RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HT-R01**

Zero to Full Domain Admin Real-World Ransomware Incident

***This session is mostly a LIVE WALKTHROUGH**

Joseph Carson

Chief Security Scientist & Advisory CISO
Delinea
@joe_carson

Who is it for?

Pentesters / Incident Response

IT & System Admin

IT Security

IT Auditors

Tech Geeks

Disclaimer & Ethics

Authorized Only

Do No Harm

Follow the Law

Educational Purpose

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.


CryLock
ENCRYPTED
11000110001111010110011010010011010000 11
What happened?
All your documents, databases, backups, and other critical files were encrypted.
Our software used the AES cryptographic algorithm (you can find related information in Wikipedia).
It happened because of security problems on your server, and you cannot use any of these files anymore. The only way to recover your data is to buy a decryption key from us.
To do this, please send your unique ID to the contacts below.
E-mail: reidcry@dr.com copy
Unique ID: [F42CECBB-50766EF9] copy
During a short period, you can buy a decryption key with a
50% discount
2 days 23:56:39
Right after payment, we will send you a specific decoding software that will decrypt all of your files. If you have not received the response within 24 hours, please contact us by e-mail crylock@consultant.com.
The price depends on how soon you will contact us.
All your files will be deleted permanently in: 4 days 23:56:39
Attention!
! Do not try to recover files yourself. this process can damage your data and recovery will become impossible.
! Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price.
! Do not contact any intermediaries. They will buy the key from us and sell it to you at a higher price.
What guarantees do you have?
Before payment, we can decrypt three files for free. The total file size should be less than 5MB (before archiving), and the files should not contain any important information (databases, backups, large tables, etc.)

You'll most likely be notified of a breach by an OUTSIDER!

- Law Enforcement
- Third Parties including customers
- Attackers contact you
- Social Media
- Employees
- Security Researchers

Incident Response

Incident Response **Checklist – Be ready**

- ✓ Ownership
- ✓ Communications
- ✓ Contact List
- ✓ Clear Definition of Threat
  1) Confidentiality – Data Loss
  2) Integrity – Data Poisoning
  3) Availability - DDOS
- ✓ In-House Capability and 3rd Party Responsibility
- ✓ Containment (Evidence)
- ✓ Press Statement
- ✓ Legal Assessment
- ✓ Eradication
- ✓ Recovery
- ✓ Lessons Learned

Be Incident Response Ready

- Time Format and Naming?
- Policies (HR, Legal, Law Enforcement)
- Evidence Gathering (Logs, Images)
- Identities and User Access
- Service Accounts (Privileged Access, Rotate)
- Go Bag (Everything you might need)
- Communications Alternative (OOB)
- Helpdesk Ready
- Incident Response Plan – Keep Updated
- Incident Response Practice Drills

