Battling Ransomware!

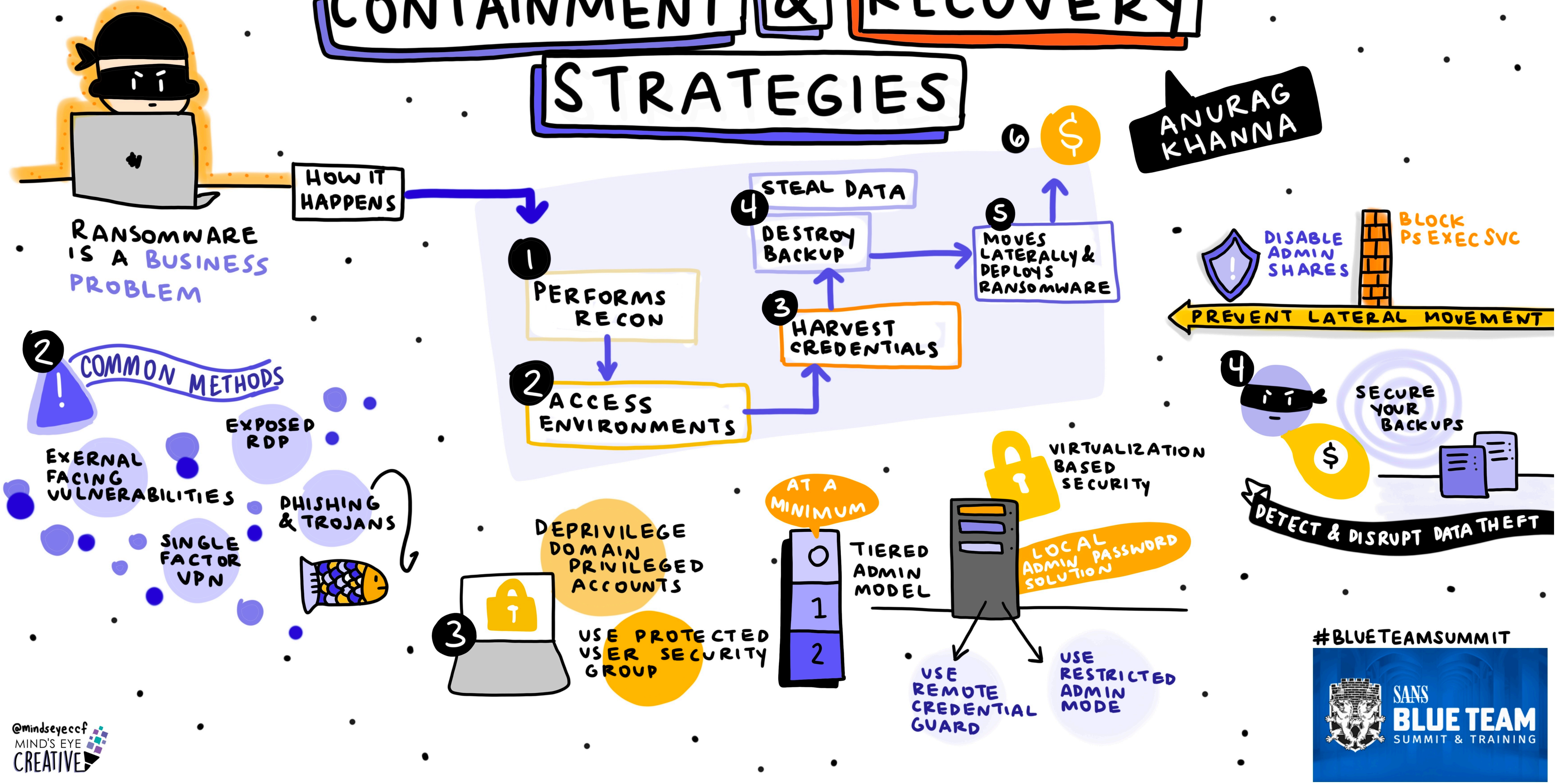
“Ransomware Preparation, Containment and Recovery Strategies”

