





How to block WannaCrypt, Locky and any other ransomware

- Sami Laiho

WHOAMI /ALL

Sami Laiho

Senior Technical Fellow

adminize.com

- IT Admin since 1996
- MCT since 2001 (MCT Regional Lead – Finland)
- MVP in Windows OS since 2011
- Specializes in and trains:
 - Troubleshooting
 - Security
 - Centralized Management
 - Active Directory
 - Hacking
 - Penetration testing
 - Social Engineering
- Trophies:
 - Best External Speaker (non-Microsoft) at Ignite 2017
 - NIC 2016, 2017 - Best Speaker
 - Best Sessions (#1 and #2) at TechTalks 2017, Helsinki
 - Best Session at AppManagEvent 2017, Utrecht
 - TechDays Sweden 2016 – Best Speaker
 - Ignite 2015 – Best male presenter ;) (#2 out of 1000 speakers)
 - TechEd Europe and North America 2014 - Best session, Best speaker
 - TechEd Australia 2013 - Best session, Best speaker



I got Certs



1,2 kg of
them

TODISTUS



SALTER

1164

Max 5000g x 1g/Max 11lb x 0.1oz

ON-OFF

ML-FL.OZ

ZERO

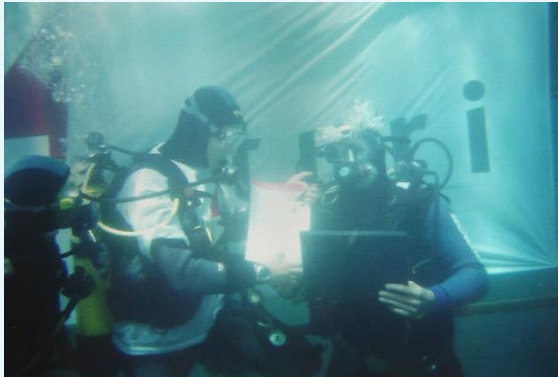
G-OZ

Adminize.com

- Established in 1983
- We deliver:
 - Adminizer
 - One-time Admin passwords for users
 - Hasslefree administration for local admin accounts
 - Training
 - Anything Microsoft
 - Anything Security
 - Onsite, Online, Offsite
 - Consulting
 - Anything Microsoft
 - Top-end troubleshooting (Online/Onsite)
 - Removing of admin rights from end users in Windows environments
 - Pentesting and Security Auditing

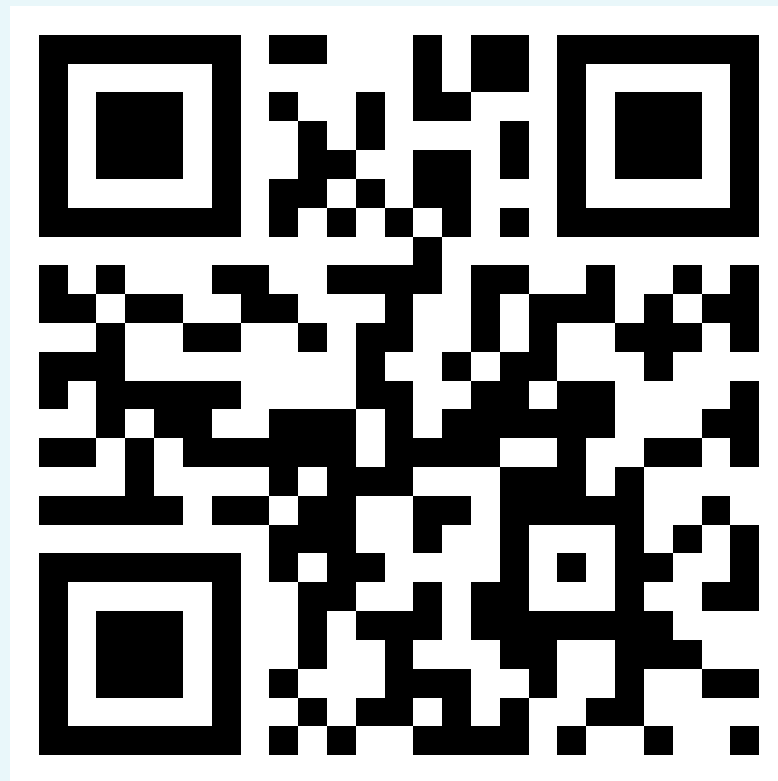


Windows XP Deep Dive in 2001



Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: <http://blog.win-fu.com/>
- Free newsletter:
<http://eepurl.com/F-GOj>
- My trainings:
 - <https://win-fu.com/ilt/>
 - <https://win-fu.com/dojo/>