The Plan and Actions

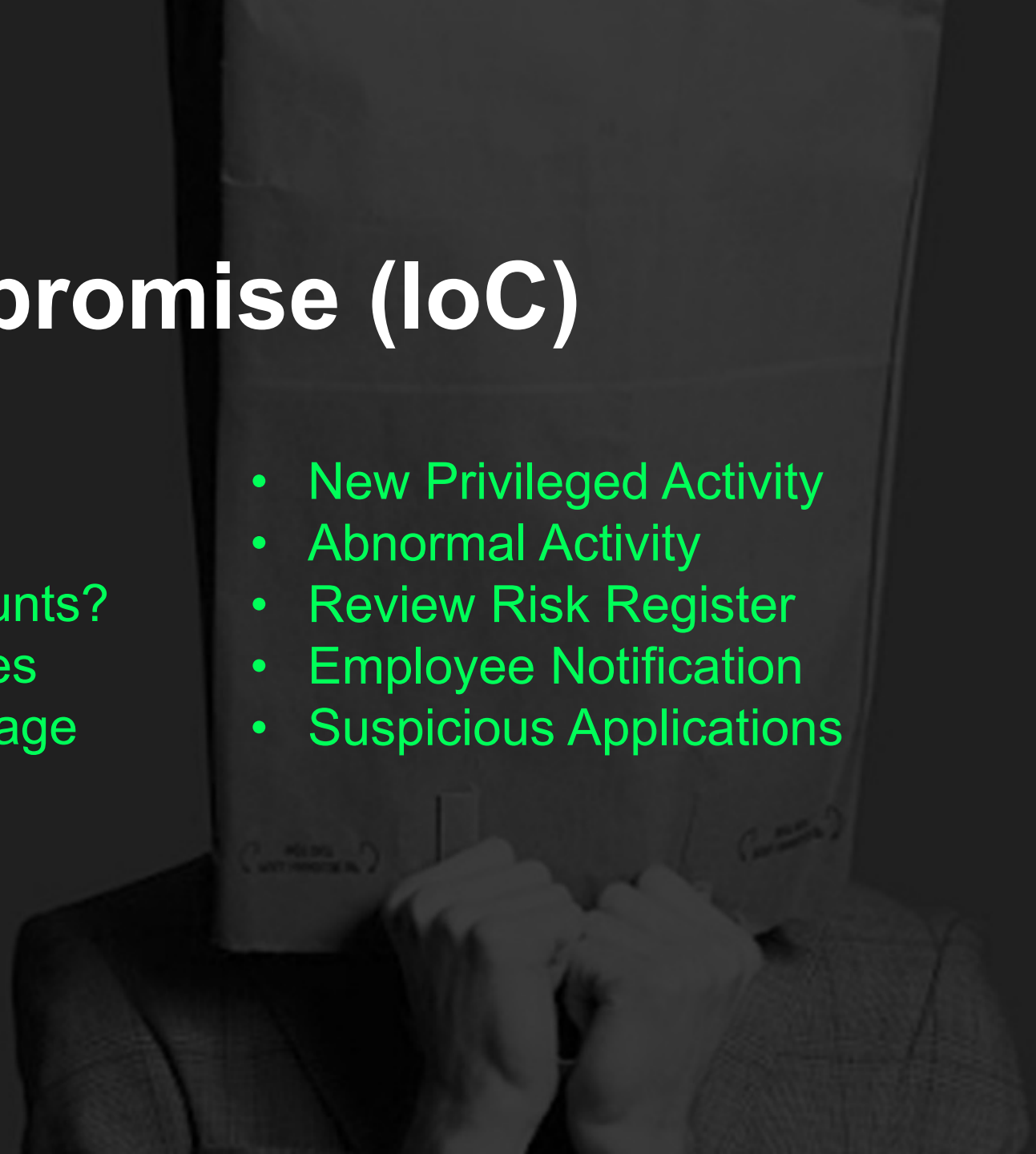
Document and Coordinate

- Mandatory Requirements
- Who is Responsible for managing – IR Plan
- Executive Summary
- Incident Response Timeline
- Attack Path – Mitre Attack Framework
- Malware Analysis
- Data Recovery and Evidence Store
- Threat Intelligence (Dark web)
- Security in Place and Mitigations to contain Incident
- Data Exfiltration
- Asset Inventory
- Network Activity

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 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 (0/8)	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 (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	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	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	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	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (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	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	Exploitation for Defense Evasion	OS Credential Dumping (0/8)	Network Service Scanning		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
			User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	File and Directory Permissions Modification (0/2)	Steal Application Access Token	Network Share Discovery		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/7)	Hide Artifacts (0/7)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Modify Authentication Process (0/4)	Valid Accounts (0/4)	Hijack Execution Flow (0/11)	Steal Web Session Cookie	Password Policy Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
						Impair Defenses (0/7)		Peripheral Device Discovery		Man in the Browser	Remote Access Software		
						Indicator Removal on Host (0/6)		Permission Groups Discovery (0/3)					
						Indirect Command Execution							

Indicators of Compromise (IoC)

- Audit Logs?
- After Password Rotation?
- Discovering New Privileged Accounts?
- Access from non-corporate devices
- Increased Network Bandwidth Usage
- Out of Hours Activity
- New Privileged Activity
- Abnormal Activity
- Review Risk Register
- Employee Notification
- Suspicious Applications



Shutdown Systems

Pull the Plug?

Can you go back to manual?

What systems are still operational?

Are the attackers still accessing your systems?

What did the attackers have access to and how did they do it?

