

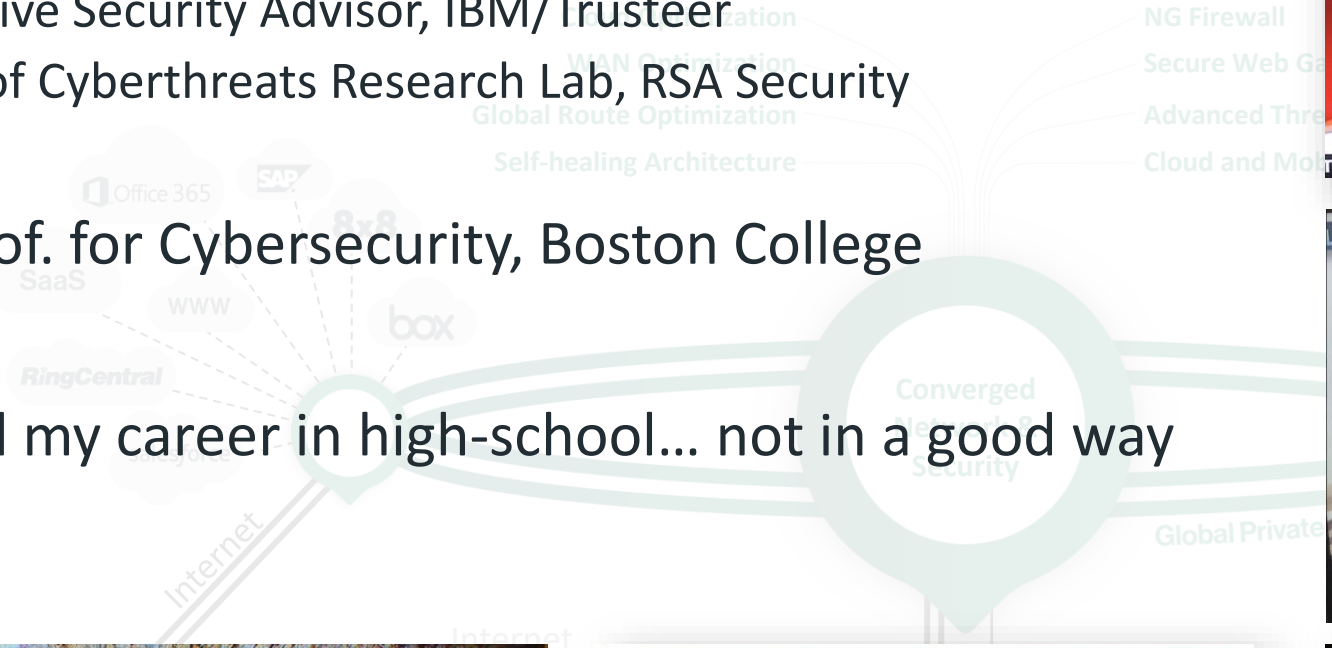


Busting Cybersecurity Myths

Etay Maor, Sr. Director Security Strategy, Cato Networks


Hi

- Some History
 - Chief Security Officer, IntSights
 - Executive Security Advisor, IBM/Trusteer
 - Head of Cyberthreats Research Lab, RSA Security
- Adj. Prof. for Cybersecurity, Boston College
- Started my career in high-school... not in a good way



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

Myth I

A close-up portrait of Captain Jack Sparrow, played by Johnny Depp. He is wearing his signature red bandana with a gold tassel, and his long, dark dreadlocks are visible. He has a slight, knowing smile and is looking off to the side. The background is a blurred outdoor setting.

