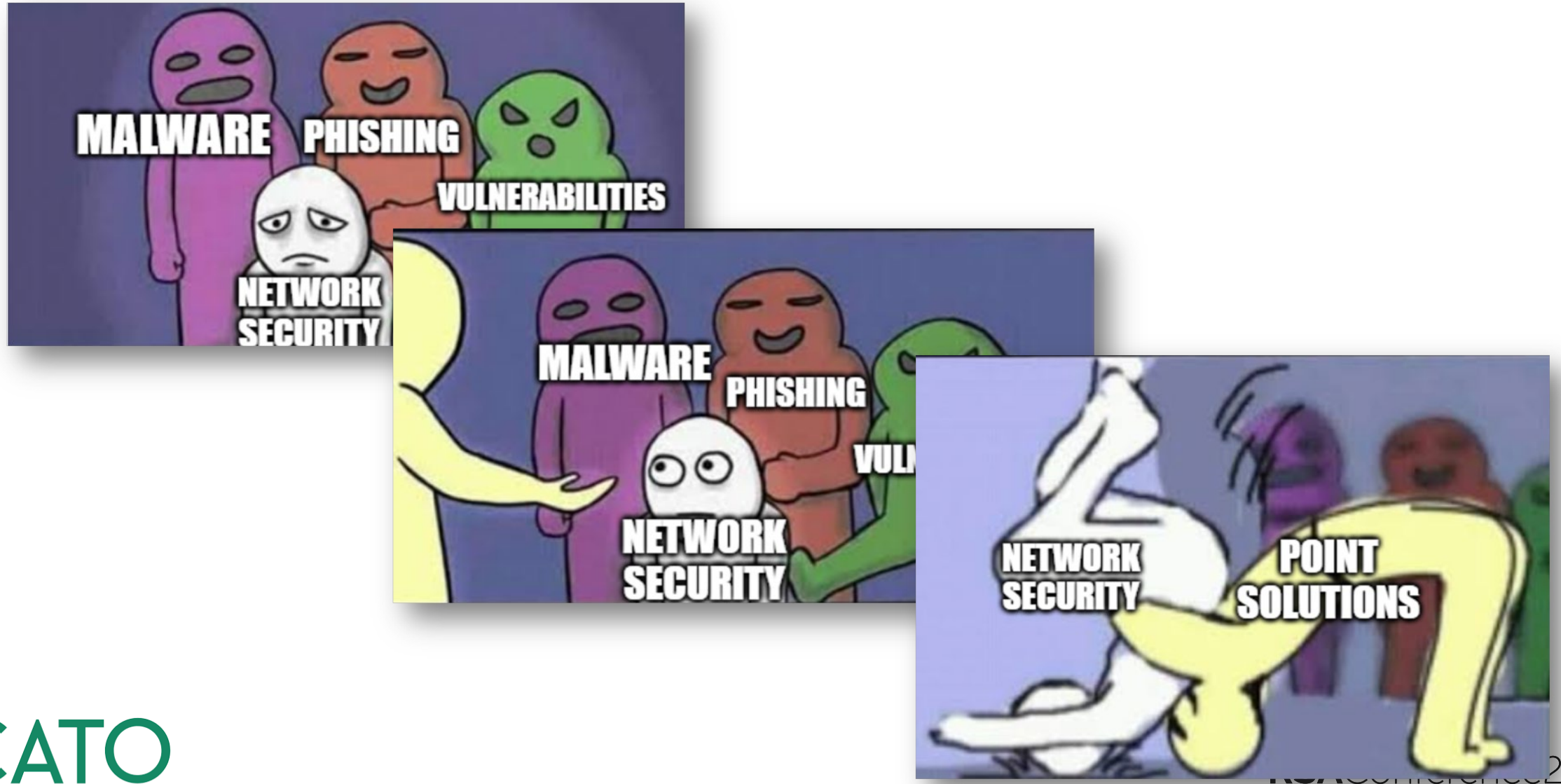
CATO NETWORKS

More Point Solutions Means Better Security (?)



