REMEDIATION CHECKLIST

for Cyber Security Incidents

Authors:

Lucas van den Berg TR-NL
Matthias Schönhofer TS-DE
Trend Micro EU-Incident Response Team

CONTENTS

1.0 PURPOSE AND SCOPE

This document was designed for urgent cyber security incidents including data theft, data encryption, ransomware and computer espionage.

- Chapter 2.0 contains quick how-to steps to technically limit the capability of a threat actor to further infiltrate and impact your IT environment.
- Chapter 3.0 contains organizational advice on how to handle the attack and further information on the nature of targeted attacks or similar events.
- Chapter 4.0 gives further technical explanations, if required.

DISCLAIMER:

Please note that the advice given in this document is not comprehensive but represents a Trend Micro selection of the most useful steps to counter a cyber attack in the very first phase of the attack.

Please note that some systems and applications, but also some Trend Micro product features, rely on the services proposed here to be limited or shut down. For example, Deep Security relies on WMI to function properly to determine the BIOS-UUID, which is the Unique identifier of the Deep Security Agent. In order to not interfere with certain security functionalities, make sure to apply the changes described in this document with great caution!

Please note that Trend Micro does not accept any responsibility for the consequences of any steps described in this document.

2.0 GENERAL INSTRUCTIONS

When breached it is important to perform the following three actions:

1. Harden your infrastructure.
2. Isolate breached systems.
3. Gain visibility.

2.1 INITIAL RANSOMWARE CHECKLIST

Use the following checklist to respond to the initial ransomware attack:

- Locate the impacted systems and isolate them.
  - □ It is advised to isolate systems via network isolation, preferably on hypervisor level or orchestrator level. This way you can easily enable or disable virtual switches and/or interfaces thus making the operation scalable.
  - □ If you do not have access to your virtual switch interfaces, locate the network cable and unplug the affected devices.
  - □ Only if you are unable to isolate the systems via the network you should power down the system. Powering down affected machines limits the possibilities for digital forensic analysis on the machine.
- Safe Communication.
  - □ After the initial compromise, Threat Actors may monitor your organization's activity and communications to understand if their actions have been detected.
  - □ Make sure you use out-of-band communication methods like Signal, Telegram or phone calls to avoid tipping off Threat Actors that they have been discovered and that mitigation actions are being undertaken.
- Identify Backups.
  - □ Keep track of systems and devices that are not perceived to be impacted so they can be prioritized for restoration and recovery.
- Information Management.
  - □ Together with your team, write a brief list with a rough timeline of events and what you know so far.
  - □ This will facilitate the handover to the Incident Response team.
- Inform your Trend Micro Account Team and await further instructions.

2.2 HARDENING YOUR INFRASTRUCTURE

- All the actions below can be performed via Group Policy Object (GPO).
- The measures below will have an impact on your operations and must be executed by IT professionals only.
- Please review chapter 4.0 for background and step-by-step guides to these suggestions.

High priority steps to be taken (please click on boxes to mark as done):

- □ Reset all administrative credentials.
- □ Remove local administrator rights from all user accounts.
- □ Reset all passwords for all users.
- □ Restrict use of PsExec.
- □ Restrict use of Powershell.
- □ Restrict use of WinRM.
- □ Restrict use of WMI.
- □ Restrict use of SMB.
- □ Restrict use of RDP.
- □ Disable Microsoft Office macros.
- □ Restrict administrative shares.
- □ Enable Powershell transcript logging.
- □ Reset the Kerberos golden tickets twice.
- □ Setup 2FA for all available applications and systems.
- □ Make use of a Privileged Access Management (PAM) solution like Microsoft LAPS.

Secondary steps to be taken (please click on boxes to mark as done):

- □ Check Group Policies / Group Policy Objects of domain controllers and identify any that should not be there, or any that have been modified.
- □ Check for account misuse.
- □ Patch all systems.
- □ Check public IP-space for exposed ports and vulnerabilities.
- □ Check Task Scheduler for unknown or suspicious tasks.
- □ Check for drives being shared that should not be, or should not exist.
- □ Configure at least 5GB of storage for Windows Event Logs.
- □ Enable the following event logs:
    - □ PowerShell Transcript Logs events.
    - □ Scheduled Tasks security events.
    - □ Failed login event logs on domain controllers.
    - □ File share auditing events.

2.3 ISOLATE SYSTEMS

When having multiple domains in your infrastructure it is important to start isolating presumably safe domains from the infected domains. This way you may stop the lateral movement of the Threat Actor.

2.4 GAIN VISIBILITY

If you are undergoing a ransomware attack or if you have the suspicion a Threat Actor is in the network, it is important to get an understanding of their complete network behaviour. Threat Actors will use unmonitored network ports and network protocols to gain persistence on the network and on servers or endpoints.

It is critical that Incident Response deploys a Deep Discovery Inspector (virtual) appliance in the network as soon as possible. This way Incident Response can monitor and analyse the east-west traffic (lateral movement) as well as north-south traffic.

A Trend Micro Incident Response analyst will analyse the recorded events and report them back to you at a set interval. It is pivotal that the analyst's alerts are being followed up upon continuously and with due dilligence since Incident Response needs to build a baseline of events happening in the infrastructure.

After the creation of the baseline, we can see anomalies happening on the network which might indicate Threat Actor behaviour.