NIC



2017 FIA FORMULA ONE WORLD CHAMPIONSHIP™



2017 FORMULA 1 ROLEX BRITISH GRAND PRIX

Finnish honesty in action



**“Crap music, slow service
Come and experience”**

nic

Logistics

- Slides available at <https://win-fu.com/share/>
 - Later on Github I guess
- Wireless
- Restrooms
- Timing:
 - 9-17 (max)
 - Breaks about every hour
 - Lunch at 12:30-13:30

Resources

Slides and demos from the conference will be available at
github.com/nordicinfrastructureconference/2018 (bit.ly/2y7JhA3)



Why are we here?

Global ransomware damage costs predicted to exceed \$5 billion in 2017, up from \$325 million in 2015.

Ransomware damages up 15X in 2 years, expected to worsen; Ransomware attacks on healthcare organizations will quadruple by 2020.

– [Steve Morgan](#), Editor-In-Chief

Menlo Park, Calif. – May 18, 2017

[Ransomware](#) — a malware that infects computers and restricts their access to files, often threatening permanent data destruction unless a ransom is paid — has reached epidemic proportions globally.



In 2015, there were numerous media and researchers stating that [ransomware was not all it's cracked up to be](#). Ransomware accounted for roughly [\\$325 million in damages in 2015](#), according to Microsoft.

After a surge of attacks the following year, [Cybersecurity Ventures](#) predicted that ransomware damages and related costs would reach [\\$1 billion annually in 2016](#).

According to the Cisco 2017 Annual Cybersecurity Report, [ransomware is growing at a yearly rate of 350%](#).

One industry expert suggests that WannaCrypt could be responsible for as much as 20% of total ransomware damage costs in 2017.

“The estimated damage caused by WannaCry in just the initial 4 days would exceed a billion dollars, looking at the massive downtime caused for large organizations worldwide” says [Stu Sjouwerman](#), founder and CEO at [KnowBe4](#), a company that specializes in training employees on how to detect and respond to ransomware attacks.

“WannaCrypt is a sign of the times” says Morgan. There’s been a gradual buildup of ransomware attacks, one more severe than the next. There was the recent Google Docs attack where a million workstations were infected within hours. At the end of last year an infection called [HDDCryptor compromised the IT network of San Francisco Municipal Transit Agency](#), paralyzing the company’s critical services for several days.

The Locky strain of ransomware hit Hollywood Presbyterian Hospital in Los Angeles last year – which led to the shutdown of its computer systems and a [\\$17,000 ransomware payout](#). There have been dozens of [ransomware attacks on the healthcare industry](#) in 2016 and 2017.

Cybersecurity Ventures predicts ransomware attacks on healthcare organizations will [quadruple by 2020](#). “Hospitals are the [number one target](#) for cybercriminals, and they are particularly vulnerable to ransomware” says Morgan.

Ransomware targets all industries, and more than just computer data. Motion pictures and anything digital are now at risk.



Training, Training, Training

Training employees how to recognize and defend against cyber attacks is the most under spent sector of the cybersecurity industry — and yet it holds out the greatest hope for combating ransomware attacks.

91 percent of attacks by sophisticated cybercriminals start through email, according to Mimecast, a leading email security firm. Spear phishing attacks on employees are commonly used to infect organizations with ransomware.

“Training employees on security will immediately bolster the cyber defenses at most companies,” says Lawrence Pingree, a research director at Gartner, because most data breaches are based on “exploiting common user knowledge gaps to social engineer them to install malware or give away their credentials.”

Phishing identification training definitely bolstered Wells Fargo’s cyber defenses, notes Chief Information Security Officer Rich Baich. Through the use of various security awareness techniques, he says, workforce susceptibility to phishing declined by more than 40 percent.

How we are gonna do this?

