



# Ransomware is Knocking your Door ! Proactive Hardening and Defense Strategies

Guillermo Diaz & Thirumalai Natarajan  
Security Transformation Services,  
Mandiant Consulting

# Thirumalai Natarajan

- Senior Manager – Consulting Services, Mandiant
- Responding & Remediating to Security Breaches
- Proactive Security Assessments
- Built & Managed Security Operations Centers
- Team Management & Business Development
- Speaker at Blackhat Asia, BSides SG, Virus Bulletin, SANS Summit etc.



# Guillermo Diaz

- Principal Consultant– Consulting Services, Mandiant
- Incident Response Remediation & Recovery
- Active Directory & Cloud Connoisseur
- Automate Everything
- Ex Microsoft
- Worked in South America, Middle East & Australia regions



# What will We talk about Today

- Ransomware Overview
- Ransomware Trends in 2021 from Mandiant cases
- Ransomware Attack Stages
- Defense Strategies to Harden the Security Posture
- Ransomware Remediation Stages
- Prepare for Enterprise Password Resets

# Ransomware Overview

# Ransomware is Evolving...

- Ransomware is not what it used to be!
- The term 'ransomware' traditionally refers to the malware used for encrypting files and entire systems
- Evolved to indicate a category of financially-motivated attacks
- Leverage extortion tactics to coerce victims into complying with demands
- 'Multifaceted extortion' is a term starting to gain traction when discussing ransomware
- Ransomware as a Service (RaaS)



ransomware

[ ran-suh m-wair ]

*noun*

- 1 malware that requires the victim to pay a ransom to access encrypted files

*Examples: Ryuk, Conti, BitPaymer, DoppelPaymer, Maze, etc.*



extortion

[ ik-stawr-shuhn ]

*noun*

- 1 the practice of obtaining something, especially money, through force or threats.

*Example: The theft of data and demand for money in exchange for not publicly releasing the stolen data*

# Evolution of Ransomware to Multifaceted Extortion

- Mainstream ransomware emerged in 2013
- Began affecting a limited number of systems
- Morphed over time to impact entire organizations
- Sophisticated actors perform targeted attacks
- Human driven attacks delete backups and encrypt host infrastructure, reducing the chance of recovery
- Ransomware as a Service (RaaS) lowers entry bar for less sophisticated actors
- Multifaceted tactics become more widespread
- Demanding payment with the promise not to release data to the public



**Manual deployment** by an attacker **after** they have penetrated an environment and have administrator-level privileges broadly across the environment.

# 2021 Ransomware Trends from Mandiant Cases

- **21 Days** – Average downtime experienced from a ransomware attack
- The median number of days between initial compromise and ransomware deployment was **7 days**; approximately a quarter of ransomware incidents occurred within **1 day** of initial attacker access.
- More than **85 percent** of ransomware deployments occurred outside normal business hours, and **55 percent** of incidents occurred between Thursday and Saturday.
- In post-compromise ransomware incidents that Mandiant responded to in 2021, actors demanded a range of ransom fees starting at \$44,999 USD and climbing to \$20 million USD, with an average ransom demand of nearly **\$4 million USD**.



# Gaining Initial Access

Method
Phishing
Exploiting vulnerable firewall, VPN appliances , Exchange Service, Web Servers
Poorly configured internet facing services
Credential stuffing and password spraying

# Multifactor Authentication (MFA)

MFA Types	MFA Enforcement	MFA Monitoring
<ul style="list-style-type: none"><li>• <b>App Codes</b><ul style="list-style-type: none"><li>• Hard / Soft Token based OTP</li></ul></li><li>• <b>App Notification</b><ul style="list-style-type: none"><li>• "Push Notification"</li></ul></li><li>• <b>SMS / Phone Call</b></li><li>• <b>Security Keys</b><ul style="list-style-type: none"><li>• External FIDO2 key</li><li>• Built-in key</li><li>• Apple / Android TouchID, Windows Hello</li></ul></li></ul>	<ul style="list-style-type: none"><li>• <b>External Access</b><ul style="list-style-type: none"><li>• Portals (OWA / SSO)</li><li>• VPN</li><li>• Vendors</li><li>• Remote Access Gateways</li></ul></li><li>• <b>Internal Access</b><ul style="list-style-type: none"><li>• RDP</li><li>• Jump Boxes</li><li>• Interactive Logon</li><li>• Applications</li></ul></li></ul>	<ul style="list-style-type: none"><li>• <b>Device Registrations</b></li><li>• <b>Token Issuance</b></li><li>• <b>Failure Mode</b></li><li>• <b>Admin Access</b></li></ul>

# MFA Methods

- **MFA Methods Most Susceptible to Phishing (Session Cookie Theft)**

- SMS
- Phone Call
- Push Notifications



**Risk:** Users accepting push notifications & validating malicious sessions

- **Why is FIDO2 / WebAuthN Effective Against Phishing Attacks?**

- The WebAuthN Client (browser) compares the domain name with the Relying Party Identifier (RP ID) of the public keys in the FIDO2 security key.
- If a domain string matches, it can be used as a method to authenticate.
- Spoofed domain = **No Match** for authentication (even if a user attempts to authenticate using the FIDO2 device)

# Password Policies

Policy	Account Type		
	Standard User	Privileged User	Service Account
Account Lockout Duration	30 minutes	0 (indefinite)	0 (indefinite)
Account Lockout Threshold	10 attempts	5 attempts	5 attempts
Enforce Password history	24 passwords	24 passwords	24 passwords
Maximum Password Age	90 days	60 days	120 days
Minimum Password Age	1 day	1 day	1 day
Minimum Password Length	15 characters	20 characters	30 characters
Complexity	Enabled	Enabled	Enabled
Reset Lockout Counter After	30 minutes	30 minutes	30 minutes
Reversible Encryption	Disabled	Disabled	Disabled