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



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 Breached Colonial Pipeline Compromised Password

Cybersecurity

Hackers breach LineageOS servers via unpatched A hacker stole more than \$55 million in crypto after a bZx developer fell for a phishing attack

LineageOS source code, O:

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

REvil

selection controls

layer controls

technique controls

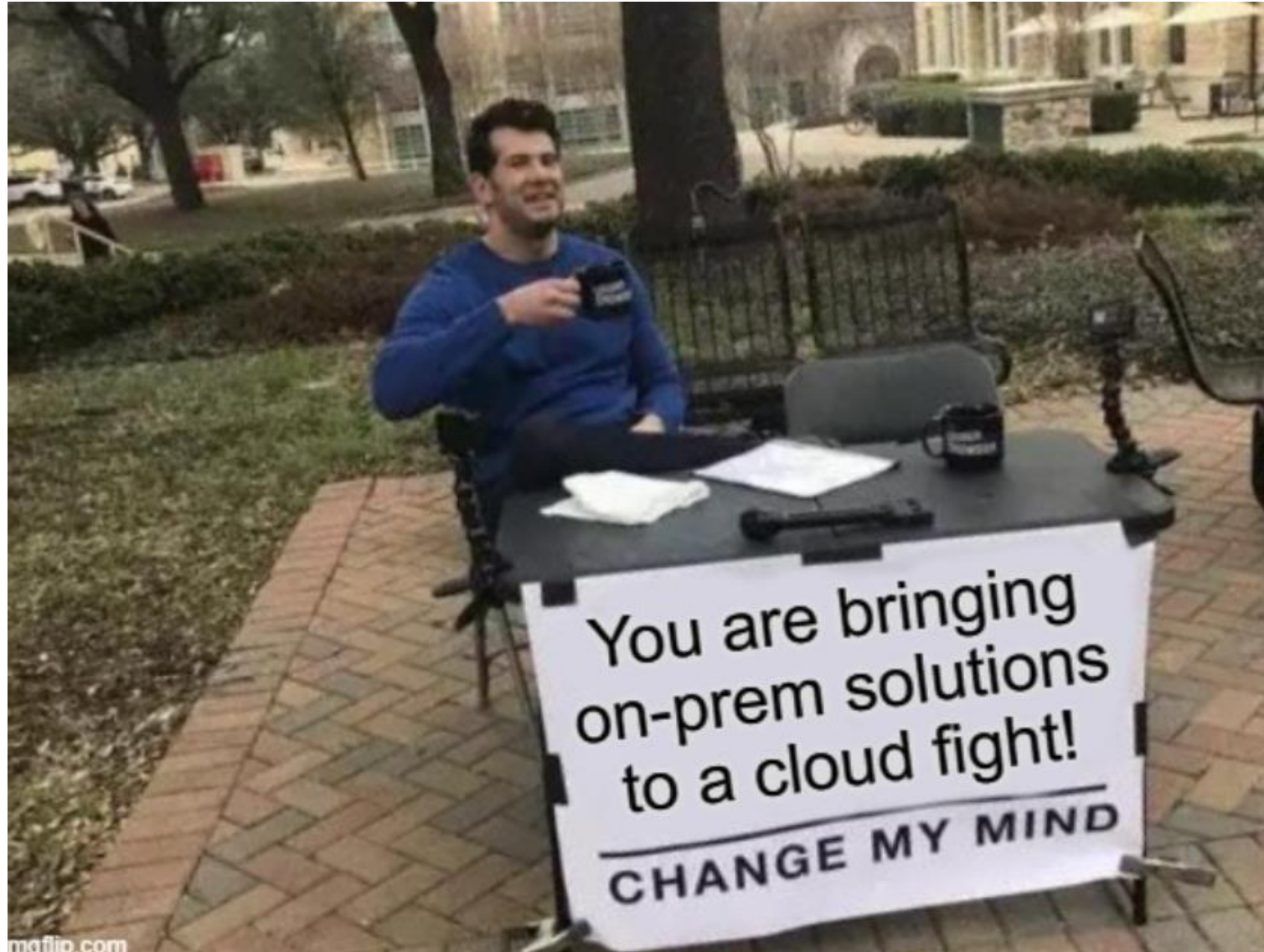
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (3/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (2/5)	Access Token Manipulation (2/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (1/3)	Scheduled Task/Job (0/6)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Configuration Repository (0/2)	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (0/4)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	File and Directory Discovery	Data from Local System	Encrypted Channel (1/2)	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/1)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Network Service Scanning	Data from Network Shared Drive	Fallback Channels	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (1/2)	Event Triggered Execution (0/15)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (0/8)	Network Sniffing	Network Share Discovery	Data from Removable Media	Ingress Tool Transfer	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Peripheral Device Discovery	Password Policy Discovery	Email Collection (0/3)	Multi-Stage Channels		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Process Injection (0/11)	Impair Defenses (1/7)	Steal or Forge Kerberos Tickets (0/4)	Permission Groups Discovery (1/3)	Permission Groups Discovery (1/3)	Input Capture (0/4)	Non-Application Layer Protocol		Resource Hijacking
				Implant Container Image	Scheduled Task/Job (0/6)	Indicator Removal on Host (1/6)	Steal Web Session Cookie	Process Discovery	Query Registry	Man in the Browser	Non-Standard Port		System Shutdown/Reboot
				Office Application Startup (0/6)	Valid Accounts (0/4)	Indirect Command Execution	Two-Factor Authentication Interception	Remote System Discovery	System Information Discovery	Man-in-the-Middle (0/2)	Protocol Tunneling		
				Pre-OS Boot (0/5)		Masquerading (1/6)	Unsecured Credentials (0/6)	Software Discovery (0/1)	System Network Configuration Discovery	Screen Capture	Remote Access Software		
				Scheduled Task/Job (0/6)		Modify Authentication Process (0/4)		System Network Connections Discovery	System Owner/User Discovery	Video Capture	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Cloud Compute Infrastructure (0/4)		System Owner/User Discovery	System Service Discovery		Web Service (0/3)		
				Traffic Signaling (0/1)		Modify System Image (0/2)		System Time Discovery	Virtualization/Sandbox Evasion (0/3)				
				Valid Accounts (0/4)		Network Boundary Bridging (0/1)							
						Obfuscated Files or Information (0/5)							
						Pre-OS Boot (0/5)							
						Process Injection (0/11)							
						Rogue Domain Controller							