- I'll show the minimum options to block RansomWare
 - You should have at least this
- But I'll show the proactive "REAL" way to go as well
 - This is what I hope you aim for
- We will also talk about less foundational cool features
 - These are a nice add on
- THIS IS FOR YOU! Tweak accordingly for Enterprises!

The High Level Topics

- Implement Basic Protections (AM, Firewall)
- Implement Principle of Least Privilege
- Implement Whitelisting (and some Blacklisting)
- Block Lateral Movement
- Implement Cool New Windows 10 Features
- Prepare for Forensics



Basics

Basic Protections

- Firewall Everything!
- BitLocker Everything!
- Use Anti-Malware, just not as your main protection!
- Get rid of SMBv1
 - If possible get rid of NTLM
- Implement MFA

Firewall

- Every computer has a firewall! NO EXCEPTIONS!
- Windows Firewall is just enough
 - You just need to tweak a few things
- Logging needs to be turned on and the log size increased
- You can prevent merging with local rules with Group Policy

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

- Inbound Rules
- Outbound Rules**
- Connection Security Rules
- Monitoring

Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address
CScript 32bit		All	Yes	Block	No	c:\windo...	Any	Any
CScript 64bit		All	Yes	Block	No	%System...	Any	Any
PowerShell 32-Bit		All	Yes	Block	No	%System...	Any	Internet
PowerShell 64-bit		All	No	Block	No	%System...	Any	Internet
PS ISE 32-bit		All	Yes	Block	No	%System...	Any	Internet
PS ISE 64-bit		All	Yes	Block	No	%System...	Any	Internet
Regsvr32 32-bit		All	Yes	Block	No	%System...	Any	Any
Regsvr32 64-bit		All	Yes	Block	No	c:\windo...	Any	Any
Rundll32.exe 32bit		All	Yes	Block	No	%System...	Any	Any
Rundll32.exe 64-bit		All	Yes	Block	No	%System...	Any	Any
WScript 32bit		All	Yes	Block	No	c:\windo...	Any	Any
WScript 64bit		All	Yes	Block	No	c:\windo...	Any	Any

Actions

- Outbound ...
- New R...
- Filter b...
- Filter b...
- Filter b...
- View
- Refresh
- Export ...
- Help
- PowerShell ...
- Copy

DEMO

NIC

BitLocker

- Everyone need BitLocker!
- **It is part of the INTEGRITY of your computer** not just encryption!
- UEFI+SecureBoot+DMA-blocks with TPM-only is just fine!
 - Some require more, 95% of my customers don't!
 - I usually say that if you use admin-rights then you need a PIN
 - READ CAREFULLY: <http://blog.win-fu.com/2017/02/the-true-story-of-windows-10-and-dma.html>

BitLocker FlowChart by me

- <http://win-fu.com/files/TPM-FlowchartV3.pdf>

DEMO

NIC

Anti-Malware

- Defender is just fine if you can take care of
 - Alerting
 - Reporting
- I disable 3rd party firewall anyway and on Windows 7 I use Security Essentials
 - I use SCEP if available – if not, then I try to use Splunk etc. Or event forwarding
- ”Defender found 85% of malware when a competitor found 96% ???”

DEMO

NIC



Principle of Least Privilege

Why?

- "In Windows there is no security if you use admin rights" – 1993 NT User Guide
- Let me show you how to show someone 😊

2016 Microsoft Vulnerabilities Study

Key findings

- Of the 189 vulnerabilities in 2016 with a Critical rating, 94% were concluded to be mitigated by removing administrator rights
- 66% of all Microsoft vulnerabilities reported in 2016 could be mitigated by removing admin rights
- 100% of vulnerabilities impacting Microsoft's latest browser Edge could be mitigated
- 100% of vulnerabilities in Internet Explorer could be mitigated by removing admin rights
- 99% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights
- 93% Critical vulnerabilities affecting Windows 10 could be mitigated by removing admin rights

2016 Microsoft Vulnerabilities Study

Key findings

- There has been a 62% rise in the total volume of vulnerabilities since 2013
- From 2013 to 2016, there was a 63% increase in the total number of Windows vulnerabilities reported
- Despite being labelled as the “most secure” Windows OS ever, Windows 10 had the highest proportion of vulnerabilities (395) compared to any other OS.
- The volume of Windows 10 vulnerabilities was 46% higher than Windows 8 and Windows 8.1