## Existing Password Policies

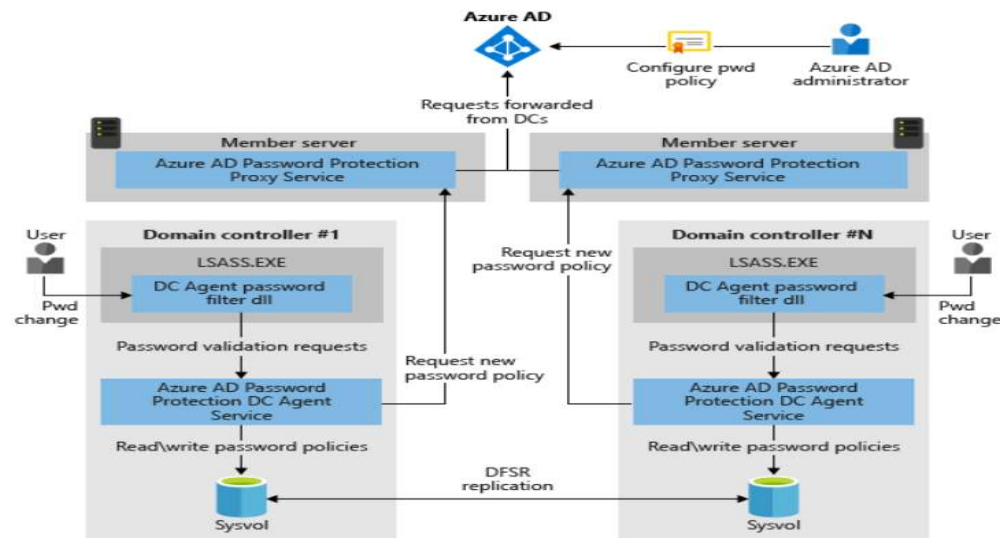
- Single Password Policy
- Multiple Password Policies

## Fine Grained Password Policy

- Privileged Accounts
- Service Accounts

# Password Protection

- Enforce Password Protections by filtering common and weak passwords
- Maintain custom banned password lists
- Eliminate Weak Passwords in the cloud and on-prem
- Azure AD Password Protection detects, and blocks known weak passwords and their variants and can also block additional weak terms that are specific to your organization.



<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

# Office Hardening

## Macro Restrictions

- Block macros in files from internet

## Trust Center Hardening

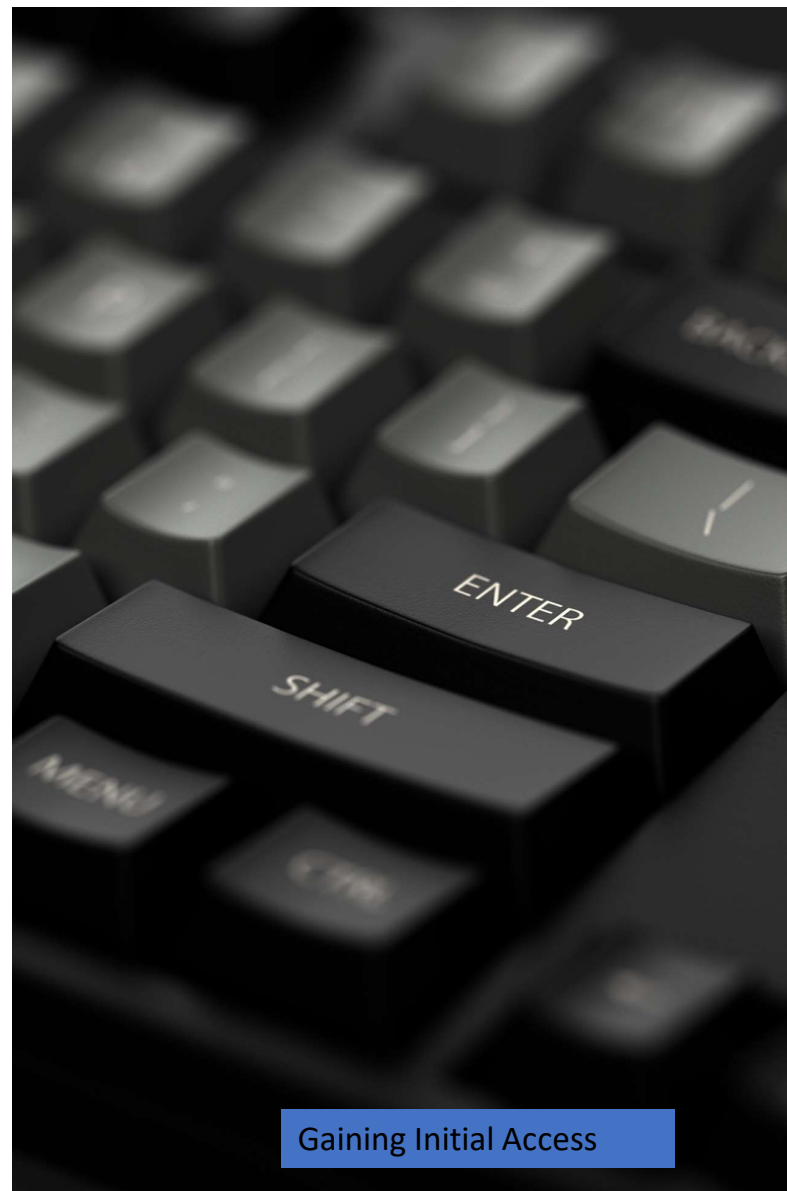
- Dynamic Data Exchange (DDE)
  - Security Advisory 4053440
- Trusted Documents
- Trusted Locations
- File Block Settings
- Protected View
- Automatic Links