Anurag Khanna

SANS Blue Team Summit 2021

v1.0

RANSOMWARE PREPARATION CONTAINMENT & RECOVERY STRATEGIES


ANURAG KHANNA
RANSOMWARE IS A BUSINESS PROBLEM
HOW IT HAPPENS
1 PERFORMS RECON
2 ACCESS ENVIRONMENTS
3 HARVEST CREDENTIALS
4 STEAL DATA
DESTROY BACKUP
5 MOVES LATERALLY & DEPLOYS RANSOMWARE
6 $
2 COMMON METHODS
EXERNAL FACING VULNERABILITIES
EXPOSED RDP
SINGLE FACTOR VPN
PHISHING & TROJANS
3
DEPRIVILEGE DOMAIN PRIVILEGED ACCOUNTS
USE PROTECTED USER SECURITY GROUP
AT A MINIMUM
0
1
2
TIERED ADMIN MODEL
VIRTUALIZATION BASED SECURITY
LOCAL ADMIN PASSWORD SOLUTION
USE REMOTE CREDENTIAL GUARD
USE RESTRICTED ADMIN MODE
DISABLE ADMIN SHARES
BLOCK PS EXEC SVC
PREVENT LATERAL MOVEMENT
4
SECURE YOUR BACKUPS
$
DETECT & DISRUPT DATA THEFT
#BLUETEAMSUMMIT
SANS BLUE TEAM SUMMIT & TRAINING
@mindseyeccf
MIND'S EYE CREATIVE

What will we talk about today?

- Ransomware!
- Anatomy of a ransomware attack
- Preparation to stop these attacks
- Responding to threat actor activity

Takeaway: Understand the ransomware attacks. prepare, prevent and respond.

Primary Motivations & Objectives

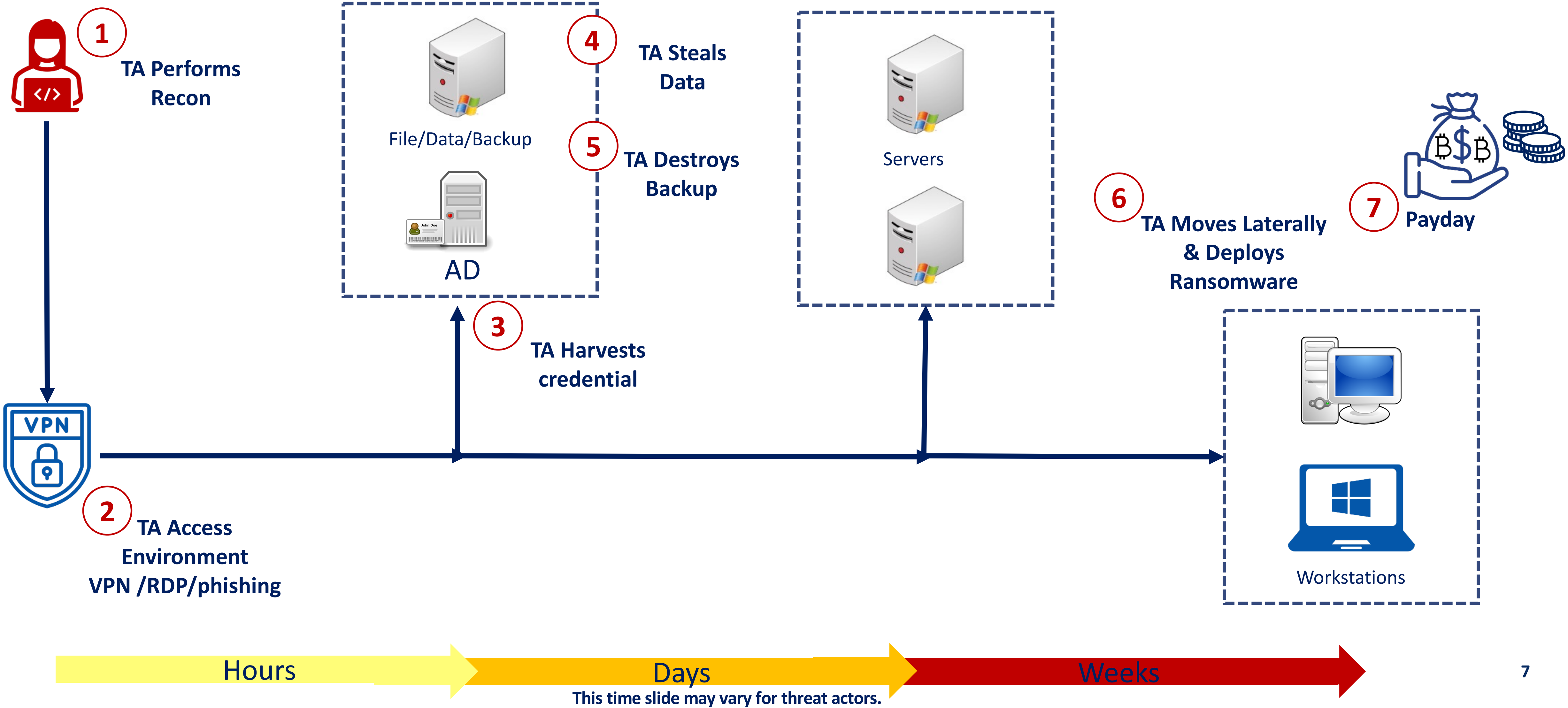
- Primary motivations
  - Escalate privileges and deploy ransomware on servers and endpoints
  - Destroy backups making it difficult to recover
  - Exfiltrate critical data from servers for extortion
  - Get Paid! – Threat Actor with a business model