- Domain Admin and DC
- All Systems
- All Data
- All Applications?
- On-Premise or Cloud?
- How long?
- What tools did they use?
- Did they leave any backdoors?
- What data did they take and how?
- What is the timeline of events?
- What evidence is remaining?

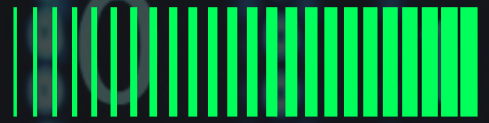
If you do become a victim of Ransomware

RESTORE BACKUP or

PAY RANSOM or

DO NOTHING
AND HOPE TO REBUILD

Find a sample of **Cryptor** from infected system



JoeSandbox Cloud BASIC

Overview | Signatures | Process Tree | Domains / IPs | Dropped | Static | Network | Hooks | Stats | Behavior | Disassembly

Windows Analysis Report JwxBYn78uM

Create Interactive Tour

Overview

General Information

Sample Name:	JwxBYn78uM (renamed file extension from none to exe)
Analysis ID:	463280
MD5:	2f2d4eb24662c916f822f9c3...
SHA1:	9d5bda347f70b8f928803a2...
SHA256:	4a47769cf06cd353a24bf01...
Tags:	CryLock, exe, Ransomware
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

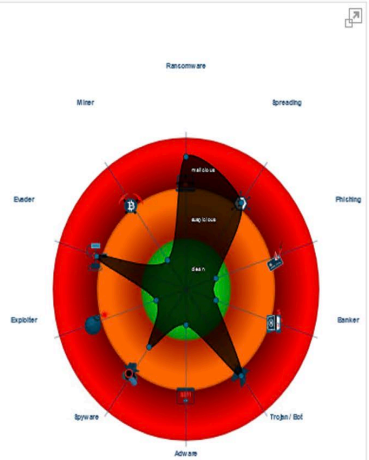
CryLock

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for submitted sample
- Found malware configuration
- Found ransom note / readme
- Multi AV Scanner detection for submitted file
- Sigma detected: Shadow Copies Deletion Using Operat...
- Sigma detected: WannaCry Ransomware
- Yara detected CryLock ransomware
- Creates HTA files
- Creates autostart registry keys with suspicious names
- Creates files in the recycle bin to hide itself
- Deletes shadow drive data (may be related to ransomw...
- Machine Learning detection for sample
- Sigma detected: Copying Sensitive Files with Credentia...
- Spreads via windows shares (copies files to share folders)
- Uses bcdedit to modify the Windows boot settings
- Uses ping.exe to check the status of other devices and ...

Classification



Process Tree

- System is w10x64
- JwxBYn78uM.exe (PID: 6636 cmdline: 'C:\Users\user\Desktop\JwxBYn78uM.exe' MD5: 2F2D4EB24662C916F822F9C3FD55C9B2)
  - svcqfn.exe (PID: 6988 cmdline: 'C:\Users\user\appdata\local\temp\svcqfn.exe' MD5: 2F2D4EB24662C916F822F9C3FD55C9B2)
    - cmd.exe (PID: 5916 cmdline: 'C:\Windows\System32\cmd.exe' /c vssadmin delete shadows /all /quiet MD5: F3BDBE3BB6F734E357235F4D5898582D)

https://www.virustotal.com/gui/file/04d8109c6c78055d772c01fefe1e5f48a70f2a65535cff17227b5a2c8506b831/detection/f-04d8109c6c78055d772c01fefe1e5f48a70f2a65535cff17227b5a