You are here!

legend

You are here!

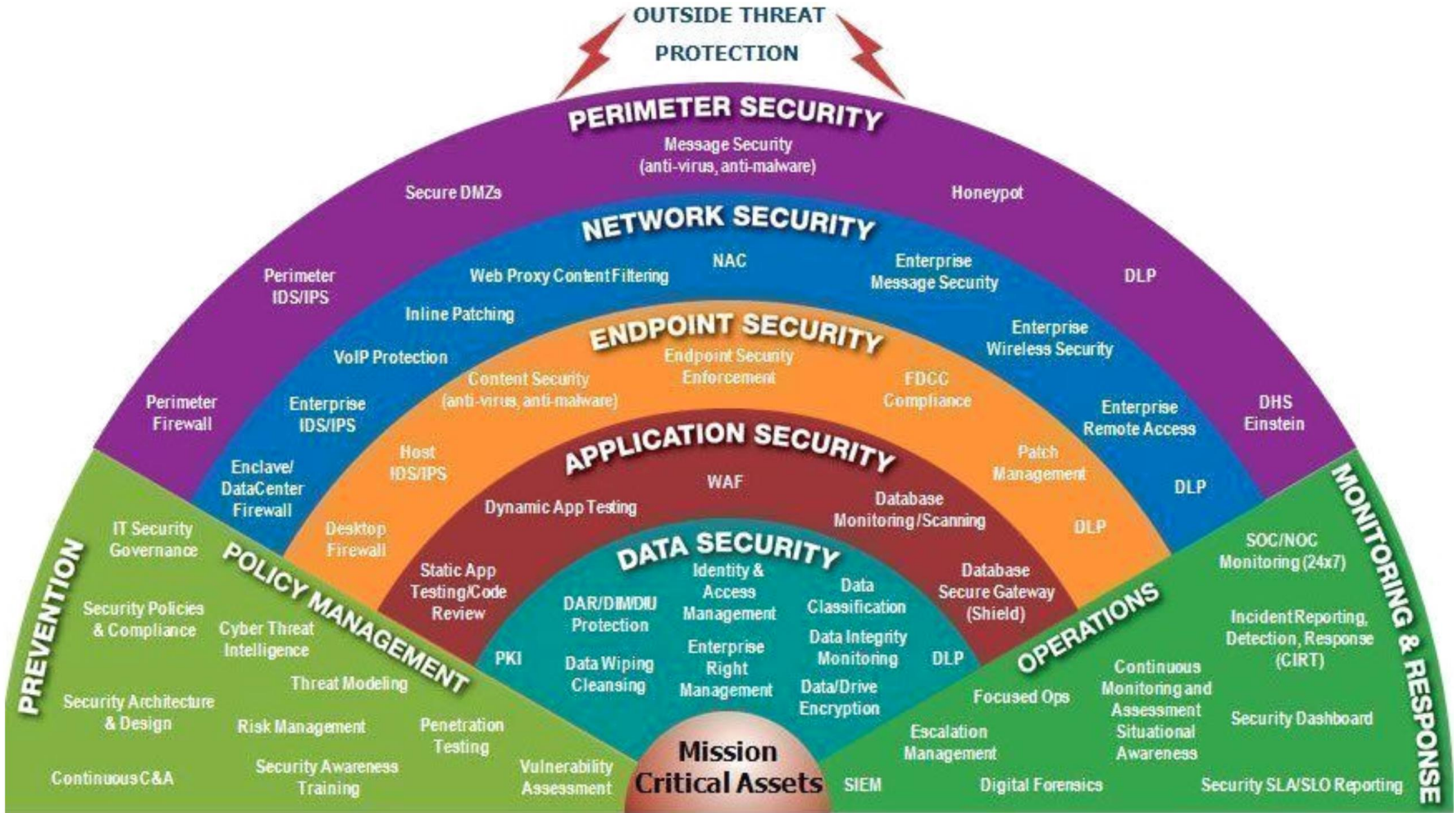
Why Is This Happening?