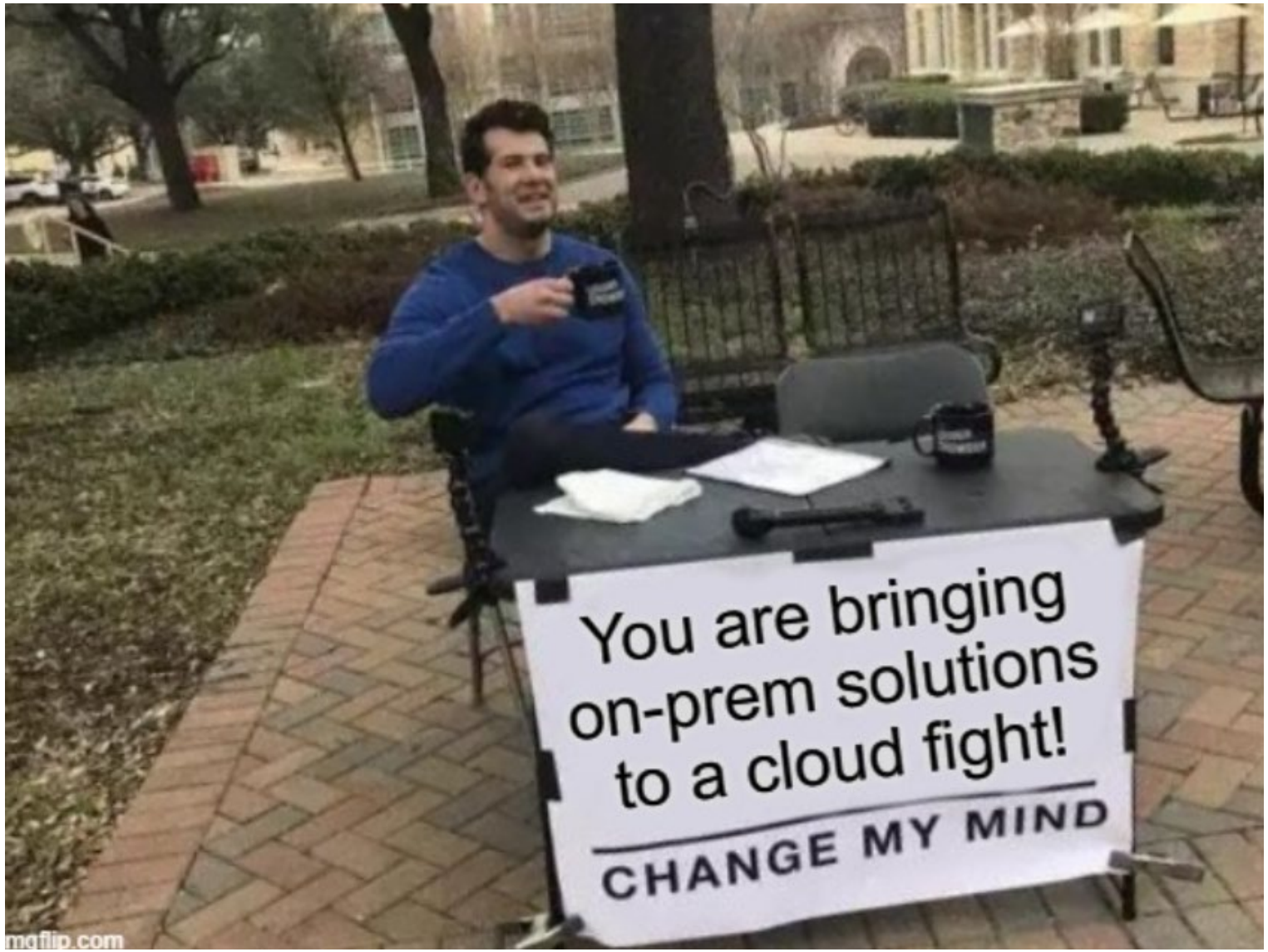
Source: Michael Fisher

Did We Add Fat Or Muscle?



CATO NETWORKS

Why Is This Happening?



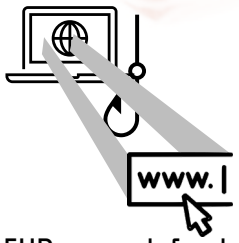
RSAConference2022

Case Study 1

Phishing

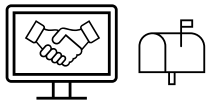
Office365 Phishing Attack Chain

Targeted Phishing Attack launched

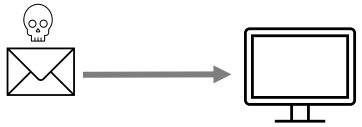


FUD in intel. feeds

Attacker compromises partner's mailbox



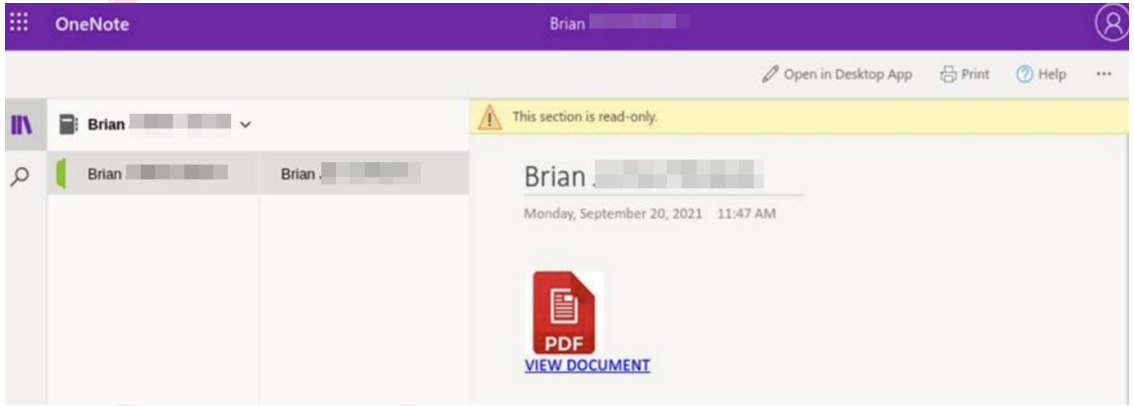
Phishing email sent



compromised "OneNote", "ClickUp", and "Glitch" web services

ClickUp

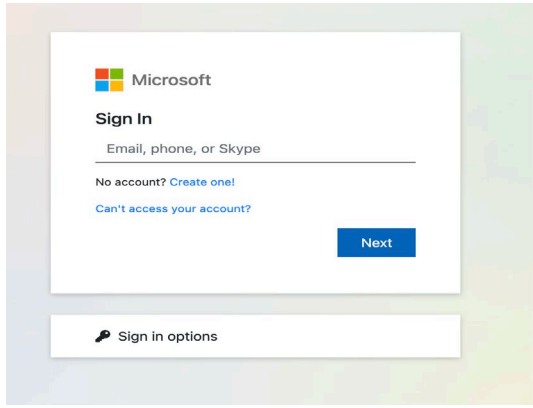
Glitch



How this can be hunted?