## Object Linking and Embedding (OLE)

- Block additional file extensions for OLE Embedding (ex: py;rb)
- OLE package activation behaviors
  - No prompt, Object will not execute

## Legacy File Blocking

- Block “old” MS Office file formats



# Additional Defense Controls

- External scanning to identify open administrative ports
- Educate users awareness and Conduct Phishing Simulation exercise
- Robust Patching process
- Sandboxing Attachments and Web Links in the emails
- Harden perimeter device configuration

# Credential Harvesting

Method
LSA Process Dump
Extracting NTDS.DIT
Kerberos Ticket Dumping
Extracting Passwords from browser
Kerberoasting
Azure AD Connect, ADFS , ADCS compromise

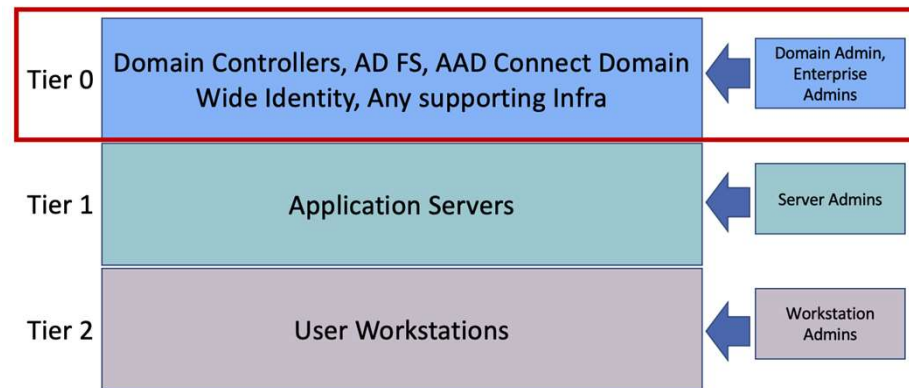


# Tiered Admin Model

- Objective = **prevent Credential harvesting and privilege escalation in AD**
- Reduce the exposure of privileged credentials amongst tiers
- Accounts of a lower tier should not be able to control systems, applications, or other accounts in a higher tier (and vice versa)
- Auth Policies / Silos, user rights Assignment Settings

## Tier 0 Definition

Tier 0 assets are the accounts, groups or other assets that have direct or indirect administrative control over the AD forest & domain, AD domain controllers, PKI, Identity or that have a direct or indirect administrative control over other assets that do.



# Credentials Protections in Endpoints

## Credentials Stored in memory

- Interactive Logon
  - Remote Desktop (RDP) Logon
  - PSEXEC *with explicit credentials*
  - Batch logon (scheduled tasks)
  - Running Services
  - RunAs (New Credentials)
  - PowerShell Remoting w/ CredSSP
- 
- ✓ Memory (LSASS process)
  - ✓ Local Accounts in SAM Database
  - ✓ Cached Credentials in Registry

## Credentials Protection

- **WDigest Authentication**
  - GPO – “MS Security Guide” ADMX template or registry key: requires KB2871997 (released in 2014)
  - Default disabled in Windows 8.1 / 2012R2 (and higher)
- **Windows Credential Manager**
  - Disable and Enforce in GPO
- **"TokenLeakDetectDelaySecs" registry key**
  - Clears credentials of logged off users after **30 seconds**, mimicking the behavior of Windows 8.1 / 2012R2 (and higher)

# Credentials Protections in Endpoints

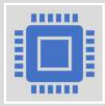
## LSA Protection

- LSA Protection for LSASS
  - Signature Verification
  - MSFT SDLC adherence
  - Prevents Reading Memory and Code Injections in LSASS
- Windows 8.1 / 2012R2 (and higher)
- Enabled w/ "RunAsPPL" registry key
- Audit Mode : Trigger Events

## Credential Guard

- Virtualization-based isolation technology for LSASS which prevents attackers from stealing credentials
- Splits Local Security Authority Subsystem Service to two processes:
  - the normal LSA process
  - The isolated LSA process (which runs in VSM = Lsalso.exe).
- Tools that recover secrets from LSA not able to access the isolated LSA process
- Windows 10 / Server 2016
- Virtual Secure Mode (VSM)

# Restricted Admin RDP



Limits in-memory exposure of admin credentials on destination endpoint accessed using the Remote Desktop Protocol (RDP)