DEMO

NIC

Basics

- Never log on as an admin!
- Do at least what I do and use different accounts
- Try to prevent interactively logging on as the secondary account (Admin)

If you can't get rid of admin rights

- Use 3rd party solutions like Avecto DefendPoint, BeyondTrust, PolicyPak etc.
 - I use Avecto on my own laptop as well
- Let devs be admins if needed but take it into control with the 3rd party solutions
- With the 3rd party solutions you get a "Better than AppLocker Whitelisting" as well, and it works on Pro!

DEMO

NIC



Implement Whitelisting

Why?

- 1000000 new malware samples per day
- Gartner says so, like does every other security company
- It's an easy and cheap way to block malware, and RANSOMWARE!

Whitelisting options

- Windows NT4+
 - User Policy driven whitelist for exe names
- Windows XP+
 - Software Restriction Policy
- Windows 7 Enterprise+
 - AppLocker
- Windows 10 Enterprise+
 - Hypervisor-based Code Integrity (HVCI)

Common things about whitelisting

- Whitelisting is the most effective way to increase a companys security!
- Effective Whitelisting works only when combined with the Principle of Least Privilege
 - Device Guard works for admins as well
- No builtin reporting
- Whitelisting is a security barrier – Blacklisting is not!

Normal Project Run (AppLocker)

- Implement log forwarding
- Implement AppLocker in Audit mode
 - Choose a pilot group
- Collect logs for at least a month
- Create rules based on logs
- Create an escape plan
- Educate Admins
- Turn on AppLocker Auditing for the rest of the environment
- Turn on AppLocker Enforcement for the pilot group
 - You can start with EXE and MSI, and then later turn on DLL and Scripts if you want to balance
- Monitor for sometime
- Turn on everywhere!
- Harden!

AppLocker HOW TO

- Keep to containers not items – Folders vs Files, Publishers vs Hashes
- Remember to audit your installation with AccessChk!
- Remember NO ADMIN RIGHTS!!

AppLocker Properties

Enforcement Advanced

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:

☒ Configured

Enforce rules

Windows Installer rules:

☒ Configured

Enforce rules

Script rules:

☒ Configured

Enforce rules

Packaged app Rules:

☒ Configured

Enforce rules

DLL rules:

☒ Configured

Enforce rules


[More about rule enforcement](#)

OK Cancel Apply

AppLocker Properties

Enforcement Advanced

Specify whether the DLL rule collection is enabled.

 **DLL rules can affect system performance**

Only enable DLL rules after thoroughly reviewing the AppLocker documentation. DLL rules can affect system performance and cause unexpected behavior if they are not properly implemented.

☒ Enable the DLL rule collection

[More about DLL rules](#)