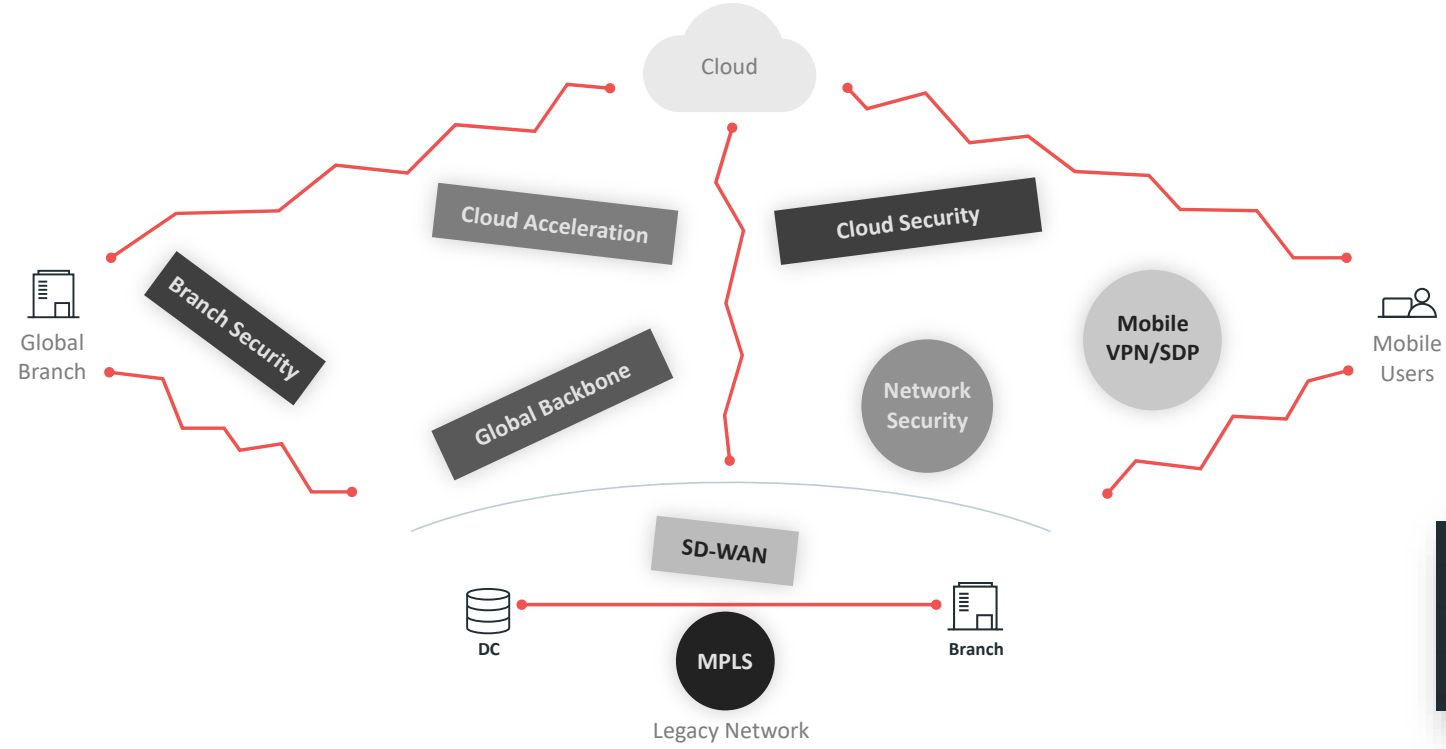
More Security Products = Better Security