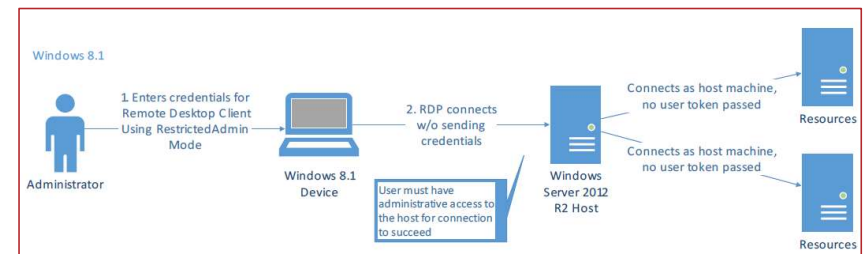


Authenticating account must be **administrator** on destination



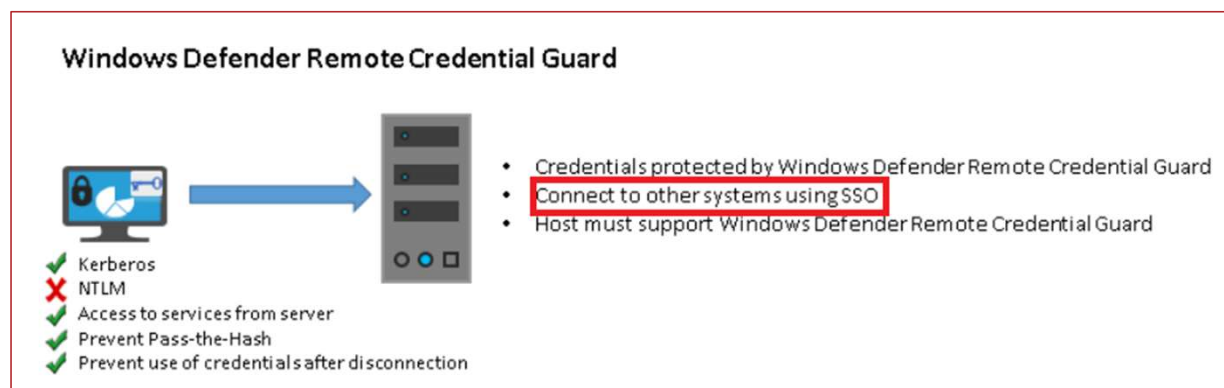
Credential user account not stored in memory; rather **the context of the user account appears as the destination machine account** (domain\destination-computer\$).

## Protected Users Group must use Restricted Admin RDP



**Client Mode (Source) - Windows 7 or Windows Server 2008 R2 (and above)**  
**Server Mode (Destination) - Windows 8.1 or Windows Server 2012 R2 (and above)**

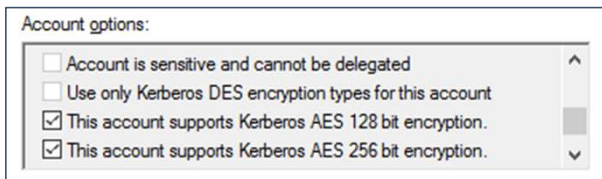
# Remote Credential Guard



- With Remote **Credential Guard**, all credentials remain on the client (origination system) – and are not directly exposed to the destination endpoint. Instead, the credentials remain on the source endpoint - and the destination endpoint requests Service Tickets from the source as needed

# Service Principal Name Hardening

- Ensure that accounts assigned an SPN have complex / hardened passwords (which cannot be easily cracked or brute-forced)
- Configure service accounts to support AES 128-bit / AES 256-bit encryption
- If AES is enabled on the KRBTGT account and TGTs are still issued with RC4 encryption – ensure the KRBTGT account's password was changed after DFL upgrade to 2008+.



DFL is 2008 or higher, the KRBTGT account will always default to AES encryption. For all other account types (user and computer) the selected encryption type is determined by the *msDS-SupportedEncryptionTypes* attribute on the account

# Privilege Escalations

## Method

Privileged Credentials/Tickets - Pass the Hash/Pass the Ticket

Abusing Delegations

Vulnerability exploitation- Zero logon, NTLM relay Attacks

Abuse SANS attribute in Certificates

DS Replication Permissions

Stealing Token Signing certificate from ADFS

# Limit identities with Privileges in Domain Controller

## Admin SD Holder Container

### Privileged Groups

- Schema Admins
- Enterprise Admins
- Domain Admins
- Administrators
- Account Operators
- Backup Operators
- Cert Publishers
- DNS Admins
- Printer Operators
- Server Operators
- Organization Management

- AdminSDHolder is an object in Active Directory to provide “template” permissions for protected accounts and groups.
- Security Descriptor Propagator (SDProp) is a process to apply this ACL template to all “protected groups”

### Built-in Privileged Accounts

- DSRM Administrator
- Administrator(RID 500)
- KRBTGT

### Privileges defined through GPOs

- Restricted Groups
- User rights Assignment Settings

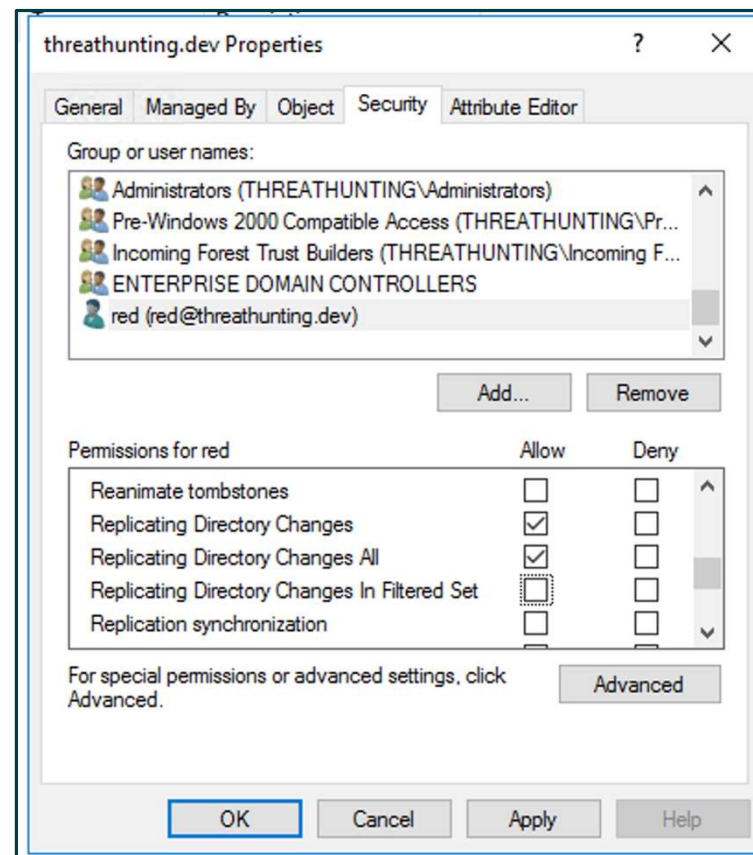


# DS Replication permissions

- Combination of two permissions:  
DS-Replication-Get-Changes  
DS-Replication-Get-Changes-All
- Allows a principal to remotely retrieve NT hashes via the MS-DRSR protocol for any security principal
- Review Identities with this permissions