Battling Ransomware

Ransomware is a business problem!

- Today we will talk about technical response to the problem
- Responding to Ransomware needs a business response
- When you respond to Ransomware - You will break stuff!
- You will break stuff! That should be ok ☺

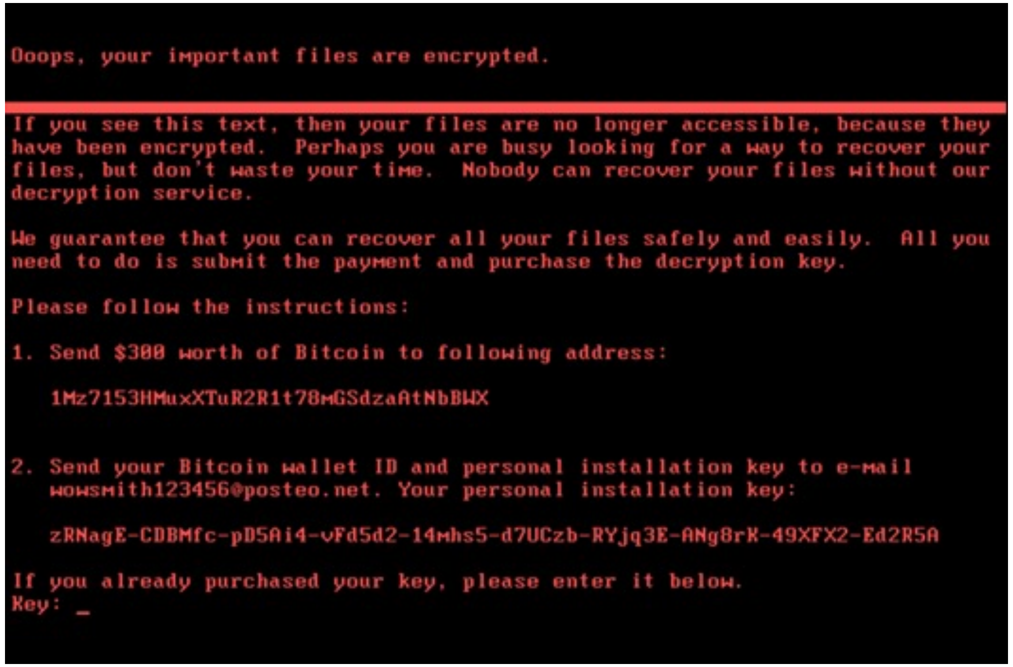
Anatomy of Ransomware attack



This time slide may vary for threat actors.

Before you saw that Ransomware message

- Threat Actor
  - Exploited an Initial vector and gained access
  - Dumped credentials in the environment
  - Moved laterally to the crown jewels
  - Exfiltrated data to intimidate to pay up
  - Pushed ransomware to lock you out



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

Ransomware Message

Ransomware is a symptom, an Action on Objectives.