04d8109c6c78055d772c01fefe1e5f48a70f2a65535cff17227b5a2c8506b831

61 / 71

Community Score

61 security vendors and 1 sandbox flagged this file as malicious

04d8109c6c78055d772c01fefe1e5f48a70f2a65535cff17227b5a2c8506b831

CryLock Ransomware.exe

direct-cpu-clock-access peexe runtime-modules

672.00 KB Size

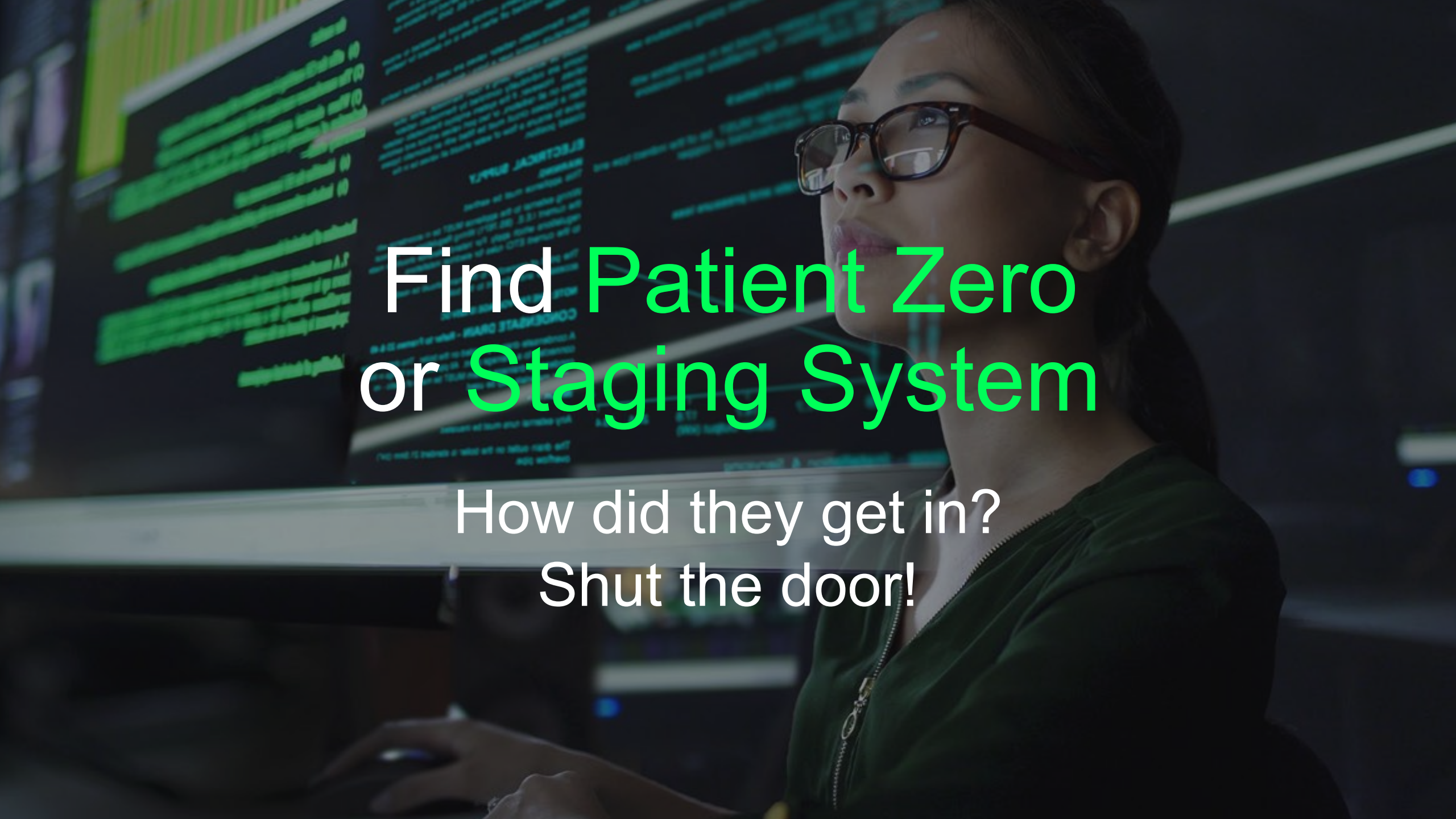
2020-12-03 18:37:36 UTC 11 months ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