Roles that (by default) that have these permissions:

- Domain Controllers
- BUILTIN\Administrators (DCs)
- Domain Admins
- Enterprise Admins
- AD DS Connector account (eg. MSOL\_ )



# Protected Users Group

Add all the privileged user accounts to the protected User groups

## Automated Protections

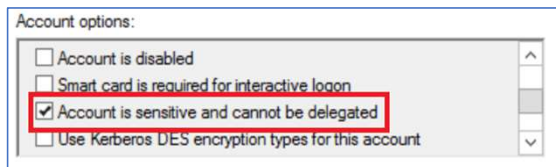
- Kerberos ticket granting ticket (TGT) expires after 4 hours
- Cached credentials are blocked
  - DC must be available to authenticate the account
- Plaintext passwords are not cached for
  - Windows Digest authentication or
  - default credential delegation (CredSSP)
- NTLM one-way function (NTOWF) is blocked.
- Kerberos pre-authentication (Server 2012 R2 or higher)
  - DES and RC4 not used
  - AES encryption enforced
- Accounts cannot be used for
  - constrained or unconstrained delegation
- Requires Domain Functional Level 2012R2

Guest	User	Built-in account for guest access to t
krbtgt	User	Key Distribution Center Service Acco
Protected Users	Security Group...	Members of this group are afforded a
RAS and IAS Servers	Security Group...	Servers in this group can access reme

# Hardening Kerberos Delegation

## 1. "Account is sensitive and cannot be delegated"

- Configure this for the privileged accounts

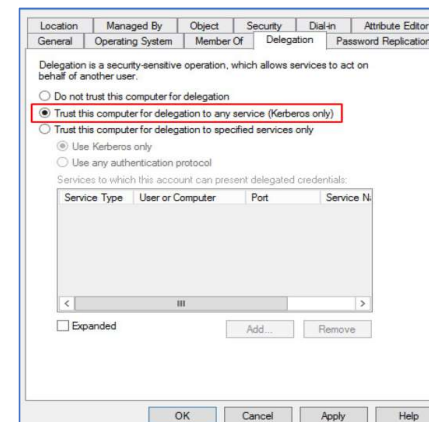


## 2. "Enable computer and user accounts to be trusted for delegation user right" (GPO)

- Determines which users can set the Trusted for Delegation setting (SeEnableDelegationPrivilege) on a user or computer object

## 3. Disable TGTDelegation across two-way trust links

## 4. Don't enable Unconstrained delegations



# Service Accounts Hardening

## Restrict logon capabilities

- Deny log on through Remote Desktop
- Deny log access to this computer from the network
- Deny log on locally

## Restrict logon to specific hosts in AD Users & Computers

- Logon Workstations Setting

## Standard Managed Service Accounts (MSA)

- Account is associated with a single endpoint
- Set with a complex (120 character) password managed and changed on a pre-defined frequency (30 days by default)

## Group Managed Service Accounts (gMSA)

- Introduced with Windows Server 2012
- gMSAs are very similar to MSAs, but they allow for a single MSA to be leveraged across multiple endpoints.

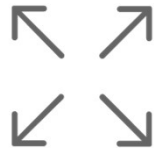
# Lateral Movements / Ransomware Deployment

Method
Deploying Ransomware through GPO
Remote Executions – PSEXEC, SC.exe, WMI, Powershell
Lateral movement through SMB, WinRM
Local Admin account
Schedule task
Compromising SCCM or WSUS servers

# Network Segmentation

## • Identity / Trust

- 802.1x and related
- VPN Authentication
- IP Address
- MAC Address



## • Visibility

- NetFlow
- ACL / FW / Proxy Logging
- Endpoint Agent Logging

Protect critical intellectual property from unauthorized applications or users

## • Isolation

- Physical topology
- VLANs, WLANs & PVLANS
- VRFs, MPLS VPN
- GRE / IPSec / DMVPN



## • Policy Enforcement

- Firewall technologies
- Access Lists (ACL's)
- Intrusion Prevention Systems

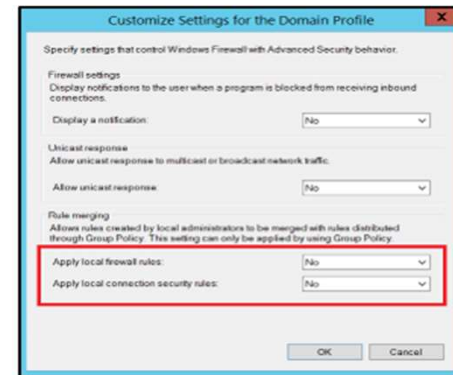
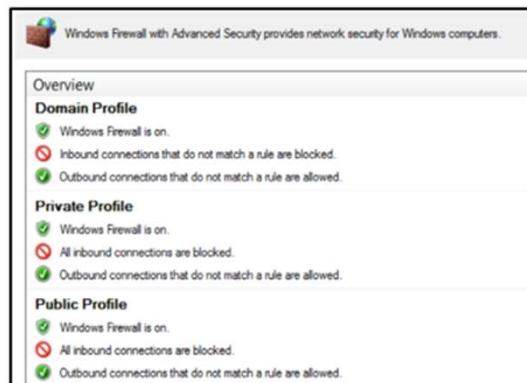
Prevent lateral movement throughout the network