Submission of data into a potential risky Web forms

ML models trained on different page elements



CATO NETWORKS

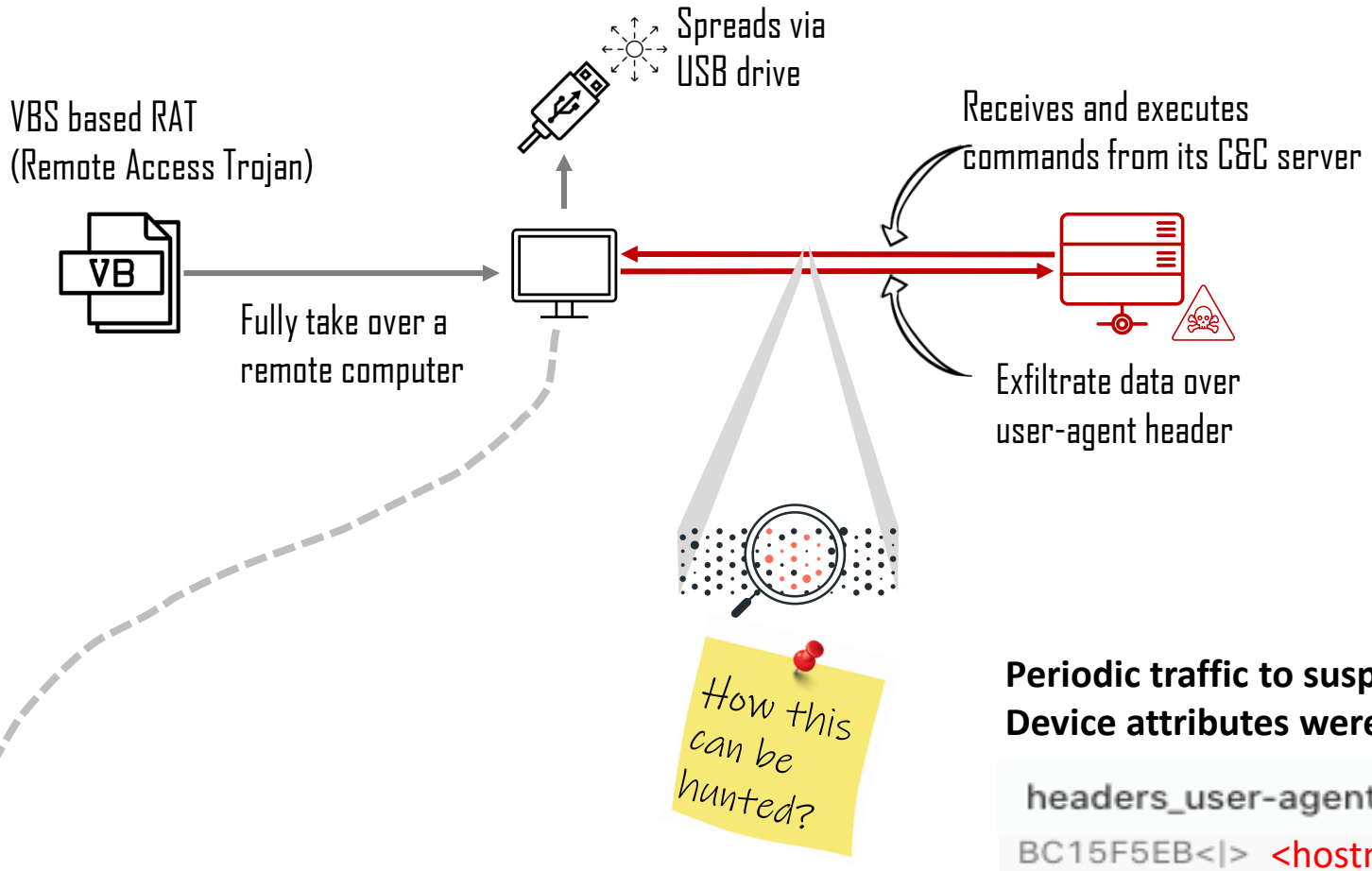
RSAConference2022

RSAConference2022

Case Study 2

Malware

Houdini Remote Access Trojan (RAT)



Periodic traffic to suspicious domains
Device attributes were found in the HTTP user-agent header

headers_user-agent

BC15F5EB<|> <hostname> <|> <username> <|>Microsoft Windows 10 Enterprise<|>plus<|>Windows Defender .Trend Micro OfficeScan Antivirus .<|>false - 4/21/2021