Ad-Aware	Gen:Variant.Barys.62761	AegisLab	Trojan.Win32.Cryakl.j!c
AhnLab-V3	Trojan/Win32.FileCoder.C4206605	Alibaba	Ransom:Win32/FileCryptor.b239af7c
ALYac	Trojan.Ransom.Cryakl	Antiy-AVL	Trojan[Ransom]/Win32.Cryakl
Arcabit	Trojan.Barys.DF529	Avast	Win32:RansomX-gen [Ransom]
AVG	Win32:RansomX-gen [Ransom]	Avira (no cloud)	TR/FileCryptor.ereit
BitDefender	Gen:Variant.Barys.62761	BitDefenderTheta	Gen:NN.ZelphiF.34670.QGW@aGQOB6...
CAT-QuickHeal	TrojanRansom.Cryakl	ClamAV	Win.Ransomware.Cryakl-9797480-0
Comodo	Malware@#o1bm28xm3jgu	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.931d0f	Cylance	Unsafe
Cynet	Malicious (score: 85)	Cyren	W32/Filecoder.U.gen!Eldorado
DrWeb	Trojan.Encoder.32204	Elastic	Malicious (high Confidence)


Following the attackers' footprints
ATTACK PATH
LIVE WALKTHROUGH OF ATTACK

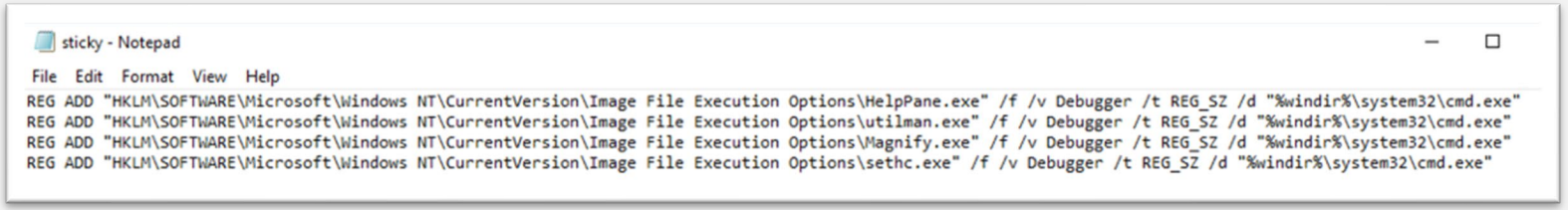

Find Patient Zero
or Staging System
How did they get in?
Shut the door!