# Harden Lateral Paths – Between Endpoints

- Block inbound access to systems using Windows Firewall or 3<sup>rd</sup> Party Endpoint technology (e.g., AV)
  - SMB (TCP/445, TCP/135, TCP/139)
  - Remote Desktop Protocol (TCP/3389)
  - Windows Remote Management / Remote PowerShell (TCP/80, TCP/5985, TCP/5986)
  - WMI (dynamic port range assigned through DCOM)

```
netfirewall set rule group="remote desktop" new enable=Yes
netsh advfirewall firewall tsh advfirewall set rule group="File and Printer Sharing" new enable=Yes
```

Protocol / Port	Windows Firewall Rule	Command Line Enforcement
SMB	Predefined Rule: <ul style="list-style-type: none"> <li>File and Print Sharing</li> </ul>	<code>netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no</code>
TCP/445, TCP/139, TCP/135		
Remote Desktop Protocol	Predefined Rule: <ul style="list-style-type: none"> <li>Remote Desktop</li> </ul>	<code>netsh advfirewall firewall set rule group="Remote Desktop" new enable=no</code>
TCP/3389		
WMI	Predefined Rule: <ul style="list-style-type: none"> <li>Windows Management Instrumentation (WMI)</li> </ul>	<code>netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no</code>
Windows Remote Management / PowerShell Remoting	Predefined Rule: <ul style="list-style-type: none"> <li>Windows Remote Management</li> <li>Windows Remote Management (Compatibility)</li> </ul> Port Rule: <ul style="list-style-type: none"> <li>5986</li> </ul>	Via PowerShell: <code>Disable-PSRemoting -Force</code>
TCP/80, TCP/5985, TCP/5986		



# Disable Admin/Hidden Shares

Common administrative and hidden shares on endpoints include:

- ADMIN\$
- C\$
- D\$
- IPC\$



Containment  
Action

## Group Policy:

Using the “MSS (Legacy)” Group Policy template, administrative and hidden shares can be disabled via a Group Policy setting (Figure 26).

- Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareServer)
  - Disabled
- Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareWks)
  - Disabled

Setting	State	Comment
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Not configured	No
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended e...	Not configured	No
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure envi...	Disabled	No
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure enviro...	Disabled	No



# Harden Local Admin Account

## Local Administrator Password Solution

- Unique password for the built-in administrator or custom account for each computer object
- Password is randomly generated on a defined interval (30-days etc.)
- Password is stored within AD for each computer object
  - ms-Mcs-AdmPwd
- Password is securely transmitted to endpoints via AES encryption and Kerberos v5 protocol

## Limit Local Admin account for lateral movement



Containment  
Action

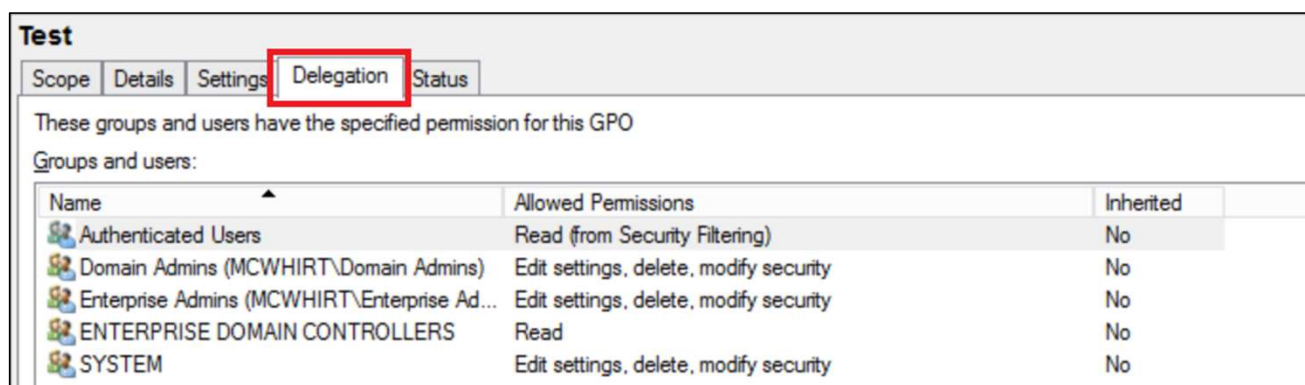
- To mitigate the usage of local administrative accounts from being used for lateral movement, utilize the SID "S-1-5-114: NT AUTHORITY\Local account and member of Administrators group" within the following settings:

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment

- Deny access to this computer from the network (SeDenyNetworkLogonRight)
- Deny log on as a batch job (SeDenyBatchLogonRight)
- Deny log on as a service (SeDenyServiceLogonRight)
- Deny log on through Terminal Services (SeDenyRemoteInteractiveLogonRight)
- Debug Programs (SeDebugPrivilege – permission used for attempted privilege escalation and process injection)

# Review Group Policy Objects Edit Permissions

- Review and Remove standard groups and accounts that were configured with edit permissions for various GPOs in Domain controller



Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (MCWHIRT\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (MCWHIRT\Enterprise Ad...	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

```
PS> $GPOPermissions = Foreach ($GPO in (Get-GPO -All )) { Foreach ($GPOPermissions  
in (Get-GPPermissions $GPO.DisplayName -All )) { New-Object PSObject -property  
@{GPO=$GPO.DisplayName;Users=$GPOPermissions.Trustee.Name;Permission=$GPOPermission  
s.Permission} } }  
PS> $GPOPermissions | Select GPO,Users,Permission
```

# Destroy Backups

Method
Delete Volume Shadow copy
Destroy VM Snapshots
Abusing Backup Software APIs
Delete Cloud storage files

# Protect Backups from Ransomware encryption

Ransomware operators often encrypt and destroy all organization's backups before launching their attack. This increases the likelihood that an organization will pay the ransom.