Image Credit: CrowdStrike

2 TA Access Environment
VPN/RDP/phishing

Initial Compromise

External Facing Vulnerabilities

Exposed RDP

Phishing & Trojans

Single Factor VPN

Ransomware actors often buy access from independent cyber criminal groups/brokers for a slice of the ill-gotten gains.

Initial Entry Point

	External Facing Vuln's	Exposed RDP	Phishing & Trojans	Single Factor VPN
Preparation	• Patch external facing services • Execute enterprise password resets for VPN Vulnerabilities • Limit external facing systems and services	• Limit exposure of RDP to internet • RDP should be behind MFA • Remove external facing RDP from Domain • Scan external facing IPs for tcp/3389	• Use Email Security Solutions • Change default programs associated with vb, js • User Awareness • Disable Macro Execution	• Use MFA for ALL accounts on VPN • Force users to enter code rather than push notifications • Disallow Priv. accounts over VPN • Monitor suspicious logins
Hunting	• Scan external facing IPs • Suspicious Logins & executions	• Hunt for suspicious Type 10 Logins • Source in different Geos • 4625s followed by a 4624 • From an External IP • From Privileged account to non-Tier 0 system	• Hunt for execution from • %APPDATA% • %TEMP% • %USERPROFILE% • Names ending in 32|64 • Execution of Scripts • Office files running code	• Hunt for impossible logins • Hunt for suspicious logins • Accounts with multiple second factors • Local accounts on VPN allowed authentication