The Trend Micro staff will assist with the deployment and configuration of the Deep Discovery Inspector network appliance.

3.0 ORGANIZATIONAL ISSUES

The present chapter addresses basic questions that will arise in the first hours of an incident and the organizational steps to be taken to react quickly.

3.1 WHAT IS RANSOMWARE?

Ransomware is a form of malware that is designed to block access to your servers and endpoints by encrypting the data present on these systems.

After encryption, a ransom note will be dropped on these systems wherein the Threat Actor will demand a ransom payment (usually in Bitcoin) in exchange for the decryption key.

In most cases the Threat Actor will also threaten to publicly disclose your data if you do not pay. The Threat Actor will usually publicize a small sub set of the stolen data on their website in order to prove that you have been breached.

3.2 COMMUNICATION WITH THE THREAT ACTOR (TA)

If you are suffering a ransomware attack, the TA's motivation is not espionage or sabotage, but financial gains. The TA will try to establish contact with you to negotiate a ransom payment.

Typically, the TA wants you to access a chat room or ransom blog site through the Tor browser, instructions on how to install and use Tor are typically given in the ransom note along with the TA blog site's address. This site typically features samples of the breached data and more information on how to communicate with the TA.

While Trend Micro IR cannot issue any direct advice on how to interact with the TA, it is not explicitly illegal to download the Tor browser and access the given site. It is common for affected companies to check the respected website via Tor browser to see if any further data has been published.

Please note that opening a password-protected ransom note may inform the TA and trigger an artificial countdown on the ransomware blog to put the ransomed company under pressure.

3.3 COMMUNICATION WITH LEGAL AUTHORITIES

Activities typically conducted by Threat Actors generally classify as criminal behaviour in nearly all jurisdictions and should be reported to legal authorities.

For EU based customers GDPR Art. 33 ("Notification of a personal data breach to the supervisory authority") states that *"(i)n the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."* (See further contents in Article 33.)

According to GDPR Art. 34, *"(w)hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."* (See further contents in Article 34.)

Further rules, laws and data regimes may apply in your region, please consult your legal council.

3.4 SHOULD I PAY IN CASE OF A RANSOMWARE ATTACK?

Most European Government CERTs advise companies not to pay the ransom:

- There is no guarantee that the key ("decryptor") of the encrypted files will actually be handed over to you after the payment of the requested ransom.
- Despite payment, the stolen data may have been sold on the Dark Net already.
- The TA may ask for an even higher ransom if you agree to paying the first

3.5 SINGLE POINT OF CONTACT & REACH OUT TO IR PROFESSIONALS

Trend Micro Incident Response professionals offer services that follow the cyclic Incident Response model as printed below. These IR services continue & complete your first steps in incident remediation and containment as outlined in this document.

It is therefore highly advisable to determine one single point of contact for communicating with Trend Micro Incident Response staff. This person should be knowledgeable about the structure of your network and have the authority to authorize actions for and by the IR team.