Threat dwell-time lasted for days

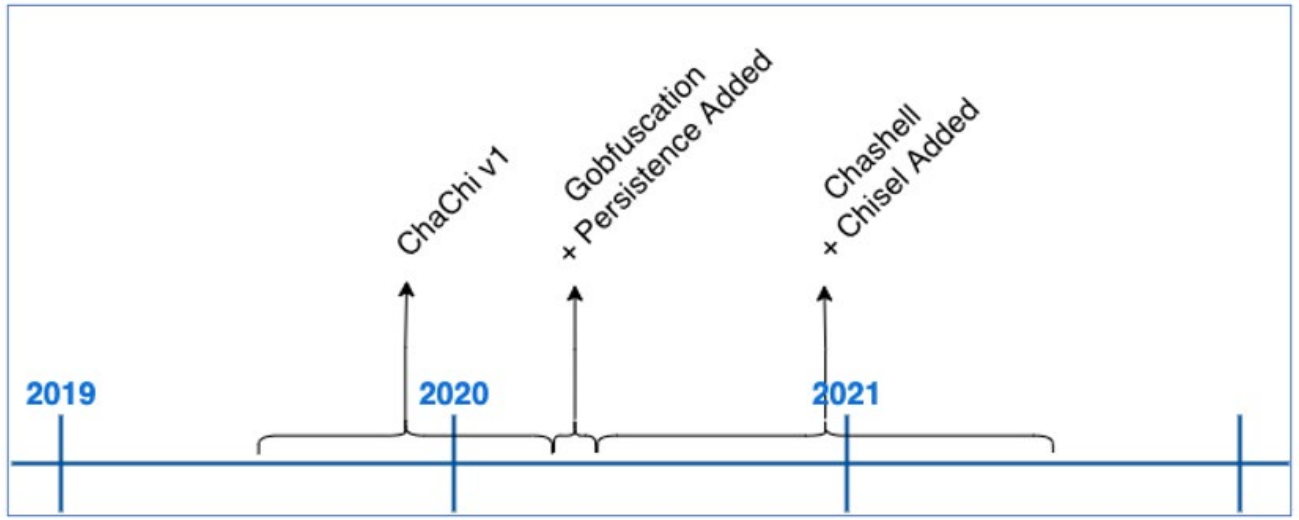
Existing external NGAV didn't detect it

CATO NETWORKS

ChaChi Backdoor

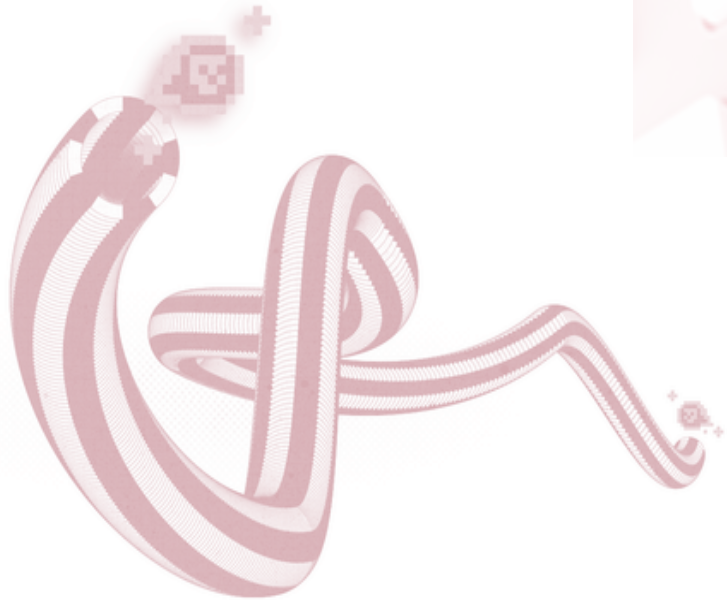
Characteristics:

- Golang based backdoor, first observed in 2019
- Cross Platform
- Stealing device attributes
- Data exfiltration via DNS Tunneling/Fallback over HTTP
- Dropping PYSA Ransomware



ChaChi Backdoor – DNS Tunneling

For attackers, DNS tunneling provides a convenient way to exfiltrate data and to gain access to a network because DNS communications are often unblocked



How this can be hunted?

DNS record detection heuristics
ML models trained on DNS traffic/Domain squatting