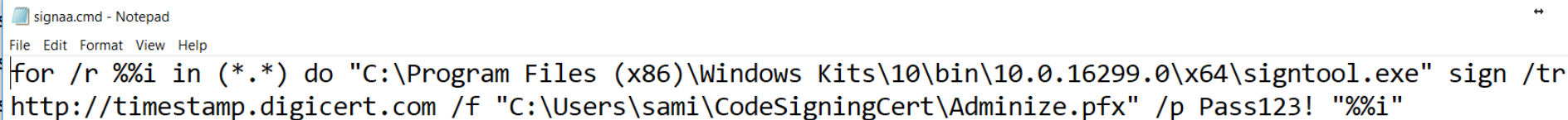
OK Cancel Apply

Local Computer Policy	Action	User	Name	Condition
<ul style="list-style-type: none"> Computer Configuration <ul style="list-style-type: none"> Software Settings Windows Settings <ul style="list-style-type: none"> Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings <ul style="list-style-type: none"> Account Policies Local Policies Windows Defender Firewall with <ul style="list-style-type: none"> Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies <ul style="list-style-type: none"> AppLocker <ul style="list-style-type: none"> Executable Rules Windows Installer Rules Script Rules DLL Rules Packaged app Rules 	<ul style="list-style-type: none"> Allow 	<ul style="list-style-type: none"> Everyone 	<ul style="list-style-type: none"> (Default Rule) All files located in the Program Files f... 	<ul style="list-style-type: none"> Path
	<ul style="list-style-type: none"> Allow 	<ul style="list-style-type: none"> Everyone 	<ul style="list-style-type: none"> (Default Rule) All files located in the Windows folder 	<ul style="list-style-type: none"> Path
	<ul style="list-style-type: none"> Allow 	<ul style="list-style-type: none"> BUILTIN\Administrators 	<ul style="list-style-type: none"> (Default Rule) All files 	<ul style="list-style-type: none"> Path
	<ul style="list-style-type: none"> Allow 	<ul style="list-style-type: none"> Everyone 	<ul style="list-style-type: none"> Signed by * 	<ul style="list-style-type: none"> Publisher
	<ul style="list-style-type: none"> Deny 	<ul style="list-style-type: none"> DESKTOP-OPVF5LT\BLOCK PS 	<ul style="list-style-type: none"> POWERSHELL.EXE, in MICROSOFT® WINDOWS® ... 	<ul style="list-style-type: none"> Publisher
	<ul style="list-style-type: none"> Deny 	<ul style="list-style-type: none"> DESKTOP-OPVF5LT\BLOCK PS 	<ul style="list-style-type: none"> POWERSHELL_ISE.EXE, version 10.0.0.0 and above, i... 	<ul style="list-style-type: none"> Publisher
	<ul style="list-style-type: none"> Deny 	<ul style="list-style-type: none"> NT AUTHORITY\Local account and mem... 	<ul style="list-style-type: none"> *\explorer.exe 	<ul style="list-style-type: none"> Path
	<ul style="list-style-type: none"> Deny 	<ul style="list-style-type: none"> NT AUTHORITY\Local account and mem... 	<ul style="list-style-type: none"> TASKMGR.EXE, in MICROSOFT® WINDOWS® OPE... 	<ul style="list-style-type: none"> Publisher

Local Computer Policy				
Computer Configuration				
Software Settings				
Windows Settings				
Name Resolution Policy				
Scripts (Startup/Shutdown)				
Deployed Printers				
Security Settings				
Account Policies				
Local Policies				
Windows Defender Firewall with				
Network List Manager Policies				
Public Key Policies				
Software Restriction Policies				
Application Control Policies				
AppLocker				
Executable Rules				
Windows Installer Rules				
Script Rules				
DLL Rules				
	Action	User	Name	Condition
	Allow	Everyone	(Default Rule) Microsoft Windows DLLs	Path
	Allow	Everyone	(Default Rule) All DLLs located in the Program Files f...	Path
	Allow	BUILTIN\Administrators	(Default Rule) All DLLs	Path
	Allow	Everyone	Signed by *	Publisher
	Deny	DESKTOP-OPVF5LT\BLOCK PS	SYSTEM.MANAGEMENT.AUTOMATION.RESOURCE...	Publisher

Signing

- 95% of Malware is not signed – just something to think about
- You can sign apps yourself
 - Use Timestamp if possible!
- If you have the cert on your computer installed:
 - **Signtool sign /v /s MY /n MyPrivateCert**
/t <http://timestamp.verisign.com/scripts/timestamp.dll> FileToSign.exe
- If not:



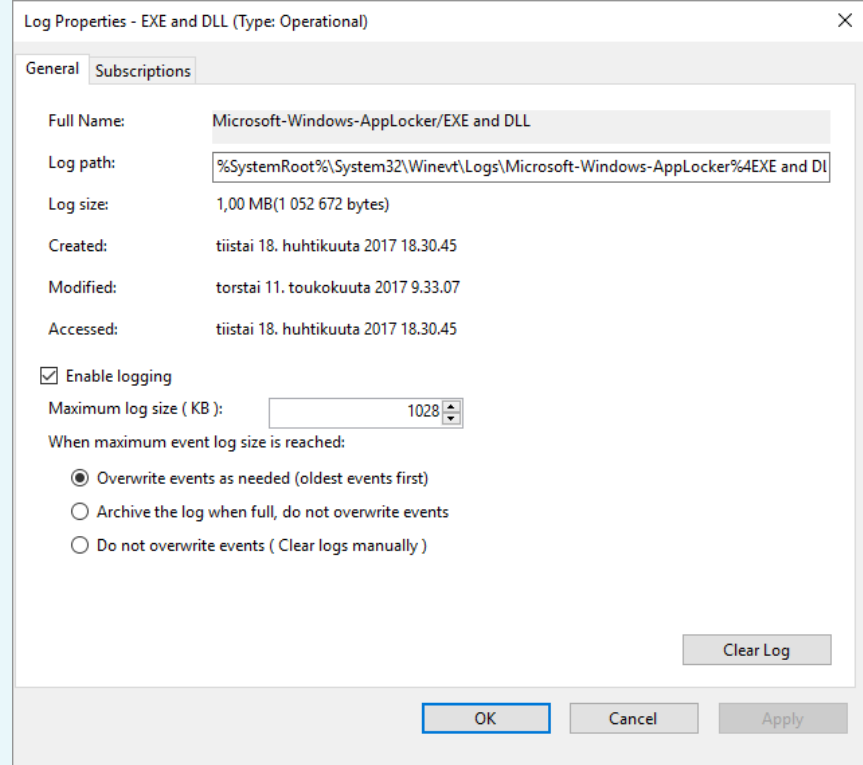
```
signaa.cmd - Notepad
File Edit Format View Help
for /r %%i in (*.*) do "C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64\signtool.exe" sign /tr
http://timestamp.digicert.com /f "C:\Users\sami\CodeSigningCert\Adminize.pfx" /p Pass123! "%%i"
```

- Guide: <https://blogs.msdn.microsoft.com/winsdk/2009/11/13/steps-to-sign-a-file-using-signtool-exe/>



AppLocker

- Log size should be increased!
 - At least 30MB



DEMO

NIC

Need to learn even more step by step?

- Join my session at 8:30 on Friday!!!

No Enterprise?

- Use Software Restriction Policy (v1)
- Not as easy or good as AppLocker but WAY better than nothing 😊

DEMO

NIC



Block Lateral Movement

MOST IMPORTANT!!!

- You can't have the same local admin username/password on two different endpoints!
- Deploy a solution to make sure it doesn't happen! If you don't care about the password you can use just: `NET USER Master Pass%random%!!`