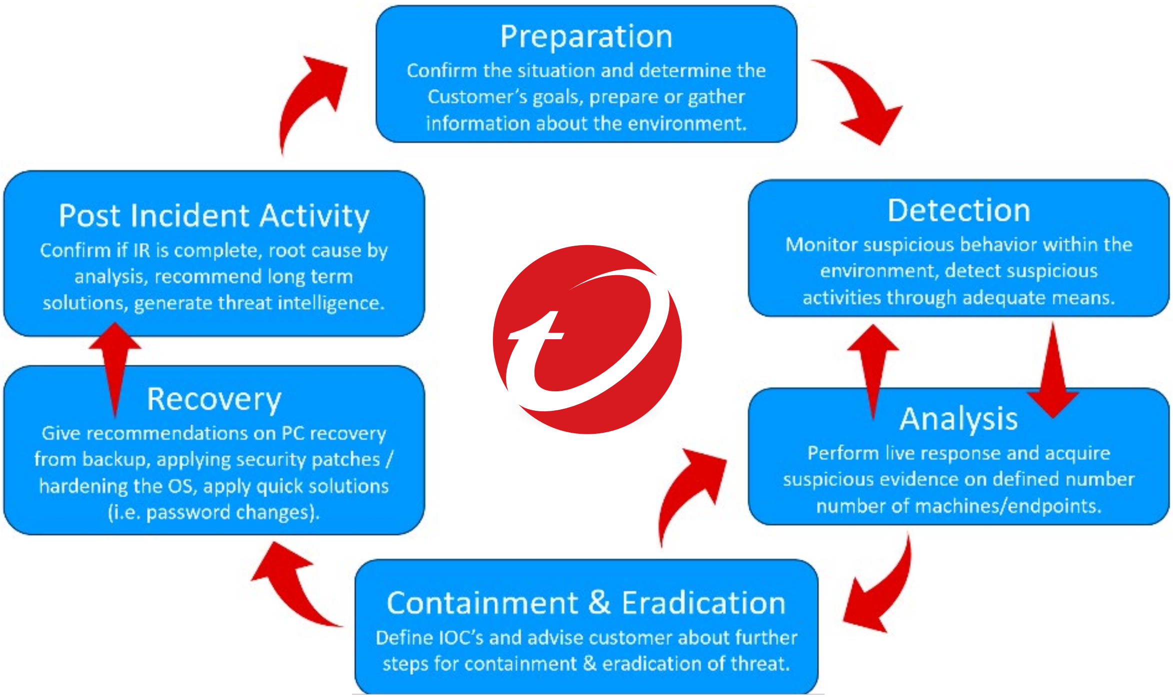

Preparation
Confirm the situation and determine the Customer's goals, prepare or gather information about the environment.
Detection
Monitor suspicious behavior within the environment, detect suspicious activities through adequate means.
Analysis
Perform live response and acquire suspicious evidence on defined number number of machines/endpoints.
Containment & Eradication
Define IOC's and advise customer about further steps for containment & eradication of threat.
Recovery
Give recommendations on PC recovery from backup, applying security patches / hardening the OS, apply quick solutions (i.e. password changes).
Post Incident Activity
Confirm if IR is complete, root cause by analysis, recommend long term solutions, generate threat intelligence.

Illustration: Cyclic incident response case model

4.0 TECHNICAL BACKGROUND

This chapter covers the technical background of the remediation points in chapter 2.0 above.

4.1 HARDENING YOUR INFRASTRUCTURE

A Threat Actor will use many different Tools, Tactics and Procedure's (TTP's) to gain persistence on your network and infrastructure.

The following tools are commonly used by Threat Actors for malicious intent. It is advised to restrict or disable the below tools, changing these settings will most likely impact your business operations and should therefore be reviewed carefully. It is important to conduct a further review of the configuration after the incident too.

We recommended the below tools to be disabled or restricted for at least endpoint-to-endpoint communication but preferably for all endpoints and servers unless specifically allowed on a per user basis:

- SMB (TCP/445, TCP/135, TCP/139).
    - The Server Message Block (SMB) protocol is a communication protocol for providing shared access to files and printers between endpoints and servers on a network.
- Remote Desktop Protocol (TCP/3389).
    - The Remote Desktop Protocol (RDP) is used to perform remote actions on endpoints or servers and to take over control of individual machines.
- Windows Remote Management / Remote PowerShell (TCP/80, TCP/5985, TCP/5986) WMI (dynamic port range assigned through DCOM).
    - Windows Remote Management (WRM), (remote) PowerShell and Windows Management Instrumentation (WMI) are used to perform administrative tasks on endpoints and servers, such as installing or uninstalling software.

Please see chapter 4.2 below for steps on how to perform these actions.

4.2 GENERAL HARDENING BY GROUP POLICY OBJECT (GPO)

When the endpoints and servers are part of a Windows Domain it is possible to deploy a Windows Firewall Policy to easily block multiple protocols:

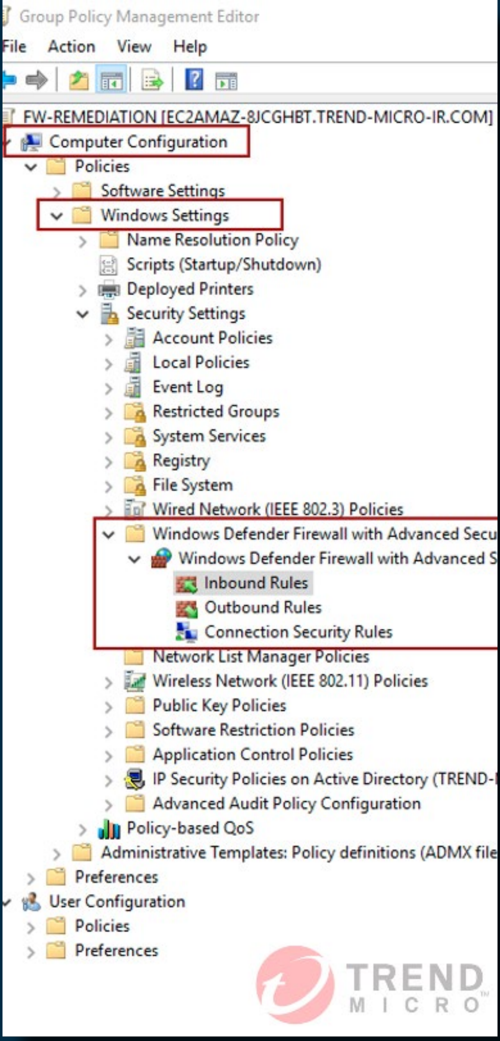
1. Limit the inbound endpoint or server traffic via the "Group Policy Management Editor":

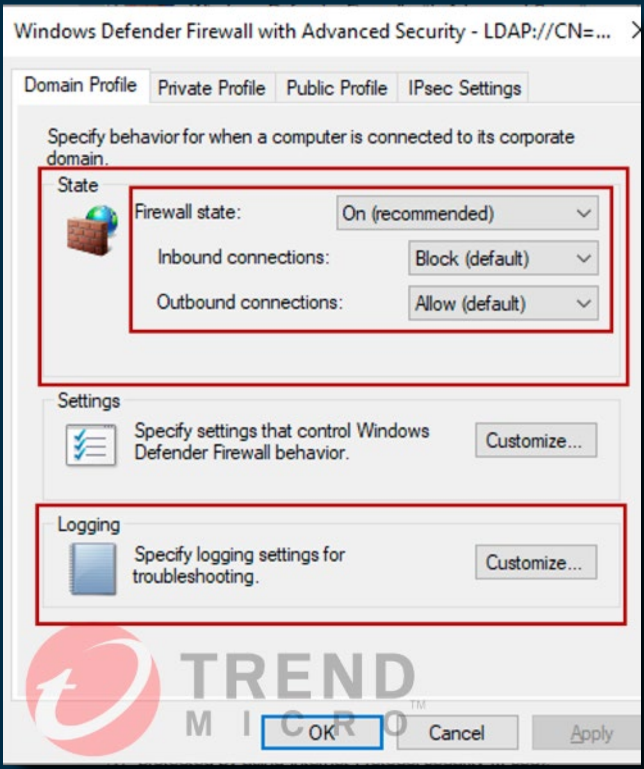
   a. Go to: "Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security".