TA Harvests credential

Mimikatz to dump credentials

Procdump to dump LSASS

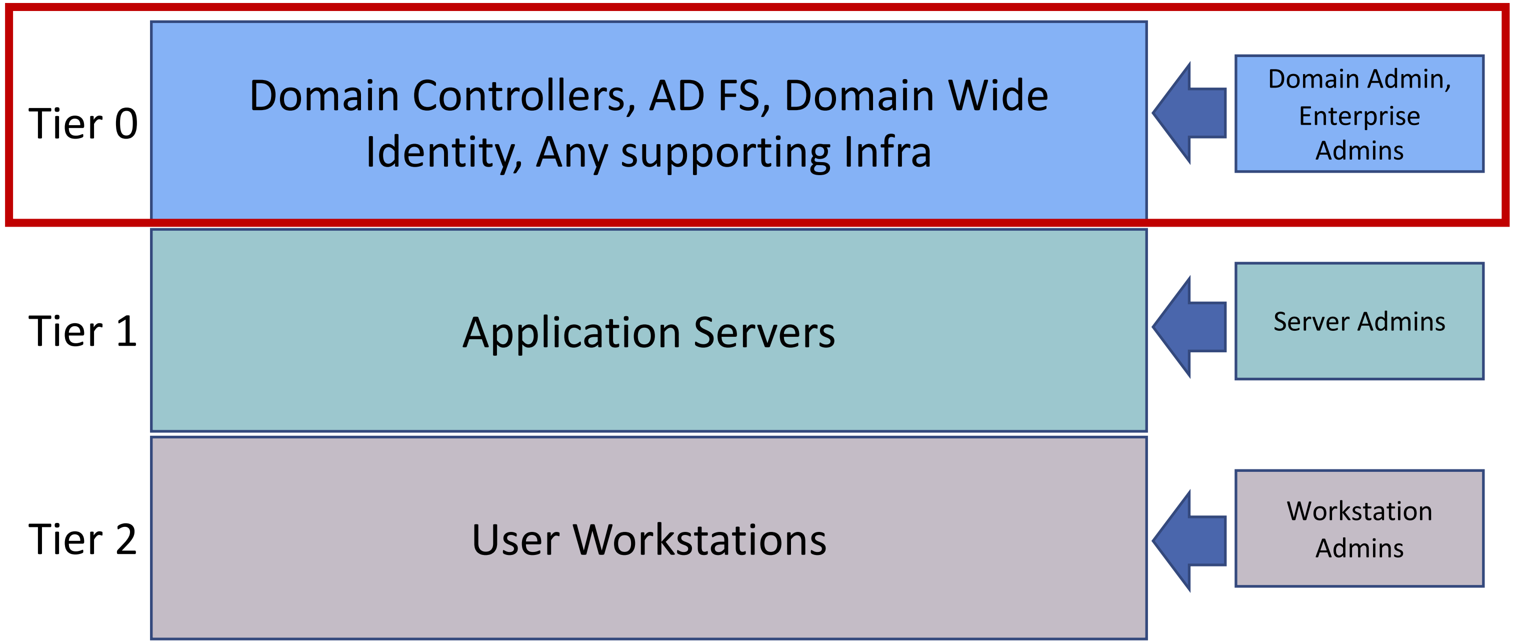
Steal NTDS.dit

Harvesting credentials is the key part of threat actor's workflow.

Secure Domain Privileged Accounts

- Deprivilege domain privileged accounts
  - Enterprise Admins, Domain Admins, Administrators and Schema Admins
  - Backup Operators, Print Operators, Server Operators, Account Operators, DNS Admins, Group Policy Creator Owners, others with privileged user rights
- Use Protected Users Security Group
  - requires DFL Windows Server 2012, implements several non configurable security protections to user accounts
- Review permissions for principals that can modify GPOs & monitor changes
  - Often attackers use GPOs to disable AV and deploy ransomware
- Disable weaker Authentication mechanisms e.g., WDigest
- At the time of incident – rotate credentials, disable accounts, remove privileges

Protect Privileged AD credentials using Tiered Admin Model



Tier 0

Domain Controllers, AD FS, Domain Wide Identity, Any supporting Infra

Domain Admin, Enterprise Admins

Tier 1

Application Servers

Server Admins

Tier 2

User Workstations

Workstation Admins

- Limit number of systems with privileged credential exposure.
- Hunt for Privileged credential usage on non domain controllers

Tier 0 Admins are allowed interactive login to Tier 0 Assets only.

Enforcing Logon restrictions

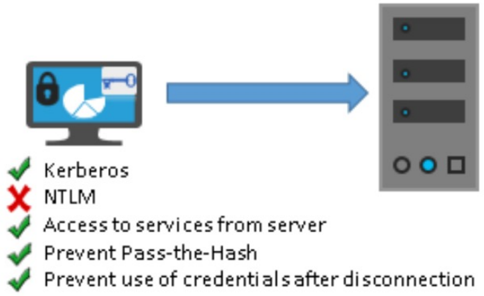
Group Policy Logon Rights Restrictions:

- Deny access to this computer from the network
- Deny logon as a batch job
- Deny logon as a service
- Deny logon locally
- Deny logon through Remote Desktop settings

Bare minimum, limit Domain level privileged accounts to Domain Controllers only.

Secure Remote Administration

- Use Remote Credential Guard
  - Protect privileged credentials when over RDP
  - Enables RDP connections without leaving credentials on target servers
  - Creds remain on the source machine, the target requests Service Tickets from the source machine as required


✓ Kerberos
✗ NTLM
✓ Access to services from server
✓ Prevent Pass-the-Hash
✓ Prevent use of credentials after disconnection

- Use Restricted Admin Mode
  - Protect privileged credentials over RDP, user logs in as local admin, as local host account
  - Solution for helpdesk support scenario
  - Remote user requires admin privilege on the endpoint

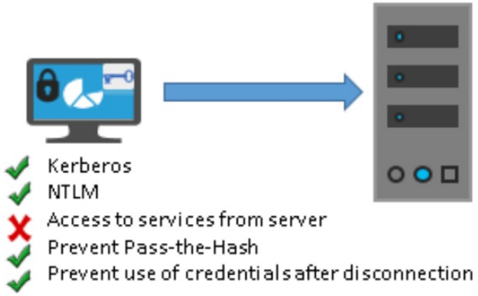

✓ Kerberos
✓ NTLM
✗ Access to services from server
✓ Prevent Pass-the-Hash
✓ Prevent use of credentials after disconnection