Myth II

More Security Products Means Better Security



So, What Are We Missing?



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



Why Is This Happening?



Why Is This Happening?



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.githubusercontent... 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: 9mbKNKq5IN 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:<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Razy.A>

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

```
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 [~]:
```



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.



Change This

REvil x +

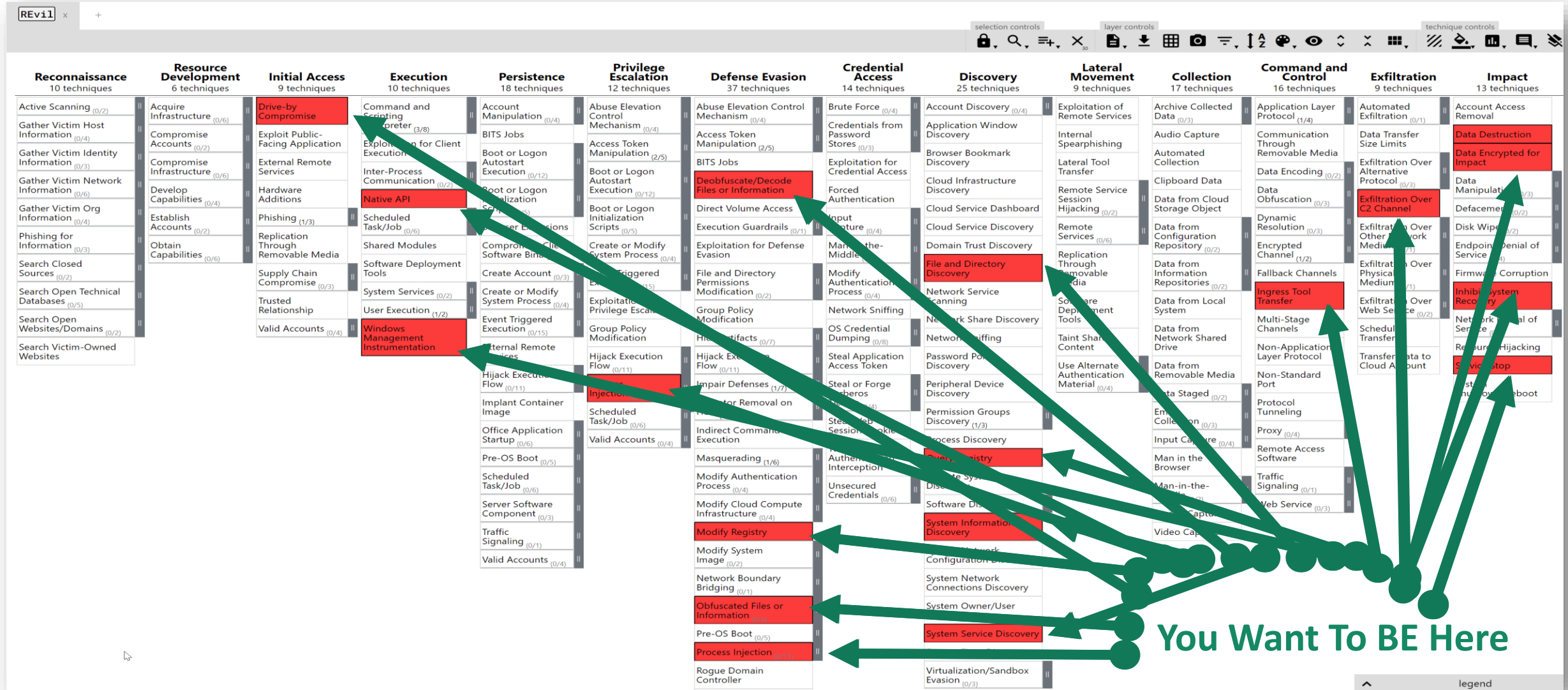
selection controls layer controls technique controls