   b. Right-click "Windows Defender Firewall with Advanced Security" and select "Properties".

   c. Set the Firewall state to "on" and configure the inbound connections to "block" and the outbound connections to "allow".

   d. Customize the Logging so it is enabled.


Group Policy Management Editor
File Action View Help
FW-REMEDIATION [EC2AMAZ-8JCGHBT.TREND-MICRO-IR.COM]
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 Defender Firewall with Advanced Secu
Windows Defender Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (TREND-
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX file
Preferences
User Configuration
Policies
Preferences
TREND MICRO


Windows Defender Firewall with Advanced Security - LDAP://CN=...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Settings

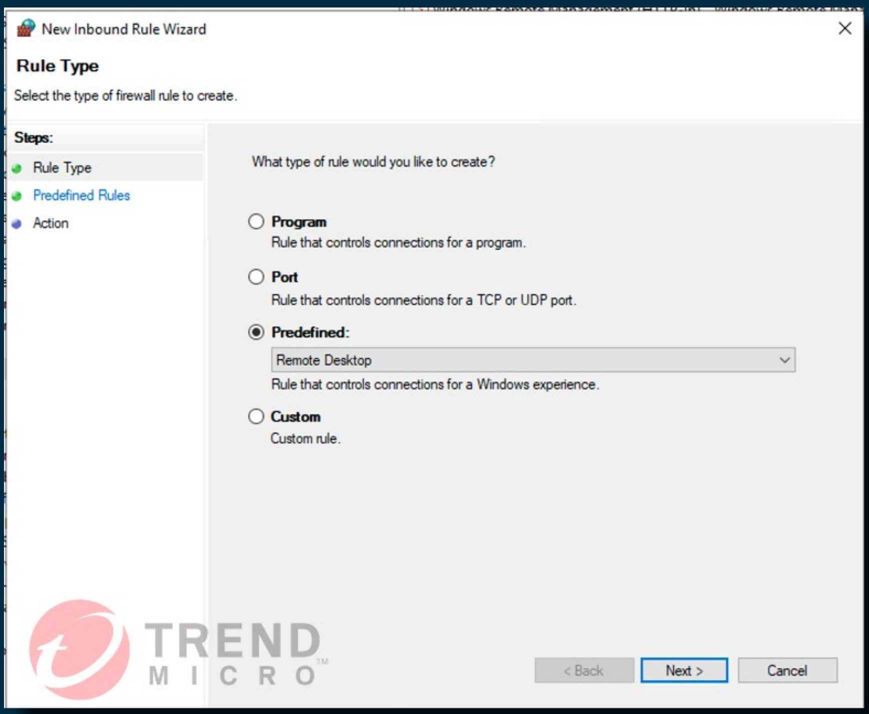
Specify settings that control Windows Defender Firewall behavior.

Logging

Specify logging settings for troubleshooting.

   e. Right-click "Inbound Rules" and select "New Rule..".

   f. Create a new inbound rule with a predefined filter.



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**
Remote Desktop
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

g. Configure the predefined filters with a block rule:

   I. File and Print Sharing.

   II. Remote Desktop.

   III. Windows Management Instrumentation (WMI).

   IV. Windows Remote Management.

   V. Windows Remote Management (Compatibility).

h. Configure a block port rule for: TCP/80, TCP/5985, TCP/5986.

i. Push the newly made policy to all endpoints and servers but remember this will have an operational impact. Make you sure have the measures in place so you can still manage machines. Preferably with exceptions on a per endpoint or server basis.

2. Via Powershell you can use the following commands:

   a. **SMB:** `netsh advfirewall firewall set rule group=”File and Printer Sharing” new enable=no`