Image Credit: Microsoft

Harden Local Admin Account

- Common local admin password on systems is a big problem
- TA’s use these credentials for lateral movement
- Prepare and deploy Local Administrator Password Solution (LAPS)
  - Rotates passwords auto-magically ☺, stores them in “ms-Mcs-AdmPwd” attribute in clear text on DC
  - Ensure correct Discretionary Access Control List (DACL) for the attribute in the domain Schema
- At time of incident:
- Limit user rights for “S-1-5-114: NT AUTHORITY\Local account and member of Administrators group”
  - Remote Login - SeDenyNetworkLogonRight, SeDenyRemoteInteractiveLogonRight
  - Other - SeDenyBatchLogonRight, SeDenyServiceLogonRight, SeDebugPrivilege

Prepare: Protect Local Security Authority (LSA)

- Prevent reading memory and code injection by non-protected processes – LSA Protection
  - Protected mode requires that any plug-in that is loaded into the LSA is digitally signed with a Microsoft signature
  - Audit mode can be used as to detect access or precursor to moving to protection
  - HKLM\SYSTEM\CurrentControlSet\Control\Lsa "RunAsPPL"=dword:00000001

- Credential guard: Isolate secrets by using Virtualization based security
  - Several hardware and software requirements
  - Ideally should be done in Preparation stage

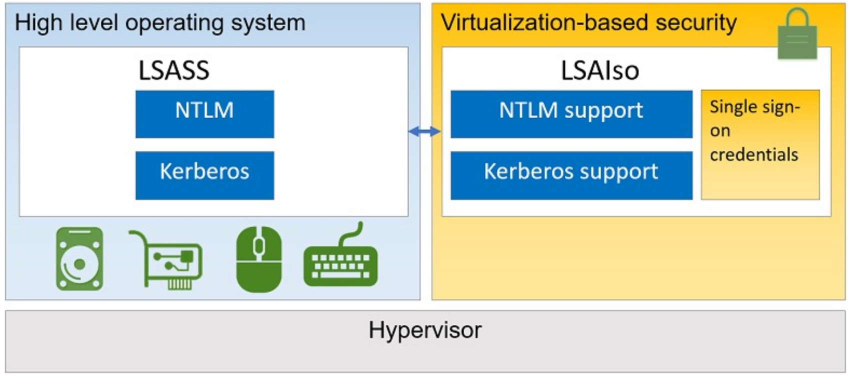

High level operating system
LSASS
NTLM
Kerberos
Virtualization-based security
LSAIso
NTLM support
Kerberos support
Single sign-on credentials
Hypervisor

Image Credit: Microsoft

Threat Actor Steals Data

FTP, sFTP

File Sync (MegaSync, rclone)

Remote Management (AnyDesk, TeamViewer)

Data Compression (zip, rar)

Data theft

- TA Compress’s data files
  - Compression utilities like 7zip, RAR, zip etc
- TA Exfiltrate’s data
  - Cloud Sync - MegaSync, pCloud
  - Data copy utilities - FTP, SFTP, Rclone, WinSCP to TA controlled infrastructure
  - Remote management - AnyDesk, TeamViewer, ScreenConnect etc.
- Detect & Disrupt data theft
  - Detect and respond to execution and installation of file sharing utilities like MegaSync
  - Detect and respond to compression of files, usage of rar, 7zip etc.
  - Implement Egress filtering rules at network level
  - Isolate systems

Threat Actor Destroys Backups

Secure backups

- Limit deletion of Volume shadow copies
- Secure your backups
  - Backup all critical systems required to run business
  - Protect backups against encryption/erasure
  - Backup on Un-Immutable storage – WORM (Write Once, Read Many)
  - Consider Offline Backups

Often it is easier and quicker to re-build from backups than to pay up and recover.