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (3/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (2/5)	Access Token Manipulation (2/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (1/3)	Scheduled Task/Job (0/6)	Browser Extensions	Browser Extensions	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Configuration Repository (0/2)	Data Obfuscation (0/3)	Defacement (0/2)	Data Manipulation (0/3)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (0/4)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Exfiltration Over Physical Medium (0/1)	Encrypted Channel (1/2)	Exfiltration Over Web Service (0/2)	Disk Wipe (0/2)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Ingress Tool Transfer	Fallback Channels	Endpoint Denial of Service (0/3)	Endpoint Denial of Service (0/3)
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (1/2)	Event Triggered Execution (0/15)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Multi-Stage Channels	Data from Local System	Exfiltration Over Web Service (0/2)	Firmware Corruption
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Non-Application Layer Protocol	Data from Network Shared Drive	Scheduled Transfer	Resource Hijacking
				Hijack Execution Flow (0/11)	Process Injection	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Non-Standard Port	Data from Removable Media	Transfer Data to Cloud Account	Service Stop
				Implant Container Image	Scheduled Task/Job (0/6)	Indicator Removal on Host (1/6)	Steal Web Session Cookie	OS Credential Dumping (0/8)		Protocol Tunneling	Data Staged (0/2)		System Shutdown/Reboot
				Office Application Startup (0/6)	Valid Accounts (0/4)	Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery (1/3)		Proxy (0/4)	Email Collection (0/3)		
				Pre-OS Boot (0/5)		Masquerading (1/6)	Unsecured Credentials (0/6)	Process Discovery		Remote Access Software	Input Capture (0/4)		
				Scheduled Task/Job (0/6)		Modify Authentication Process (0/4)		Query Registry		Traffic Signaling (0/1)	Man in the Browser		
				Server Software Component (0/3)		Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Web Service (0/3)	Man-in-the-Middle (0/2)		
				Traffic Signaling (0/1)		Modify Registry		Software Discovery (0/1)			Screen Capture		
				Valid Accounts (0/4)		Modify System Image (0/2)		System Information Discovery			Video Capture		
						Network Boundary Bridging (0/1)		System Network Configuration Discovery					
						Obfuscated Files or Information (0/1)		System Network Connections Discovery					
						Pre-OS Boot (0/5)		System Owner/User Discovery					
						Process Injection (0/1)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
								Virtualization/Sandbox Evasion (0/3)					

^ legend

You are here!