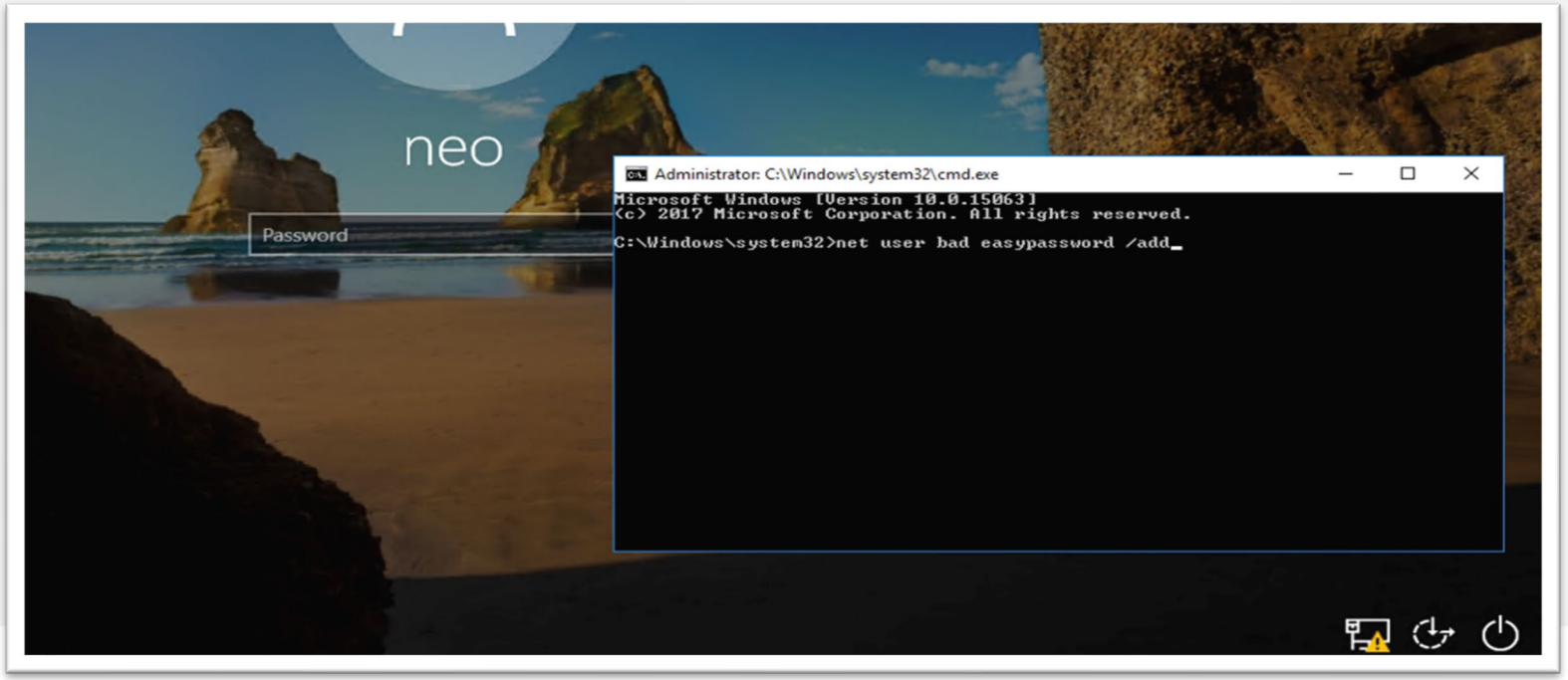
Initial access

Staging systems


Disable Security
Using Local Admin

Persistence & Backdoors





Elevate Privileges

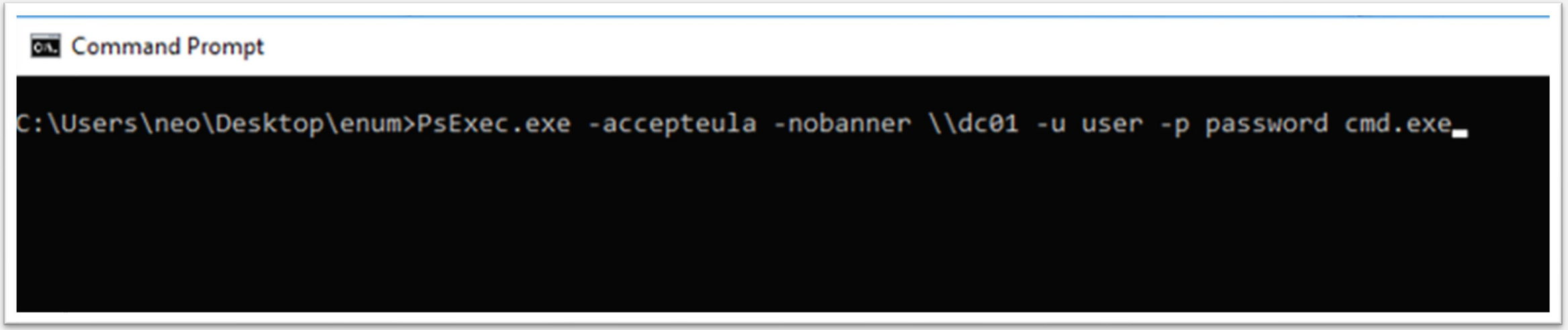
MIMIKATZ

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest]
'UseLogonCredential"=dword:00000001
```

```
  .#####.   mimikatz 2.2.0 (x64) #17763 Apr  9 2019 00:54:23
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonPasswords full