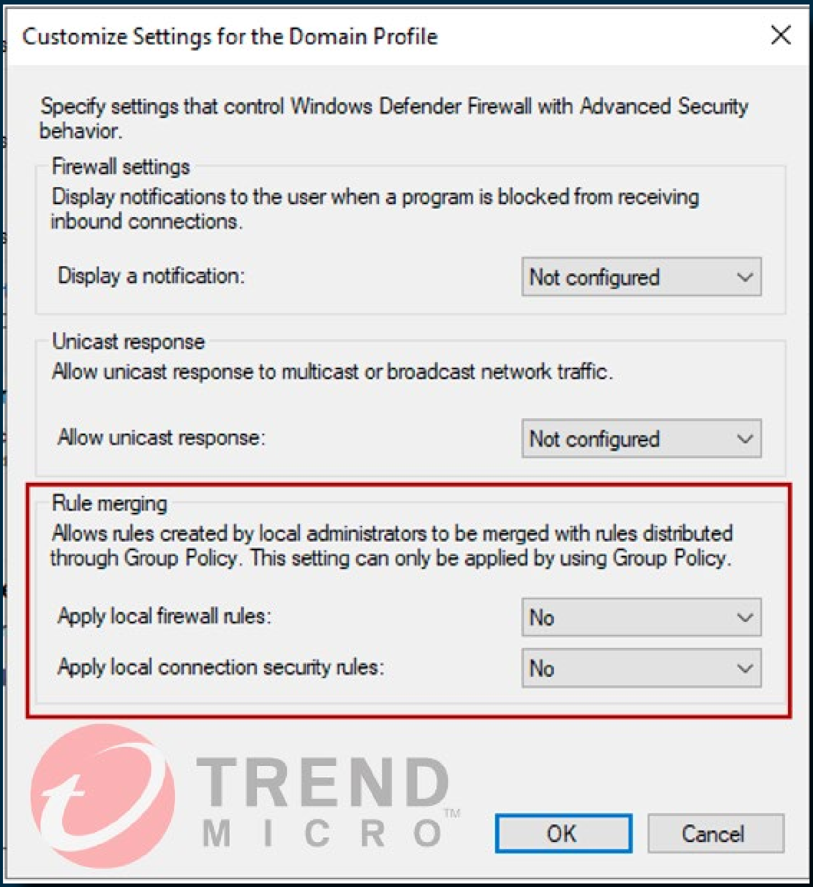
   b. **RDP:** `netsh advfirewall firewall set rule group=”Remote Desktop” new enable=no`

   c. **WMI:** `netsh advfirewall firewall set rule group=”windows management instrumentation (wmi)” new enable=no`

   d. **WinRM:** `netsh advfirewall firewall set rule group=”Windows Remote Management” new enable=no`

.

3. To ensure that only the newly made firewall rules are enforced and cannot be overridden on the endpoint or server, make sure to set the "Apply local firewall rules" and "Apply local connection security rules" to "No" for all



Customize Settings for the Domain Profile

Specify settings that control Windows Defender Firewall with Advanced Security behavior.

Firewall settings

Display notifications to the user when a program is blocked from receiving inbound connections.

Display a notification: Not configured

Unicast response

Allow unicast response to multicast or broadcast network traffic.

Allow unicast response: Not configured

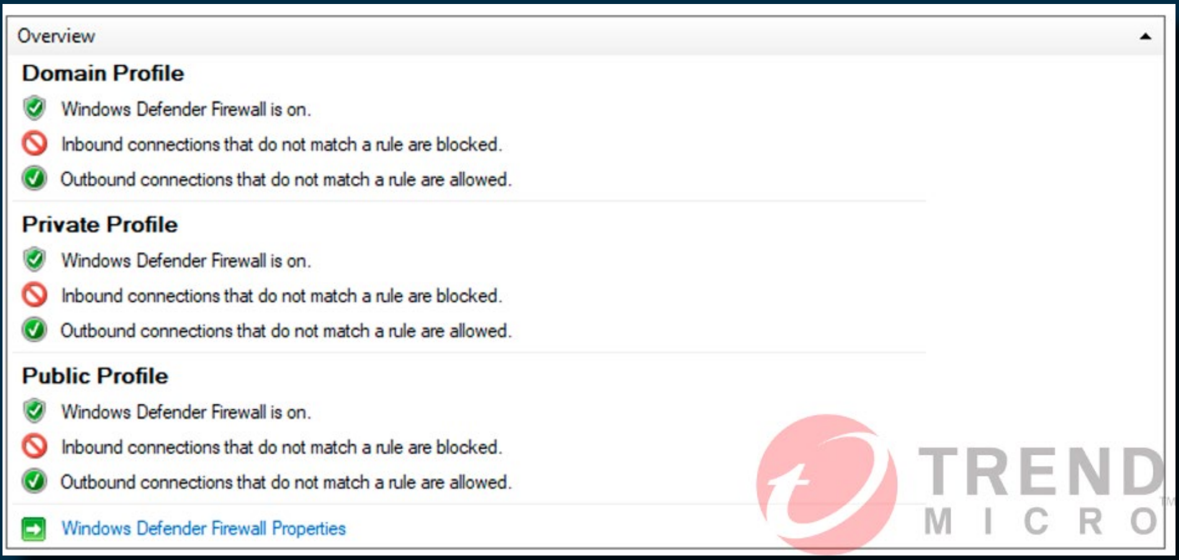
Rule merging

Allows rules created by local administrators to be merged with rules distributed through Group Policy. This setting can only be applied by using Group Policy.