To This



What Are Attackers Saying?

- Secure vulnerable ports
- Use proper passwords
- Write in a “real” programming language
- Employ the right people
- Watch for misconfigured firewalls

What Are Attackers Saying?

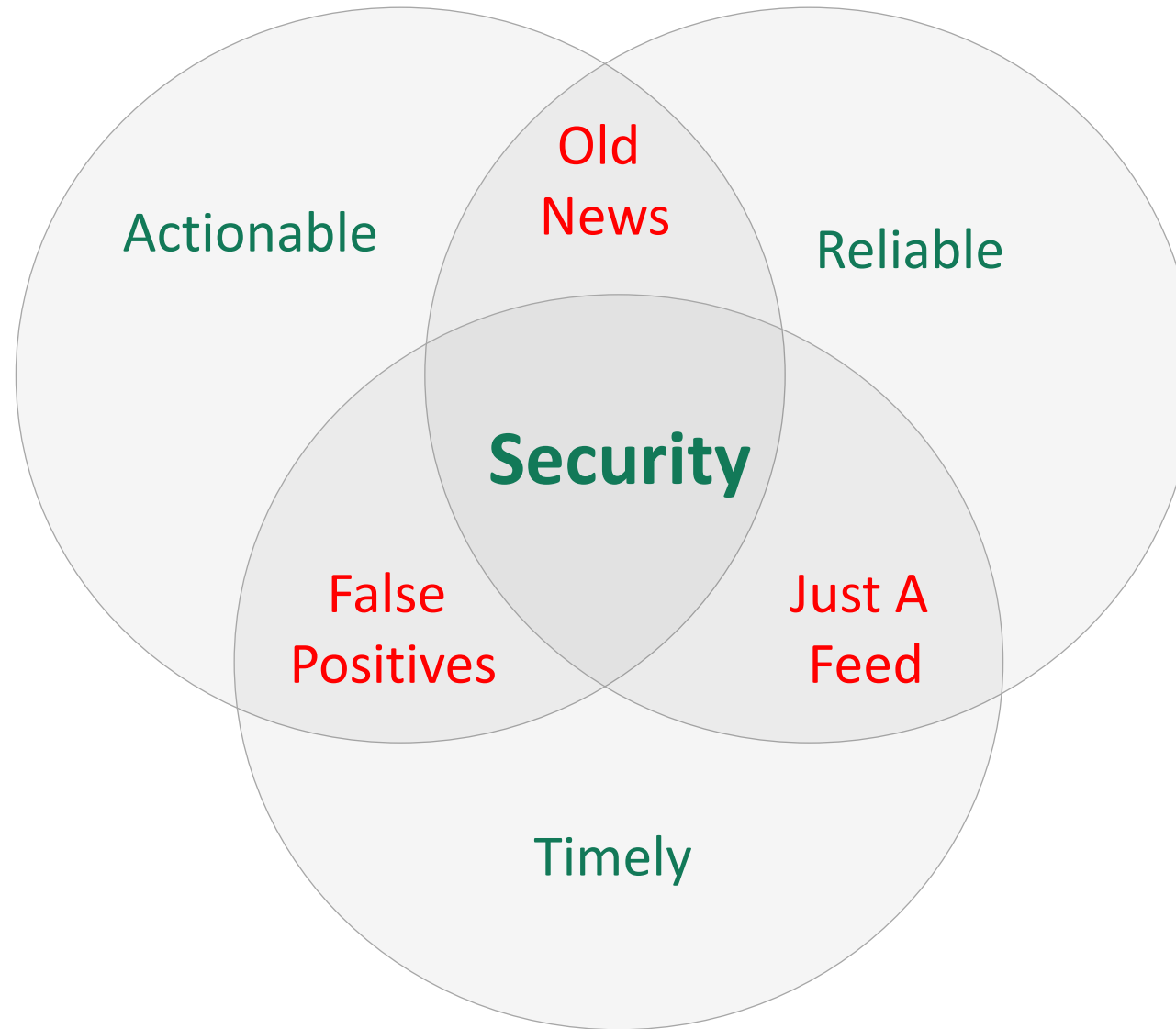
07/28/2020 00:47:12

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.