6a64ede5bafc055ef8f118a3d5f94fc9897a189afc775f.1b9ef0996b94e369c0651ee934f3694f9318a93efdca8c932.oneidrive.org
51a551 205145beb3177169fe86a1eefe62b3fb0e45ed8a9755d60.3dcba07923f02337fb89ee97d62a4998ca079d13fa3fea82f.oneidrive.org
7abc01ffd56051eb0284607965e6ebbca37ecc2ac0147de2d77a2d067929db9.65c1a03863c7b915956d0af9ce5fb690ed9b2d0f79f5194dc.oneidrive.org
223330ca7b72cf2e5d54a518799ee3e7fdceb9aadebefa2a635f12e3ebea7fe.8a87c158b4dd45102278cc057b4e4c3e563afa9c71b8fba69.oneidrive.org
d3d782237da10971557de0d2ca3526018d6d9a9f7b73c093927baab626c6d98.1233cfc303528c3f48700348f15b15cf2995c7026b7fde77d.oneidrive.org
8005e8eeb92f4019c617fa3d0668589b779ec217960ce206d9f01278dddc8bc.eeb62fad948dcf19a2941ade601a231cf76770211e536c36f.oneidrive.org
f1a945efa8a4d9316e84b6ecb0a8511838bc91f436733eec6fd5fc1cbaeee6f.032ab1d1de9703b9657f5eb81f8b6178dfd48e0866e8e8002.oneidrive.org
f1a945efa8a4d9316e84b6ecb0a8511838bc91f436733eec6fd5fc1cbaeee6f.032ab1d1de9703b9657f5eb81f8b6178dfd48e0866e8e8002.oneidrive.org
4629e521dfa188f99661dc2b6e29e29802025ba5258138f80a6e2d3fb927bfb.0a96e890f0a2de58f21f95ac0ae9d72dfa2aff248d7f97dba.oneidrive.org
4629e521dfa188f99661dc2b6e29e29802025ba5258138f80a6e2d3fb927bfb.0a96e890f0a2de58f21f95ac0ae9d72dfa2aff248d7f97dba.oneidrive.org
022654b8b4328e9840d1dcaaf6d8f4e6437e4e08414aca69d1d0141a83b0339.954de55fa46814aeda8ec84f7f956ba49574362b45b3db4e1.oneidrive.org
022654b8b4328e9840d1dcaaf6d8f4e6437e4e08414aca69d1d0141a83b0339.954de55fa46814aeda8ec84f7f956ba49574362b45b3db4e1.oneidrive.org
851578cd5e2e523dde1aa0e52316b7ce4d4bb45b0c7f7a2f47f5db3afd8246c.b9b381a562915097ce052f80e19e7c2bdb6698fff4e09cbf0.oneidrive.org
c631349ba014c7e4eab1fd16a671fe11b23252786ea9b653a028ec52f08b3bc.3fa734edc72e23ed91e04a151c90087a02dd080c4be02bd42.oneidrive.org
f1a945efa8a4d9316e84b6ecb0a8511838bc91f436733eec6fd5fc1cbaeee6f.032ab1d1de9703b9657f5eb81f8b6178dfd48e0866e8e8002.oneidrive.org
022654b8b4328e9840d1dcaaf6d8f4e6437e4e08414aca69d1d0141a83b0339.954de55fa46814aeda8ec84f7f956ba49574362b45b3db4e1.oneidrive.org
4629e521dfa188f99661dc2b6e29e29802025ba5258138f80a6e2d3fb927bfb.0a96e890f0a2de58f21f95ac0ae9d72dfa2aff248d7f97dba.oneidrive.org
9a0fb80809edea3fc4a7c5eea23cdf15300f7f1496f1032dd6f1997ce4a7640.56df3f45a9cbe8f9b78290bb17729e26aa5a70a8a91008cb6.oneidrive.org
e7311d00c62dbfc740fb5ae8005dc96ef5a3273edb671af93472b2e4bf76d2b.51416997fc8cdd335b917c1ac45d82e0a698bfcb21b1b2462.oneidrive.org
e7311d00c62dbfc740fb5ae8005dc96ef5a3273edb671af93472b2e4bf76d2b.51416997fc8cdd335b917c1ac45d82e0a698bfcb21b1b2462.oneidrive.org
55fbd0837d3f5d4448fb80700723093836e240dbe5e18363356e0094d859698.997a714a260283f24c0bc15e64433a2f6afdef2299c16126e.oneidrive.org
1991594e76aff5c4d0f631e37d18083a2a61f7fdd4addf6e71087a63075e43a.5d63fcf0094e14d4ab8f70b19dc8fa3cec7ab3b486fa37265.oneidrive.org
e7311d00c62dbfc740fb5ae8005dc96ef5a3273edb671af93472b2e4bf76d2b.51416997fc8cdd335b917c1ac45d82e0a698bfcb21b1b2462.oneidrive.org
337fbb396f9b4a0abfa4bb2290e1d967b06c473119fe15ca765b5f25d27a250.3055bc02ebdcf2f03633e8dddf811e878d09fcde05d4b1e66.oneidrive.org
337fbb396f9b4a0abfa4bb2290e1d967b06c473119fe15ca765b5f25d27a250.3055bc02ebdcf2f03633e8dddf811e878d09fcde05d4b1e66.oneidrive.org
5a9412e057bcf0462a0b06091793bda98baed8161ba89ebd0c146f53df54b72.bf0fe4601c6e4d022c8043507b2d67452a9616914dc971fc4.oneidrive.org
5a9412e057bcf0462a0b06091793bda98baed8161ba89ebd0c146f53df54b72.bf0fe4601c6e4d022c8043507b2d67452a9616914dc971fc4.oneidrive.org
015b00492ecf03039b91644731de9e2a2c77a97f1cbf7b9cc476249ec57a5f7.8e96b31d3a59f404e36e4741aee23ab3a50ba4b35b1099b5b.oneidrive.org
015b00492ecf03039b91644731de9e2a2c77a97f1cbf7b9cc476249ec57a5f7.8e96b31d3a59f404e36e4741aee23ab3a50ba4b35b1099b5b.oneidrive.org
337fbb396f9b4a0abfa4bb2290e1d967b06c473119fe15ca765b5f25d27a250.3055bc02ebdcf2f03633e8dddf811e878d09fcde05d4b1e66.oneidrive.org
023b5a4e70a2d3f627047a9a93f67f68cf29f892be6195165e2e6f7788935cc.5a02661529217659a5c0b755058fc02317ac99f9870d018ab.oneidrive.org
5a9412e057bcf0462a0b06091793bda98baed8161ba89ebd0c146f53df54b72.bf0fe4601c6e4d022c8043507b2d67452a9616914dc971fc4.oneidrive.org
015b00492ecf03039b91644731de9e2a2c77a97f1cbf7b9cc476249ec57a5f7.8e96b31d3a59f404e36e4741aee23ab3a50ba4b35b1099b5b.oneidrive.org