Create backup standards that includes,

- Implement immutable backups to prevent unauthorized access to, deletion and encryption
- Follow the 3-2-1 backup strategy. This means storing three copies of data, on two devices, and one offsite.
- Maintain at least one copy of offline storage
- Continue using Backup encryption at-rest and in-transit where applicable
- Consider increasing the backup retention policy
- Require MFA for backup deletion requests and access requests
- Segmenting backup servers and restricting both inbound and outbound network traffic
- Ensure that backup administrator related passwords are unique and strong by storing them in a privileged access management solution

# Monitoring Backup Operations – Use Case & Playbook

Create alerts to indicate an attacker or malicious insider tampering with backups.

- Mass deletion of backups or metadata
- Deletion of Volume Shadow copies
- Failed backup jobs
- Unexpected configuration changes in Backup Servers
- Deletion of VM Snapshots
- Unauthorized access attempts to backup servers
- Critical backup services stopped
- PowerShell with command line win32\_shadowcopy
- leveraging native Windows utilities by adversaries to disable or delete system recovery features like vssadmin.exe, bcdedit.exe, wbadmin.exe, wmic shadow
  - Wmic.exe with command line shadowcopy delete
  - Vssadmin.exe with command line resize shadowstorage
- Cloud Storage deletion activities

# Disable OneDrive synchronization



Containment  
Action

Disable OneDrive synchronization on endpoints to minimize the impact of encrypted files and ransom notes being automatically synced to OneDrive cloud storage

Block OneDrive file syncing to a specific Tenant ID of the impacted organization:

- Step 1 :Computer Configuration > Policies > Administrative Templates > OneDrive > Allow syncing
  - OneDrive accounts for only specific organizations
  - Disabled | Not Configured
- Step 2 : Computer Configuration > Policies > Administrative Templates > OneDrive > Block syncing
  - OneDrive accounts for specific organizations
  - Enabled
  - Specify a TenantID for blocking synchronization
- The TenantID can be found in the Directory ID box of the Properties page in Azure Active Directory

# Ransomware Recovery Validation

Recovery Detailed Configuration Design Documents

Purchase Cyber Security Insurance

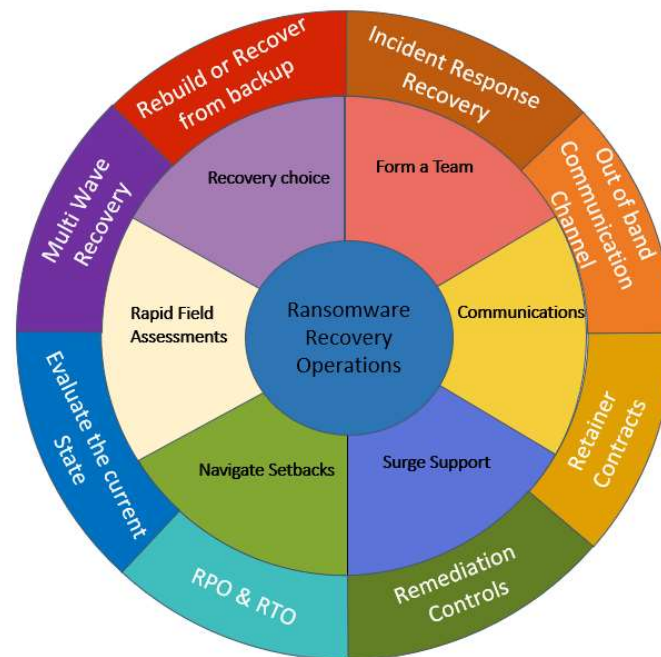
Purchase a Cyber Security Retainer

Robust Ransomware Recovery Plan

Regular Testing of Recovery Plan

Ransomware Recovery Playbook

Develop Communications Plan



GAIN CONTROL

>

ORGANIZE

>

RAPID FIELD  
ASSESSMENT

>

ENVIRONMENT  
RECOVERY

# Data Exfiltration

Method
Cloud Sync- MegaSync, OneDrive, DropBox, pCloud
Microsoft BITS
Remote Management Solutions – AnyDesk, TeamViewer
FTP, SFTP, RoboCopy services



# Defense & Detection – Data Exfiltration

- Robust Monitoring of egress traffic that includes transfer rate/ upload size
- Enable and Monitor Net Flow Logs
- Identify crown jewel data and enable stringent defense controls
- Data classification and leakage prevention (DLP Solution)
- Prevent execution and installation of file sharing utilities megaSync, pCloud
- Block Remote Management Solutions such as anydesk, teamviewer etc.

# Ransomware Remediation Stages

# Ransomware Remediation Stages

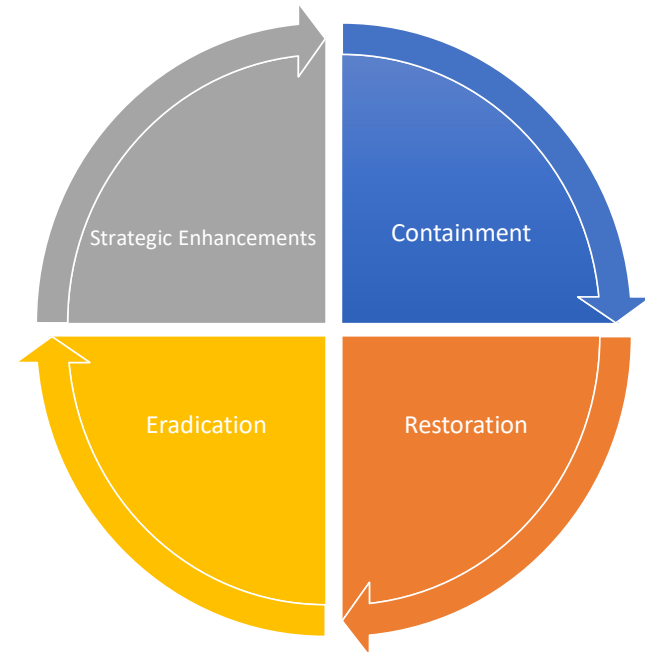
The four phases of remediation are organized in two parts:

## Part 1 - Remediate the current incident

1. **Containment** - Take actions to disrupt attacker activities, monitor, harden and remove the attacker from a sensitive system or network segment to regain control of the affected environment.
2. **Restoration** - Take actions to restore encrypted endpoints, applications, and services, to reestablish business functionalities.
3. **Eradication** - Remove an attacker from the environment and implement security improvements to inhibit the attacker from quickly regaining access to the environment. Should be performed in a concise and coordinated manner hour window.

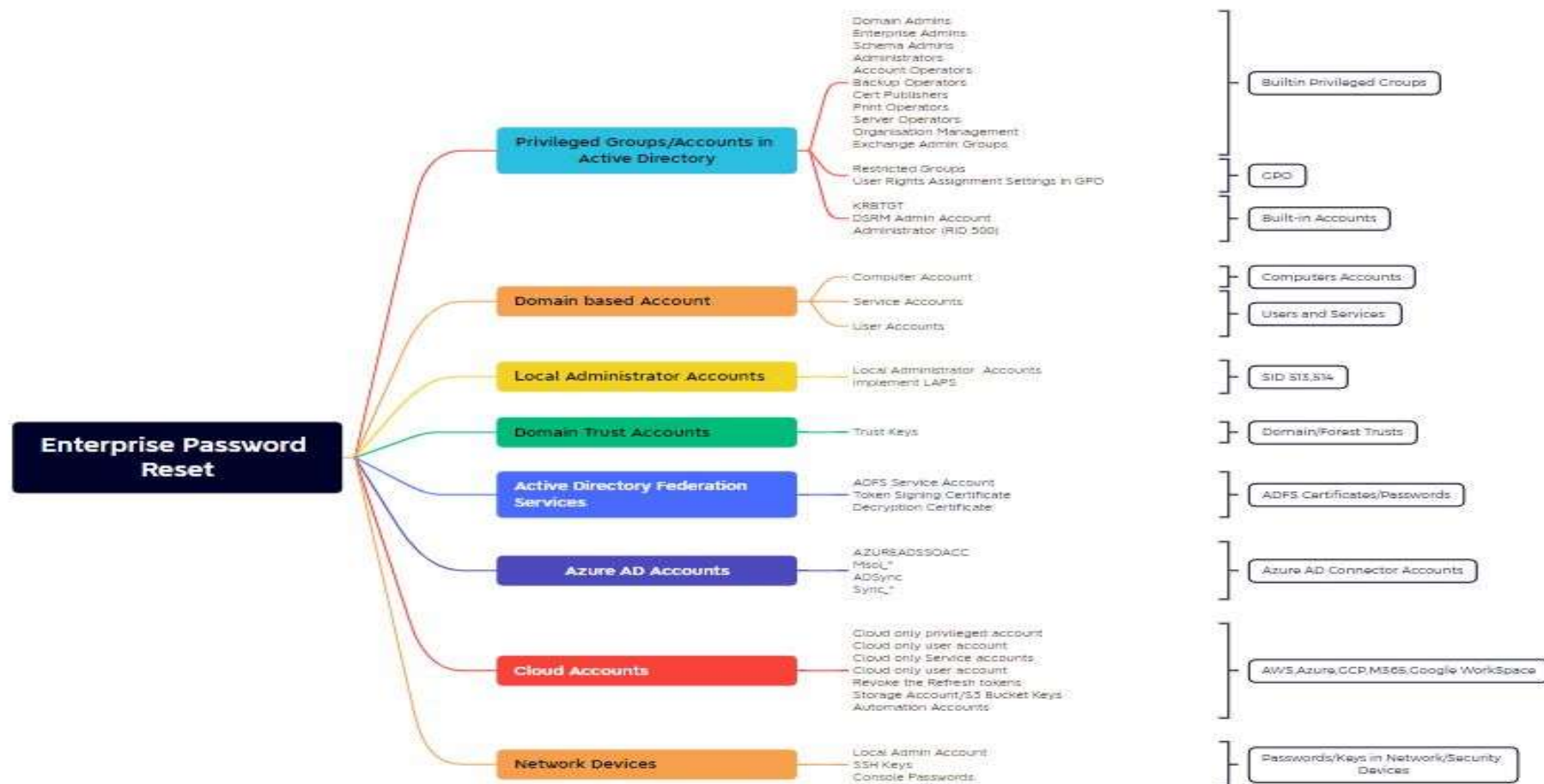
## Part 2 - Improve the organization's security posture

4. **Security Enhancement** - Enhance the security posture of the organization (e.g., process improvements, privileged account management, network re-architecture)



# Prepare for Enterprise Password Resets

# Prepare for the Enterprise Password Reset



# Thanks for Listening !

**Thirumalai Natarajan**

 @Th1ruM

 [www.linkedin.com/in/thirumalainatarajan](https://www.linkedin.com/in/thirumalainatarajan)

**Guillermo Diaz**

 [www.linkedin.com/in/gmodiaz/](https://www.linkedin.com/in/gmodiaz/)