LAPS / Adminizer

Deploying LAPS

Microsoft Local Admin Password Solution (LAPS) – Deployment Steps



Shameless Plug

- <http://blog.win-fu.com/2015/10/adminizer-still-beats-laps.html>

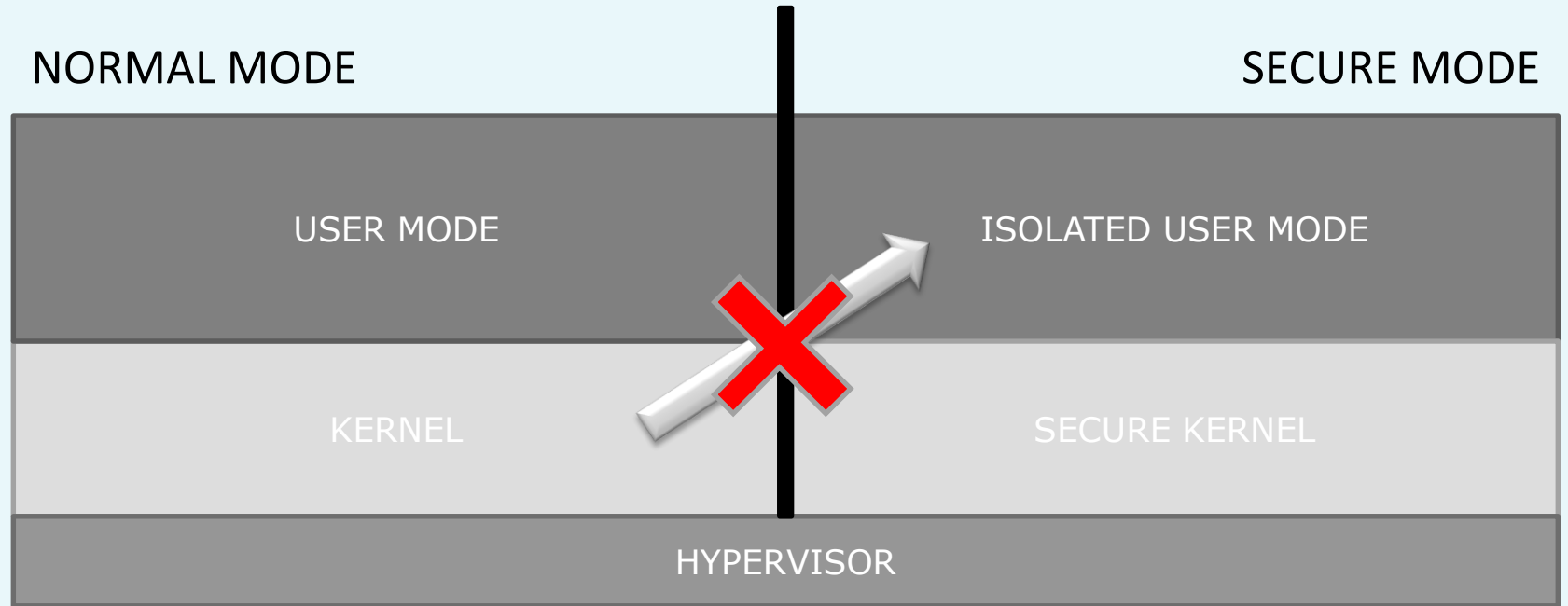
Lazy way

- Windows 7
 - Deny access to Local Administrators from the network
 - Requires [KB 2871997](#)
- Windows 8.1/10
 - Deny access to Local Administrators from the network



Deploy Credential Guard

Normal and Secure mode



Credential Guard

- Applications will break if they require:
 - Kerberos DES encryption support
 - Kerberos unconstrained delegation
 - Extracting the Kerberos TGT
 - NTLMv1
- Applications will prompt and expose credentials to risk if they require:
 - Digest authentication
 - Credential delegation
 - MS-CHAPv2
- Problems I've encountered
 - F5 Big-IP Edge Client – VPN client
 - Check Point Capsule – Client for cloud firewall
 - Cylance Protect - Antivirus

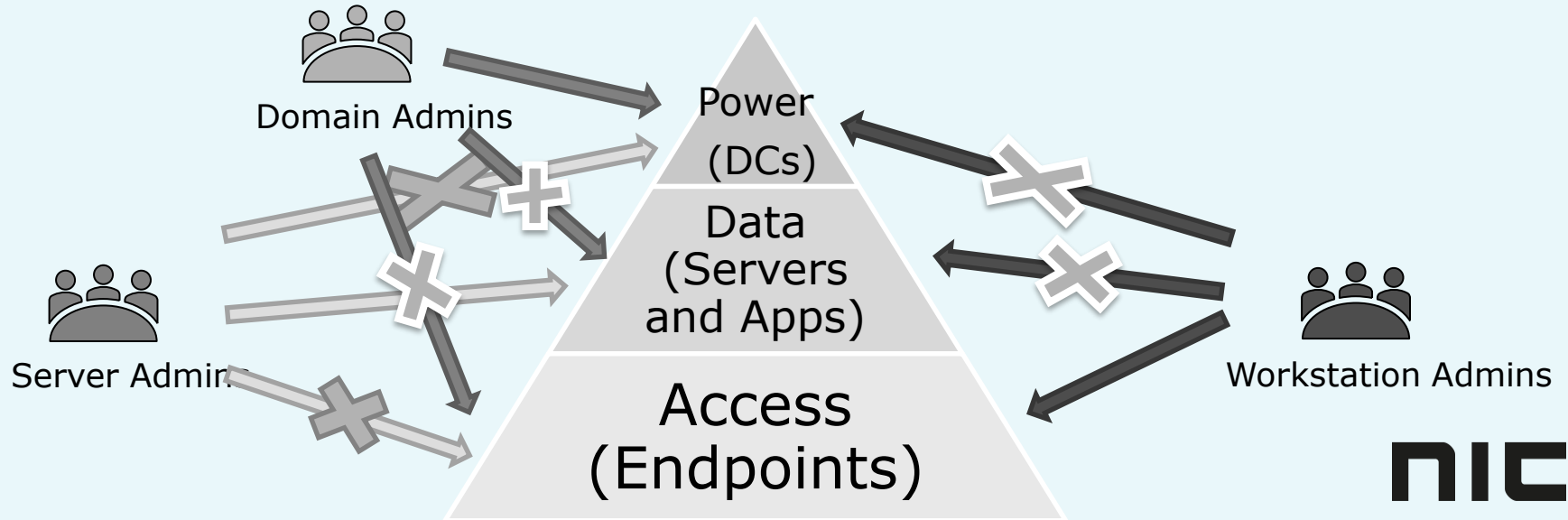
CredGuard does not block
STUPIDITY...