6

TA Moves Laterally
& Deploys
Ransomware

Ransomware Deployment/Lateral Movement

SMB Shares

PsExec

Remote Desktop Protocol

Windows Remote Management

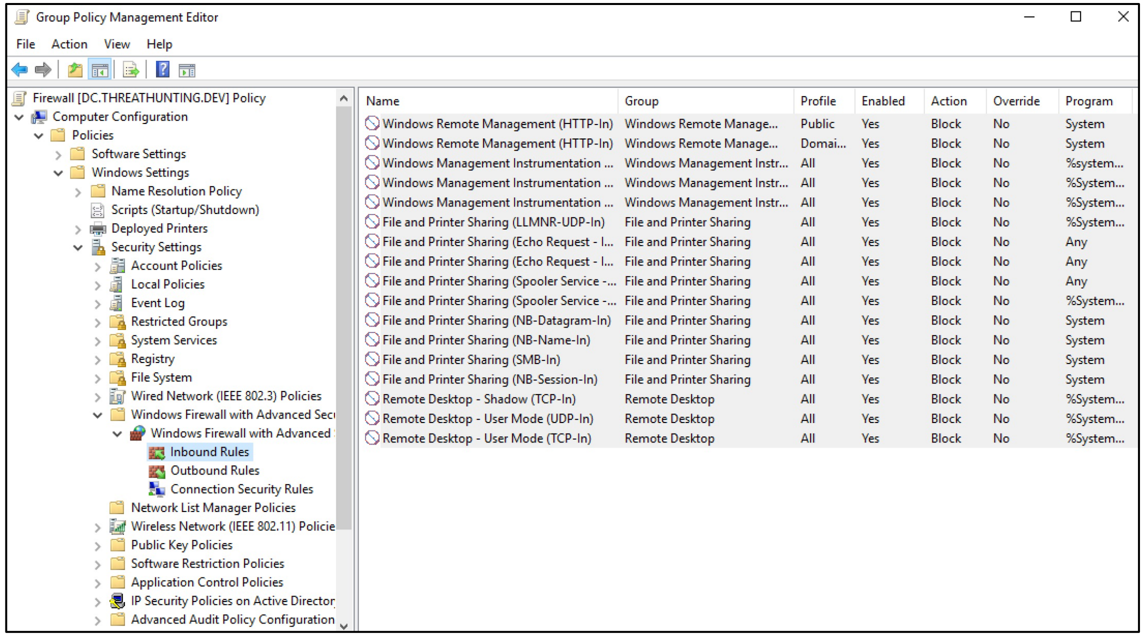
WMI

Group Policy

Segment Endpoints

- Use Local Host Firewall to limit opportunities for lateral movement
  - GPO to deploy Windows Firewall Policy
  - Create exceptions as needed

Protocol	Command Line
SMB tcp/445, tcp/139, tcp/135	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`
Remote Desktop Protocol tcp/3389	`netsh advfirewall firewall set rule group="Remote Desktop" new enable=no`
WMI tcp/153 + dynamic ports	`netsh advfirewall firewall set rule group="Windows Management Instrumentation (wmi)" new enable=no`
WinRM tcp/80, tcp/5985, tcp/5986	`netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no`



- Firewall [DC.THREATHUNTING.DEV] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Secu
            - Windows Firewall with Advanced
              - Inbound Rules
              - Outbound Rules
              - Connection Security Rules
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policie
          - Public Key Policies
          - Software Restriction Policies
          - Application Control Policies
          - IP Security Policies on Active Director
          - Advanced Audit Policy Configuration

Name	Group	Profile	Enabled	Action	Override	Program
Windows Remote Management (HTTP-In)	Windows Remote Manage...	Public	Yes	Block	No	System
Windows Remote Management (HTTP-In)	Windows Remote Manage...	Domai...	Yes	Block	No	System
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block	No	%system...
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block	No	%System...
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block	No	%System...
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block	No	%System...
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Block	No	Any
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Block	No	Any
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	Yes	Block	No	Any
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	Yes	Block	No	%System...
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block	No	System
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block	No	System
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block	No	System
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block	No	System
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block	No	%System...
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block	No	%System...
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block	No	%System...

Block PsExec & Likes

- Admin shares are used to move laterally and copy executables
- Disable Admin Shares using local commands or Group Policy

Disable LanManServer Service

```
sc stop "LanManServer”
sc config "lanManServer" start=disabled
```

Disable Shares using Registry

```
reg ADD
HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters
/v AutoShareWks/AutoShareServer /t REG_DWORD /d 0
```