Authentication Id : 0 ; 1726027 (00000000:001a564b)
Session           : RemoteInteractive from 4
User Name         : neo
Domain            : MATRIX
Logon Server      : CYBER-DC
Logon Time        : 2/11/2021 12:16:13 PM
SID               : S-1-5-21-2629657287-2071852410-1843873068-1107
        msv :
         [00000003] Primary
         * Username : neo
         * Domain   : MATRIX
         * NTLM     : 13b1e64400203ecf38b1fdea2b11a09f
         * SHA1     : 27247eb4ca11e05f910b41451ce2a0a95366c150
         * DPAPI    : 68043041cbae5792b8df309b796d2d89
        tspkg :
        wdigest :
         * Username : neo
         * Domain   : MATRIX
         * Password : Password321!
        kerberos :
         * Username : neo
         * Domain   : MATRIX.LOCAL
         * Password : (null)
        ssp :
        credman :
```

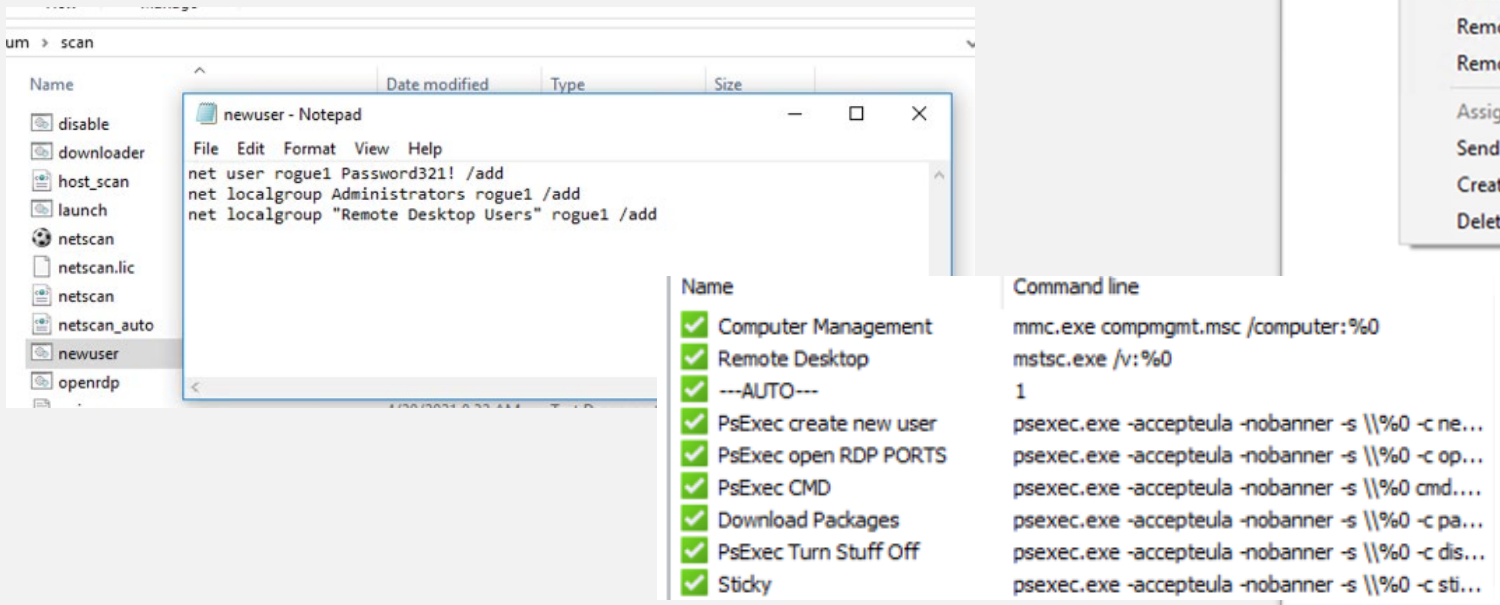
Lateral Moves

Using PsExec

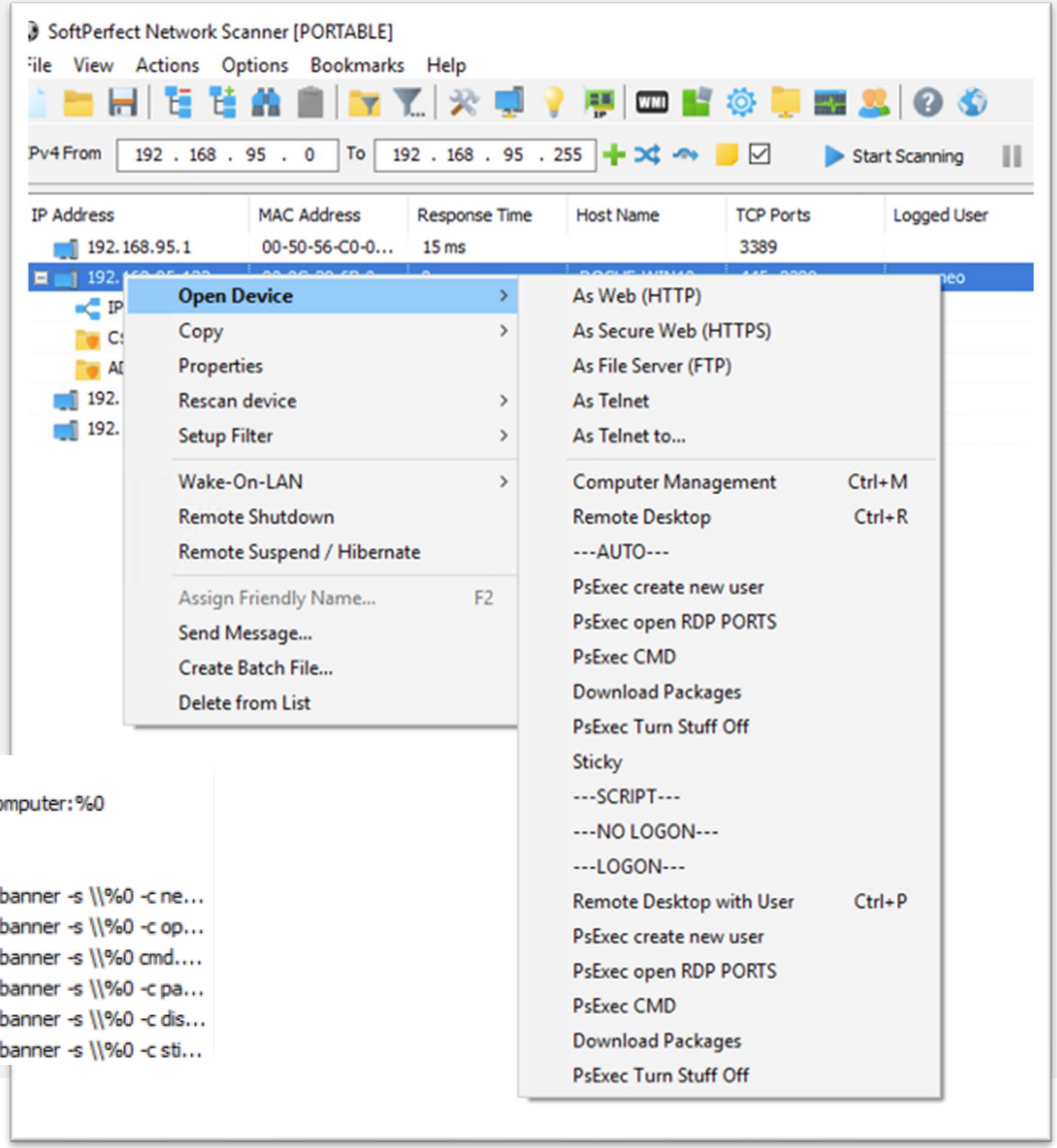


Automation

Mostly using batch scripts



Name	Command line
Computer Management	mmc.exe compmgmt.msc /computer:%0
Remote Desktop	mstsc.exe /v:%0
---AUTO---	1
PsExec create new user	psexec.exe -accepteula -nobanner -s \\%0 -c ne…
PsExec open RDP PORTS	psexec.exe -accepteula -nobanner -s \\%0 -c op…
PsExec CMD	psexec.exe -accepteula -nobanner -s \\%0 cmd.…
Download Packages	psexec.exe -accepteula -nobanner -s \\%0 -c pa…
PsExec Turn Stuff Off	psexec.exe -accepteula -nobanner -s \\%0 -c dis…
Sticky	psexec.exe -accepteula -nobanner -s \\%0 -c sti…




What can we do to
reduce the risks?

Top tips to stop Ransomware based on this ATTACK

- **Education & Cyber Hygiene**
- **Backup & Test**
- **Zero-Trust & Least Privilege**
- **Privileged Access Management**
- **Application Control**
- **Patch and Update Security**

RSAConference2022

”Understanding hacker techniques and processes is the best way to defend against cyber attacks, and focusing on business risks is the best way to get security budget.“

– Joseph Carson