Apply local firewall rules: No

Apply local connection security rules: No

Your overview should look as follows:



Overview

Domain Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Private Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Public Profile

- ✓ Windows Defender Firewall is on.
- ⊘ Inbound connections that do not match a rule are blocked.
- ✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

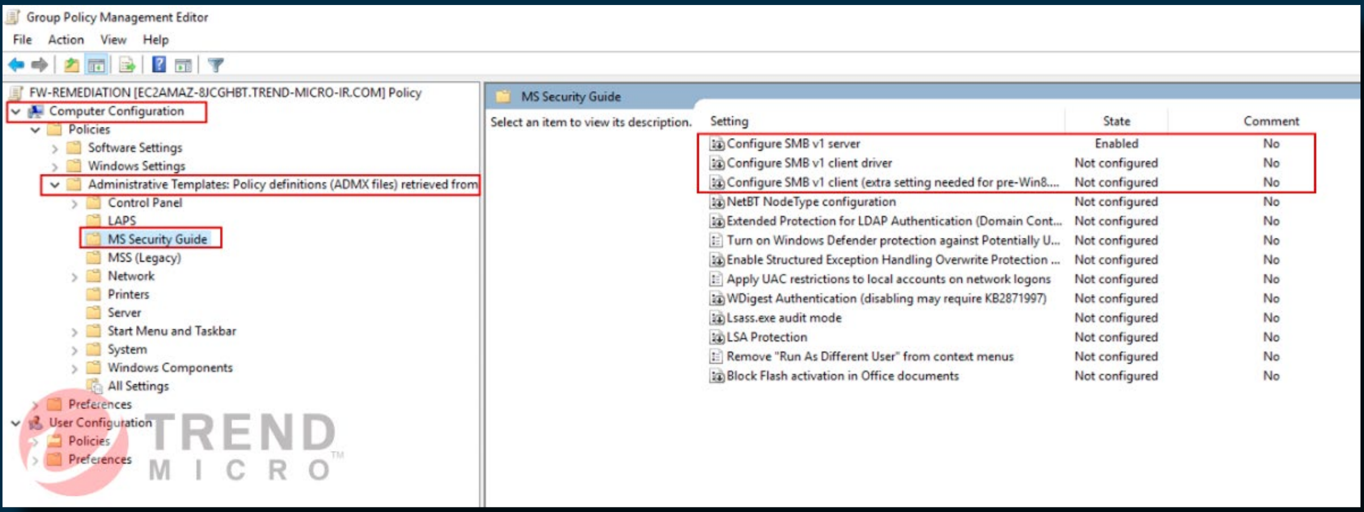
4.3 APPLY MICROSOFT BEST PRACTICE GPO'S

When a Threat Actor finds out SMB v1 is accessible they can use this for malicious intent such as, but not limited to, the EternalBlue exploit.

Disable SMB v1 in the following way:

1. Download the appropriate baseline from the "Microsoft Security Compliance Toolkit 1.0" on your Domain Controller and unpack the archive.
2. Copy the ".admx" files to "C:\Windows\PolicyDefinitions" (adjust as required).
3. Copy the ".adml" files from the folder "en-US" to " C:\Windows\PolicyDefinitions\en-US" (adjust as required).
4. Go to: "Computer Configuration > Policies > Administrative Templates > MS Security Guides".
5. Disable all SMB v1 options.

With the importing of the new Microsoft Best Practice GPO's, you can now select to disable multiple legacy protocols and enable logging for several services. Please review these closely and adjust to your security preferences.



Setting	State	Comment
Configure SMB v1 server	Enabled	No
Configure SMB v1 client driver	Not configured	No
Configure SMB v1 client (extra setting needed for pre-Win8....	Not configured	No
NetBT NodeType configuration	Not configured	No
Extended Protection for LDAP Authentication (Domain Cont...	Not configured	No
Turn on Windows Defender protection against Potentially U...	Not configured	No
Enable Structured Exception Handling Overwrite Protection ...	Not configured	No
Apply UAC restrictions to local accounts on network logons	Not configured	No
WDigest Authentication (disabling may require KB2871997)	Not configured	No
Lsass.exe audit mode	Not configured	No
LSA Protection	Not configured	No
Remove "Run As Different User" from context menus	Not configured	No
Block Flash activation in Office documents	Not configured	No

4.4 2-FACTOR AUTHENTICATION

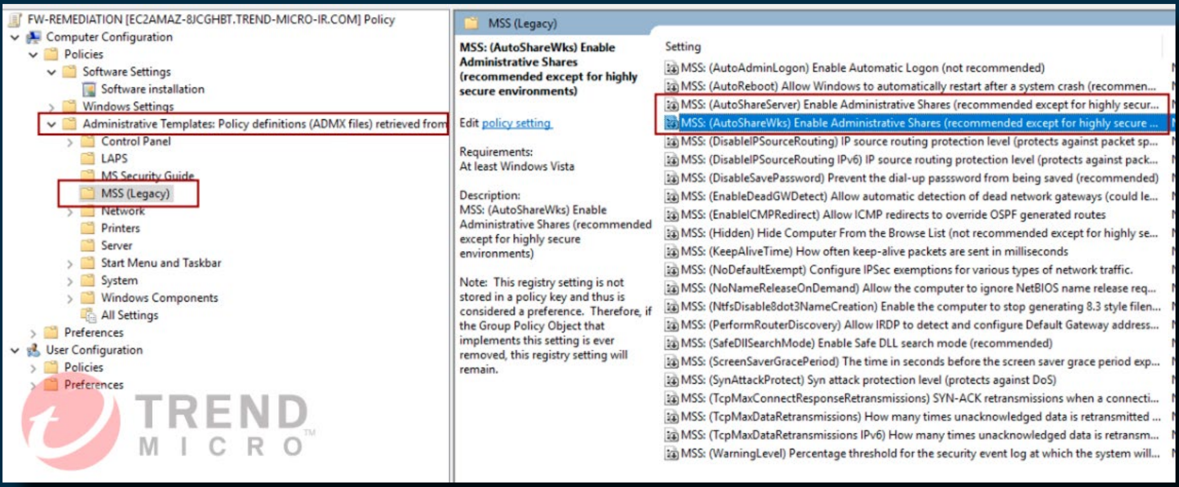
If external-facing RDP must be utilized for operational purposes, multi-factor authentication should be enforced for connectivity. This can be accomplished either via the integration of a third-party multi-factor authentication technology or by leveraging a Remote Desktop Gateway using RADIUS.