CATO NETWORKS

RSAConference2022

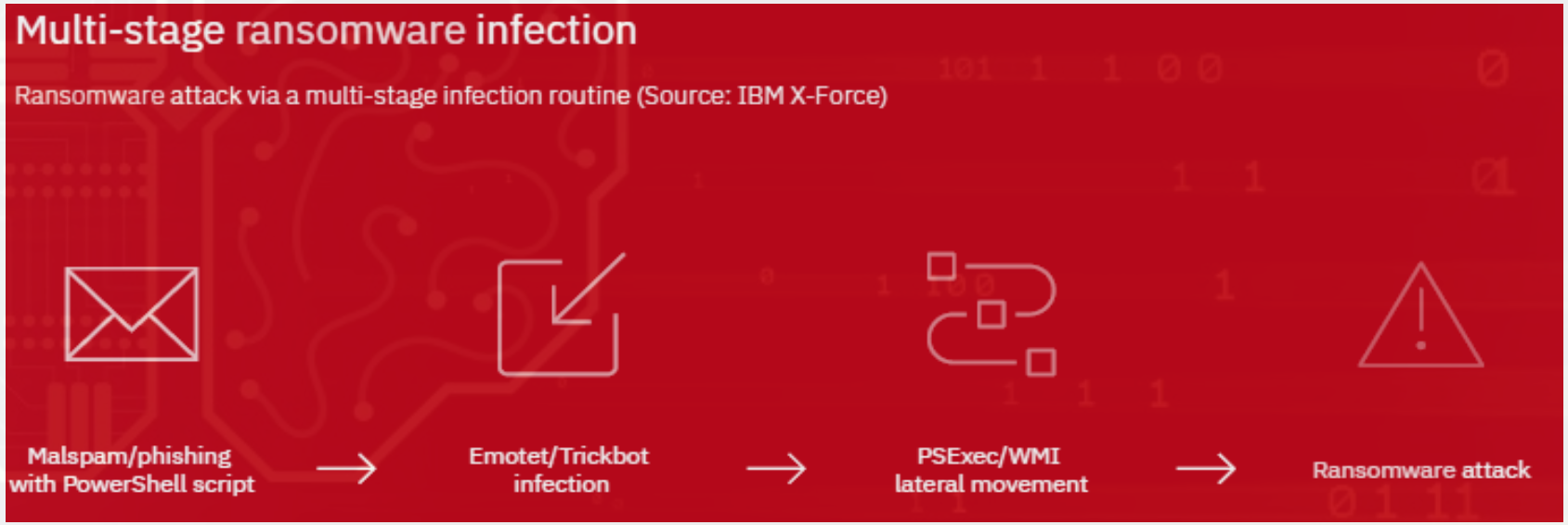
Case Study 3

Ransomware

Ransomware Propagation and Encryption

Characteristics:

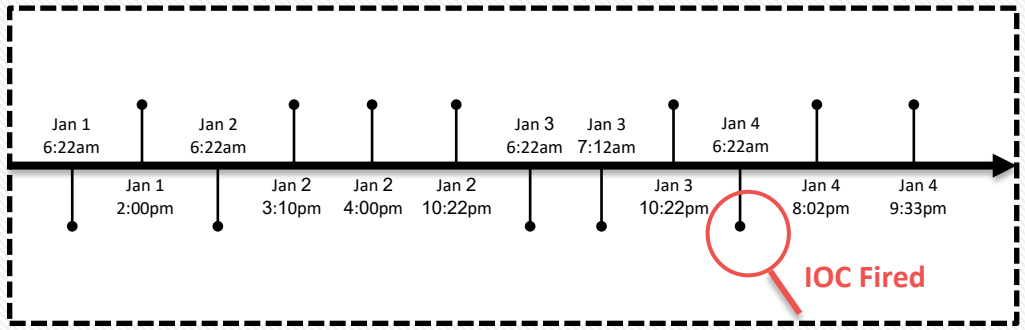
- Ransomware typically encrypts files and renames them too, **usually by changing their file extension**
- Ransomware determines what data to encrypt by iterating through files on local systems and **SMB network shares**