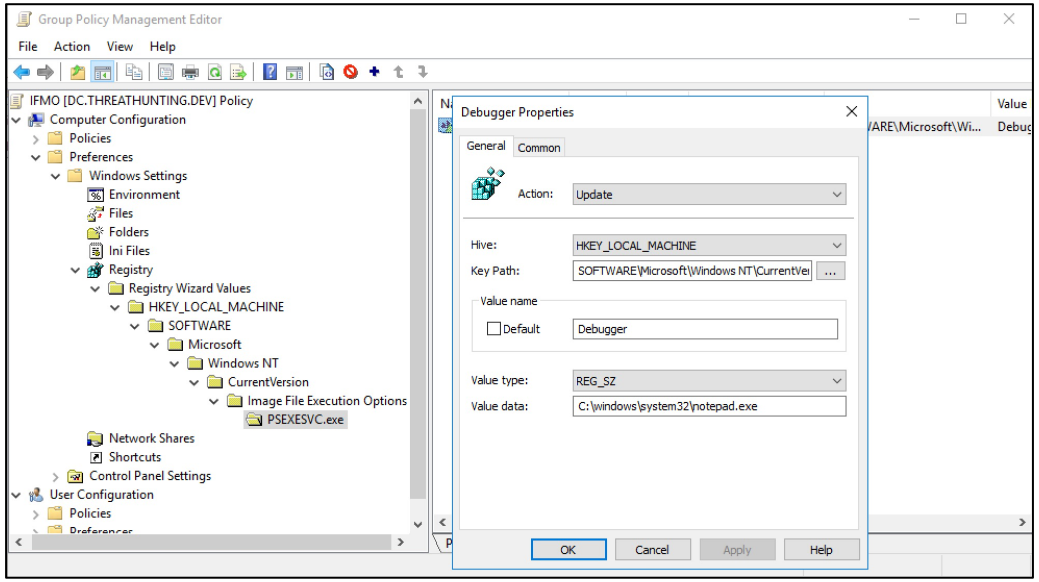
Create a fake PsExec Service

```
sc.exe create PSEXESVC start=disabled binpath=calc.exe
```

Disabling Admin & Hidden shares may impact availability of systems, exclude Domain Controllers.

Block PsExecSvc & other Executables

- Block named executables
  - Image File Execution Options (IFEO) are used for debugging
  - "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options”
  - Will result in execution of another configured executable
- Application Control
  - Best deployed as part of preparation
  - Effective control to enforce with default policies during the incident



Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SOFTWARE\Microsoft\Windows NT\CurrentVer

Value name

□ Default Debugger

Value type: REG_SZ

Value data: C:\windows\system32\notepad.exe

IFEO Configuration

Tools of the Trade

- Reconnaissance
  - adfind, Bloodhound, Powersploit, net.exe, nltest.exe, whoami.exe, ping.exe, Advanced IP Scanner, batch scripts, systeminfo.exe
- Credential Harvesting
  - Mimikatz, ProcDump, Ntdsutil, reg.exe
- Lateral Movement
  - WinRM, PowerShell, mstsc, PsExec, WMI
- Frameworks
  - Cobalt Strike, Metasploit, PowerShell Empire
- Remote Access
  - Anydesk, Teamviewer, ScreenConnect

Battle Ransomware

In midst of ransomware attack?

- Isolate key systems
- Isolate & Secure online Backup servers
- Isolate at-least one domain controller (preferable with the FSMO role)
- Ensure you know DSRM passwords
- Disrupt Threat Actor activity
- Crank-up protection on your endpoint security solution
  - Machine Learning, Protection Mechanisms, Behavioral Protection, host Firewalls

Ransomwared?

- Prepare: Create a policy on would you pay or not
- Talking to TA Operators:
  - Ransomware operators are often open to negotiations
  - Use a professional negotiation organization like Coveware
- Often it would be easier/less time consuming to recover from backup
- Even with decryptors, recovery is not instantaneous

Must do to protect against Ransomware

- Implement Multi Factor Authentication - **MFA** for **ALL** users on **ALL** external facing services
  - Remove non approved remote management tools
- Limit Privileged Access in your environment
  - Minimize accounts with domain privileges
    - Domain Admin is not the only privileged group
- Use Unique Local Admin Passwords
  - **Local Administrator Password Solution** is your BFF
- Patch Management is critical
  - **PATCH PATCH PATCH** devices, servers and clients
- Backups, offline or WORM

Thanks for listening!

🐦 @khannaanurag