4.5 RESTRICT ADMINISTRATIVE SHARES

Some ransomware variants will attempt to use administrative or hidden shares including those that are not explicitly mapped to a drive letter and use these for binding to endpoints and servers. You can disable the administrative shares by using the "Microsoft Security Guide" Group Policy template from the Microsoft Security Compliance Toolkit.

.

1. Via the "Group Policy Management Editor" follow the steps below to disable these services:
2. Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareServer)
3. Computer Configuration > Policies > Administrative Templates > MSS (Legacy) > MSS (AutoShareWks)
4. Disable the services.



MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)

Edit policy setting

Requirements:
At least Windows Vista

Description:
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)

Note: This registry setting is not stored in a policy key and thus is considered a preference. Therefore, if the Group Policy Object that implements this setting is ever removed, this registry setting will remain.

MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommen...
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secur...
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure ...
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet sp...
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against pack...
MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)
MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could le...
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes
MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly se...
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds
MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release req...
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filen...
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway address...
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period exp...
MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)
MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connecti...
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted ...
MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransm...
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will...

Alternatively, you can use the following Powershell command:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

4.6 RESET THE KERBEROS GOLDEN TICKETS TWICE

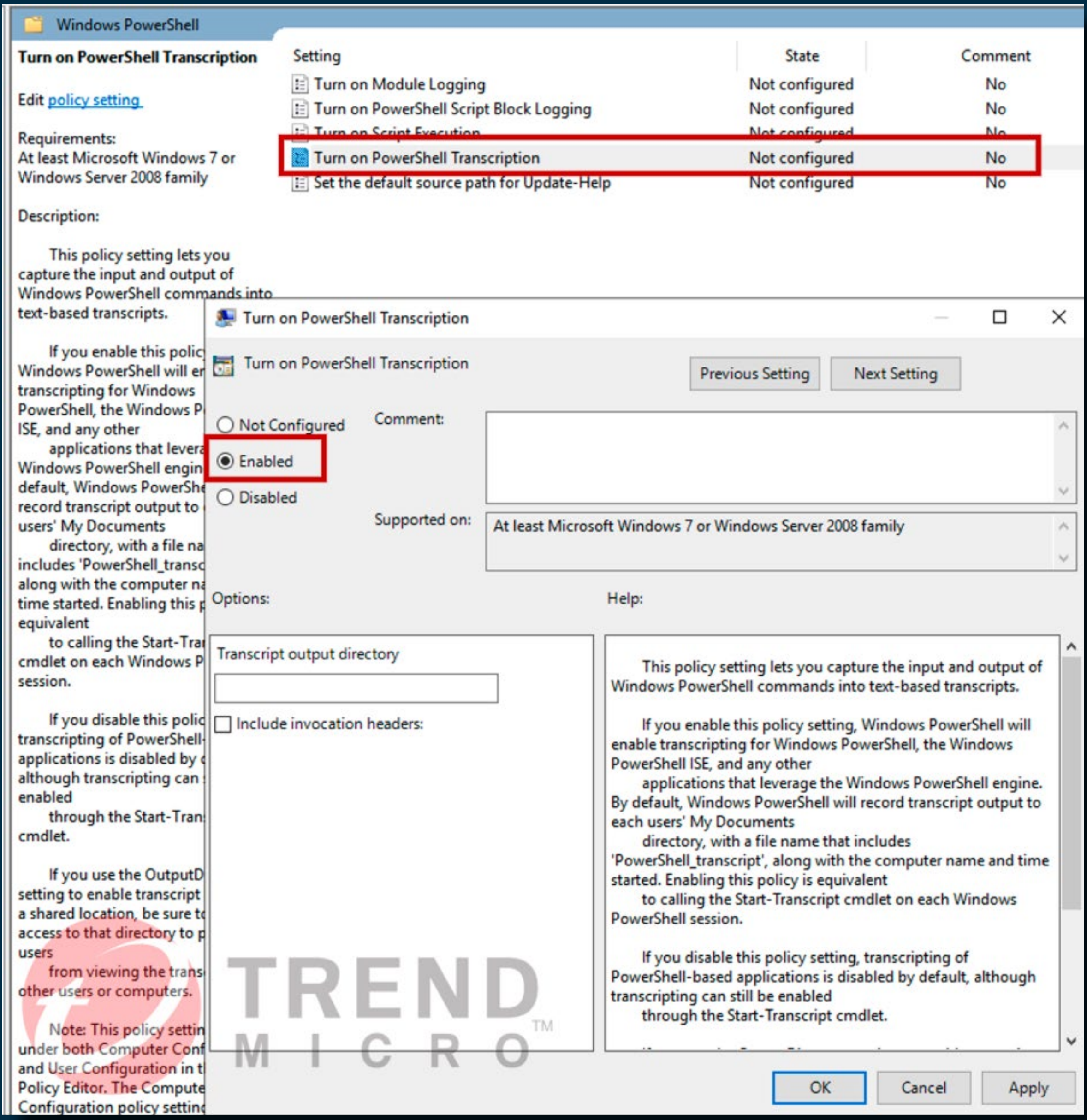
To avoid falling victim to a "Skeleton Key Attack" it is important to reset the Kerberos Golden Ticket twice. Microsoft has published a bespoke PowerShell script to perform this action. **Run this script twice** because the script will initially reset the Kerberos password once.

https://github.com/microsoft/New-KrbtgtKeys.ps1

4.7 ENABLE POWERSHELL LOGGING

Via the "Group Policy Management Editor" go to the following and enable:

1. Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell
2. Enable Powershell Transcription.