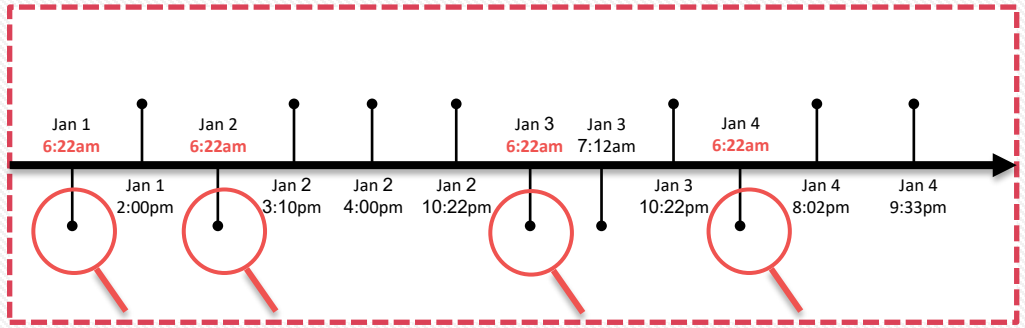


RSAConference2022

Summary

Combating cyber threats using AI & ML





100TB Daily

Raw Flows

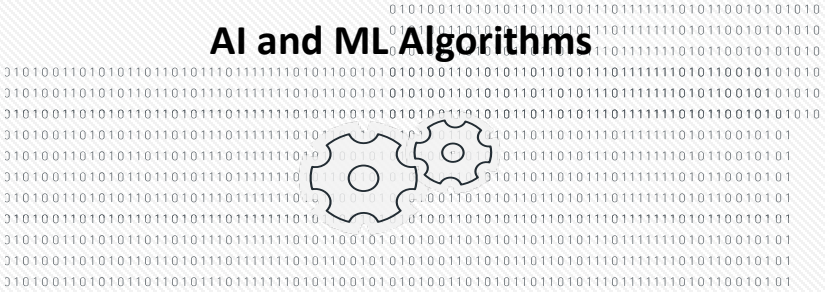
Rich Flow Context

Src IP | Application | Dest IP | Protocol | Target | OS | URI | URL

TLS signature | DNS resolving | Client type | User agent | DGA | Port

Request body | HTTP header | Header order | First packet

AI and ML Algorithms



~20 Flows

For verification, containment, and communication

CATO NETWORKS

Malware Network Activity

4DD551A2A853C411E005795FA63CE640.online

4E4ECDE4BD35A25A212C438F7CFE55B9.online

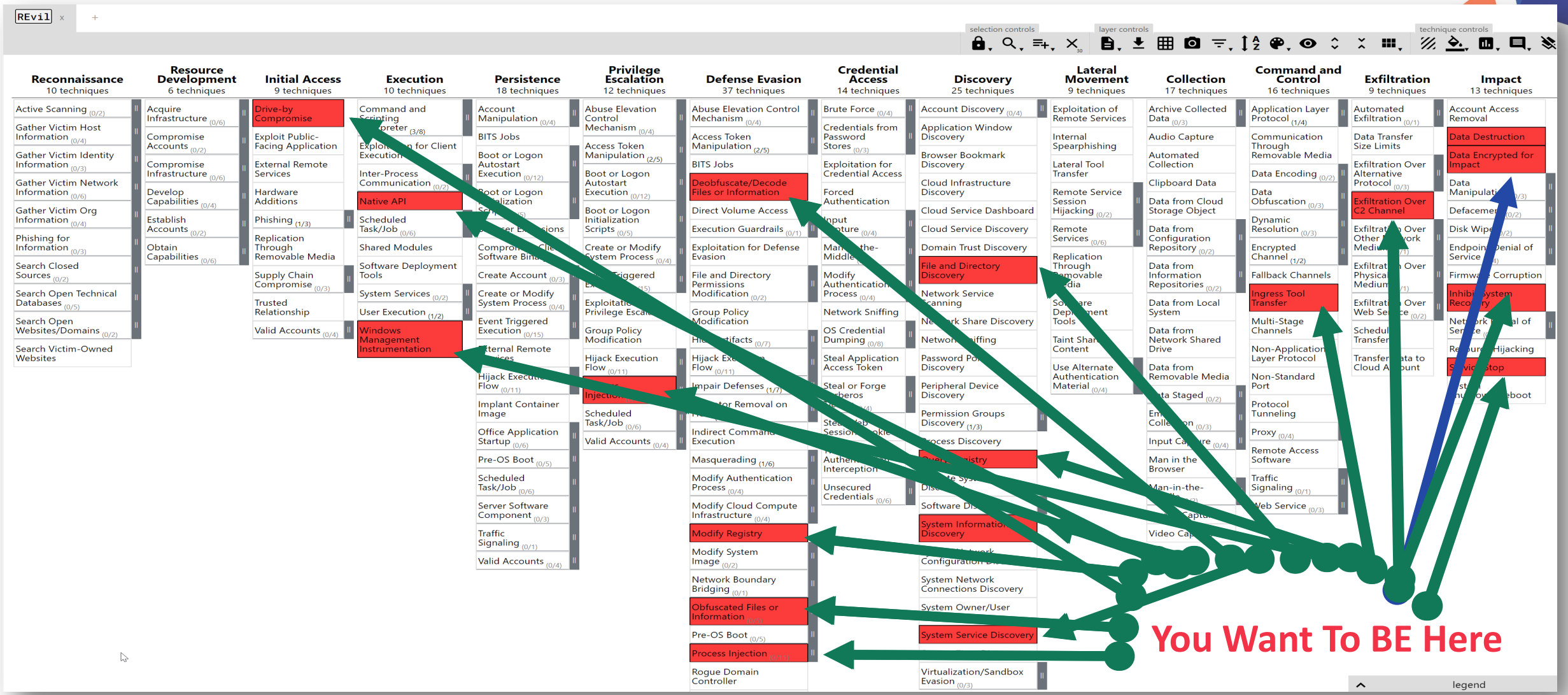
A9D5F0F6FF1E417FD0F26A42405A6F5E.online

DEF651313D9BBF292A6C6484E3F076CF.online

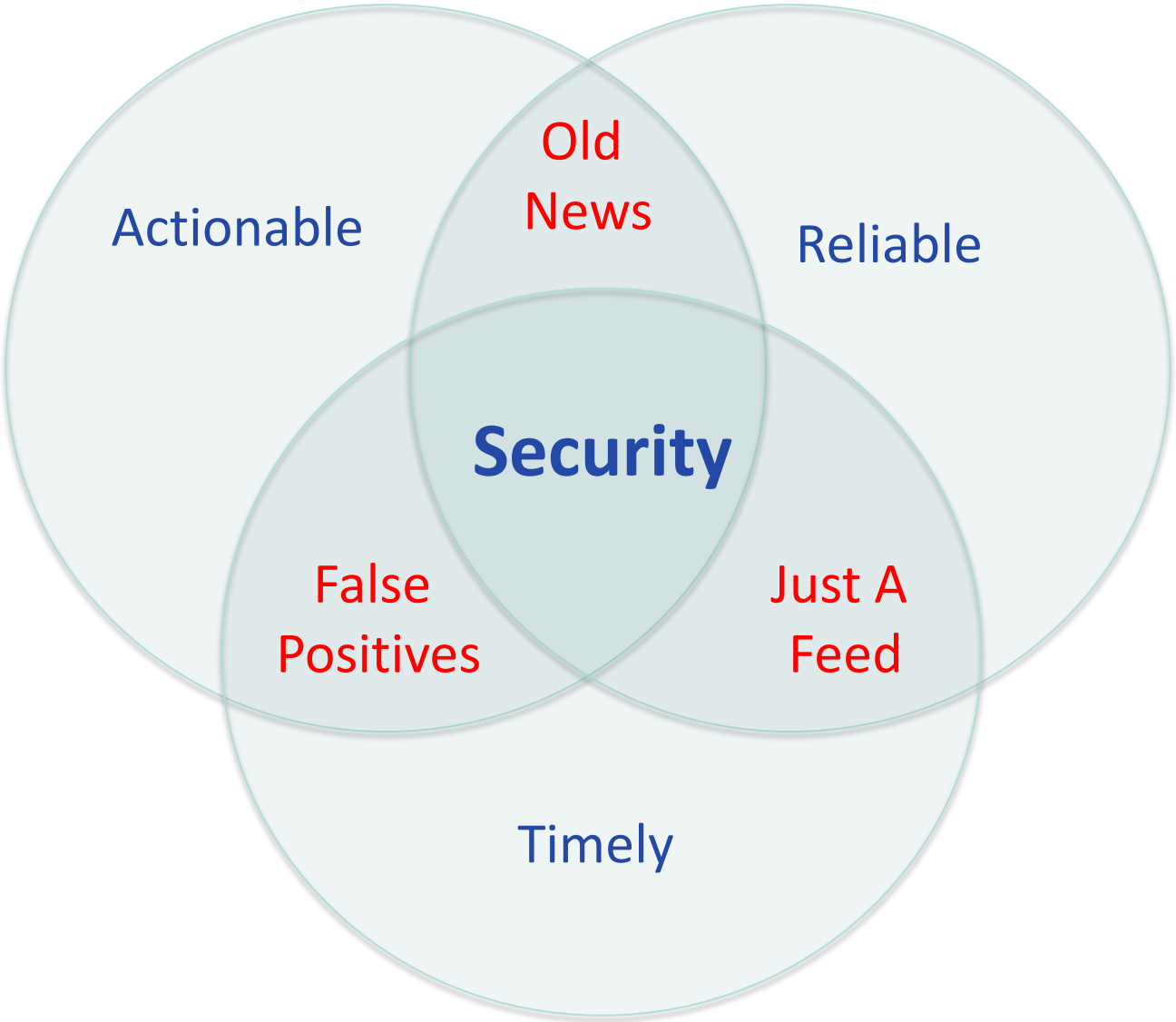
Domain	URI
A9D5F0F6FF1E417FD0F26A42405A6F5E.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]
DEF651313D9BBF292A6C6484E3F076CF.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]
4DD551A2A853C411E005795FA63CE640.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]
4E4ECDE4BD35A25A212C438F7CFE55B9.online	/sta.php?g=[redacted]&o=6&b=&v=3.0&l=pub1all&i=all&s=[redacted]

CATO NETWORKS

To This


REvil
selection controls
layer controls
technique controls
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)
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)
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (0/15)
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)
Group Policy Modification
Hijack Execution Flow (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
Hijack Execution Flow (0/11)
Impair Defenses (1/7)
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 (0/5)
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
Modify Authentication Process (0/4)
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
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
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (1/3)
Software Discovery
System Information Discovery
System Network Connections Discovery
System Owner/User
System Service 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)
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
Man in the Browser
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 Web Service (0/2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot
You Want To BE Here
legend

It’s Only Good As Your Intel



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

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

CATO NETWORKS

Apply

- Start looking for those blind spots in your security people, processes and technology
- Asses the threats your organization is likely to experience and financial losses
- Define a protection strategy that will reduce costs and friction for your clients
- Select a seamless omnichannel solution that is based on AI, ML with a combination of customized heuristics/rules security protections
- Continue to assess the ever-changing threat landscape and associated risks