It's Only Good As Your Visibility



Bonus Myth – Attackers Use Their Own Servers

Aka – LOL? LOC!

For Sale

Genesis Wiki									
News									
Bots									
Generate FP									
Orders									
Purchases									
Payments									
Tickets									
Software									
Profile									
Invites									
Logout									
Bots									
Extended Search									
BOT NAME / Filter bot name									
Any									
RESOURCES KNOWN / OTHER									
Filter resource name/domain: paypal,ebay.com,hotmail.com...									
COUNTRY / HOST									
PRICE									
Filter IP/Country/OS									
Filter \$									
D6E9E17A5BB4B906FF708AD581110557									
2021-01-24 01:38:41									
2021-01-26 00:14:41									
Live									
31A46C2C9C1218BFFB6960DE876F6701									
2021-01-25 06:35:48									
2021-01-26 00:14:41									
Google									
9DD2ADE02B27CBF6A187B7FBB393635E									
2021-01-22 18:28:34									
2021-01-26 00:14:41									
Netflix									
Facebook									
www.chegg.com									
Amazon									
Yahoo									
9C85A9FF04CA9AEF9DF7493320CFE554									
2021-01-25 12:13:32									
2021-01-26 00:14:41									
Live									
Hootsuite									
127.0.0.1									
localhost									
elearning.nesoformacion.com									
tplinkrepeater.net									
F7D00592ED356CB320A562C5D61193C4									
2021-01-25 16:56:48									
2021-01-26 00:14:41									
Live									
Spotify									
Amazon									
FirefoxAccount									
OnlyFans									
WesternUnion									
Facebook									
BolStore									
air.com,rosettastone.mobile,Cour...									
com.babbel.mobile.android.en									
com.aidungeon									
7CEFB0A8B2C7D119D4B3F296BD768F75									
2021-01-25 16:54:32									
2021-01-26 00:14:41									
Fiverr									
AppleStore									
Office365									
Instagram									
Live									
Facebook									
Aliexpress									
PayPal									
Twitter									
my.wondershare.com									
zamunda.net									
www.zamunda.net									

For Sale

F7D00592ED356CB320A562C5D61193C4

Add to Cart Reserve Buy

Country	NL
Resources	39
Browsers	2
Installed	2021-01-25 16:56:48
Updated	2021-01-26 00:14:41
Ip	24.132...
Os	Windows 10 Home
Price Usd	22.00

Browsers for Genesis Security:

Last update info: 2021-01-26 00:14:41

F7D00592ED356CB320A562C5D61193C4

chrome	
Cookies	490 (2021-01-26 00:03:58)
firefox	
Cookies	2651 (2021-01-26 00:03:58)

Resources: 39 = 0 39 0

Facebook	3	Live	3	BolStore	2	OnlyFans	1	Spotify	1	Twitter	1
Reddit	1	FirefoxAc...	1	LinkedIn	1	WesternUnion	1	Amazon	1		

com.jagex.oldscape.android	4	com.lgi.ziggotv	2	air.com.rosettastone.mo...	2	tv.twitch.android.app	1
com.discord	1	com.snapchat.android	1	com.aidungeon	1	authenticate.riotgames.com	1
com.instagram.android	1	paiq.nl	1	secure.runescape.com	1	com.soundcloud.android	1
auth.riotgames.com	1	com.miHoYo.GenshinImpact	1	login.unive.nl	1	com.babbel.mobile.andro...	1
m.chaturbate.com	1	anilist.co	1				

Last update Saved Logins: 2021-01-25 17:14:17
Last update Form Parser: 1970-01-01 00:00:00
Last update Inject Script: 1970-01-01 00:00:00



The Network for Whatever's Next

Thank You!