Windows PowerShell

Turn on PowerShell Transcription

Edit policy setting

Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family

Description:

This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

If you enable this polic Windows PowerShell will er transcripting for Windows PowerShell, the Windows P ISE, and any other applications that levera Windows PowerShell engin default, Windows PowerShe record transcript output to users' My Documents directory, with a file na includes 'PowerShell_transc along with the computer na time started. Enabling this p equivalent to calling the Start-Trar cmdlet on each Windows P session.

If you disable this polic transcripting of PowerShell- applications is disabled by although transcripting can enabled through the Start-Tran cmdlet.

If you use the OutputD setting to enable transcript a shared location, be sure t access to that directory to p users from viewing the trans other users or computers.

Note: This policy settin under both Computer Conf and User Configuration in t Policy Editor. The Compute Configuration policy settin

Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on PowerShell Script Block Logging	Not configured	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Not configured	No
Set the default source path for Update-Help	Not configured	No

Turn on PowerShell Transcription

Turn on PowerShell Transcription

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Transcript output directory

□ Include invocation headers:

Help:

This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents directory, with a file name that includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session.

If you disable this policy setting, transcripting of PowerShell-based applications is disabled by default, although transcripting can still be enabled through the Start-Transcript cmdlet.

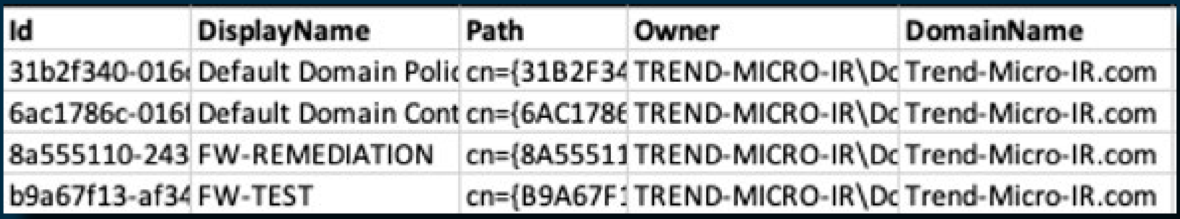
4.8 GROUP POLICY OBJECT MONITORING

It is common for Threat Actors to deploy ransomware or other malicious content by modifying an existing GPO or by creating a new GPO. You should proactively review the configuration of the configured GPO's on the Domain Controllers and review any changes that have been made and ensure only expected behavior is found.

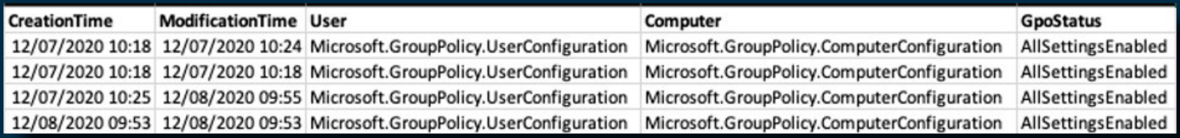
An easy way to do this is via Powershell, use the following script on your domain controller:

```
get-gpo -all | export-csv -path "c:\temp\gpo-list-1.csv"
-NoTypeInformation
```

The export can look like the following:



Id	DisplayName	Path	Owner	DomainName
31b2f340-016	Default Domain Polic	cn={31B2F34	TREND-MICRO-IR\Dc	Trend-Micro-IR.com
6ac1786c-016	Default Domain Cont	cn={6AC178	TREND-MICRO-IR\Dc	Trend-Micro-IR.com
8a555110-243	FW-REMEDIATION	cn={8A5551	TREND-MICRO-IR\Dc	Trend-Micro-IR.com
b9a67f13-af34	FW-TEST	cn={B9A67F	TREND-MICRO-IR\Dc	Trend-Micro-IR.com



CreationTime	ModificationTime	User	Computer	GpoStatus
12/07/2020 10:18	12/07/2020 10:24	Microsoft.GroupPolicy.UserConfiguration	Microsoft.GroupPolicy.ComputerConfiguration	AllSettingsEnabled
12/07/2020 10:18	12/07/2020 10:18	Microsoft.GroupPolicy.UserConfiguration	Microsoft.GroupPolicy.ComputerConfiguration	AllSettingsEnabled
12/07/2020 10:25	12/08/2020 09:55	Microsoft.GroupPolicy.UserConfiguration	Microsoft.GroupPolicy.ComputerConfiguration	AllSettingsEnabled
12/08/2020 09:53	12/08/2020 09:53	Microsoft.GroupPolicy.UserConfiguration	Microsoft.GroupPolicy.ComputerConfiguration	AllSettingsEnabled

Securing Your Connected World