DEMO

NIC

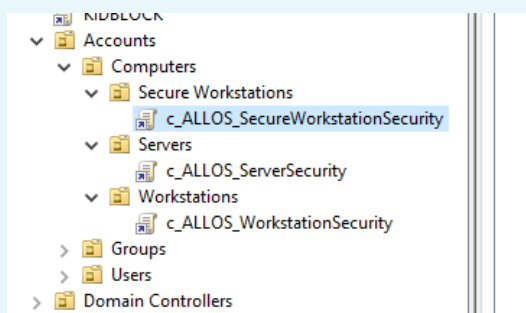
Mitigating PtH?

- Split your environment into three layers
- Never allow higher layer admins to logon to lower layers



My AD

- Management WS



A screenshot of the Group Policy Management console. The left pane shows the hierarchy: Group Policy Management > Forest: XENONIA.local > Domains > XENONIA.local > c_ALLOS_SecureWorkstationSecurity. The right pane shows the configuration for the selected GPO.

Group Policy Management
File Action View Window Help

Group Policy Management
Forest: XENONIA.local
Domains
XENONIA.local
c_ALLOS_Avecto
c_ALLOS_DomainSecurity
c_ALLOS_IPsec
c_ALLOS_PowerOptions_RDP_GPO
c_ALLOS_Shortcuts
Default Domain Policy
KIDBLOCK
Accounts
Computers
Secure Workstations
c_ALLOS_SecureWorkstationSecurity
Servers
c_ALLOS_ServerSecurity
Workstations
c_ALLOS_WorkstationSecurity
Groups
Users
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs

c_ALLOS_SecureWorkstationSecurity
Scope Details Settings Delegation

c_ALLOS_SecureWorkstationSecurity
Data collected on: 24.3.2017 15.06.15

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	XENONIA\G_Server_Admins, XENONIA\Domain Admins, NT AUTHORITY\Local account and member of Ad
Deny log on as a batch job	XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on as a service	XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on through Terminal Services	XENONIA\Domain Admins, XENONIA\G_Server_Admins

Restricted Groups

Application Control Policies

User Configuration (Enabled)

Normal Workstation

Group Policy Management

File Action View Window Help

Group Policy Management

Forest: XENONIA.local

- Domains
 - XENONIA.local
 - c_ALLOS_Avecto
 - c_ALLOS_DomainSecurity
 - c_ALLOS_IPsec
 - c_ALLOS_PowerOptions_RDP_GPO
 - c_ALLOS_Shortcuts
 - Default Domain Policy
 - KIDBLOCK
 - Accounts
 - Computers
 - Secure Workstations
 - c_ALLOS_SecureWorkstationSecurity
 - Servers
 - c_ALLOS_ServerSecurity
 - Workstations
 - c_ALLOS_WorkstationSecurity
 - Groups
 - Users
 - Domain Controllers
 - Group Policy Objects
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

c_ALLOS_WorkstationSecurity

Scope Details Settings Delegation

c_ALLOS_WorkstationSecurity

Data collected on: 24.3.2017 15:06:16

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	XENONIA\G_Server_Admins, XENONIA\Domain Admins, NT AUTHORITY\Local account and member of Administrators group
Deny log on as a batch job	XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on as a service	XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on locally	XENONIA\Domain Admins, XENONIA\G_Server_Admins
Deny log on through Terminal Services	XENONIA\Domain Admins, XENONIA\G_Server_Admins

Restricted Groups

Group	Members	Member of
XENONIA\G_Workstation_Admins		BUILTIN\Administrators

Windows Firewall with Advanced Security

Application Control Policies

User Configuration (Enabled)

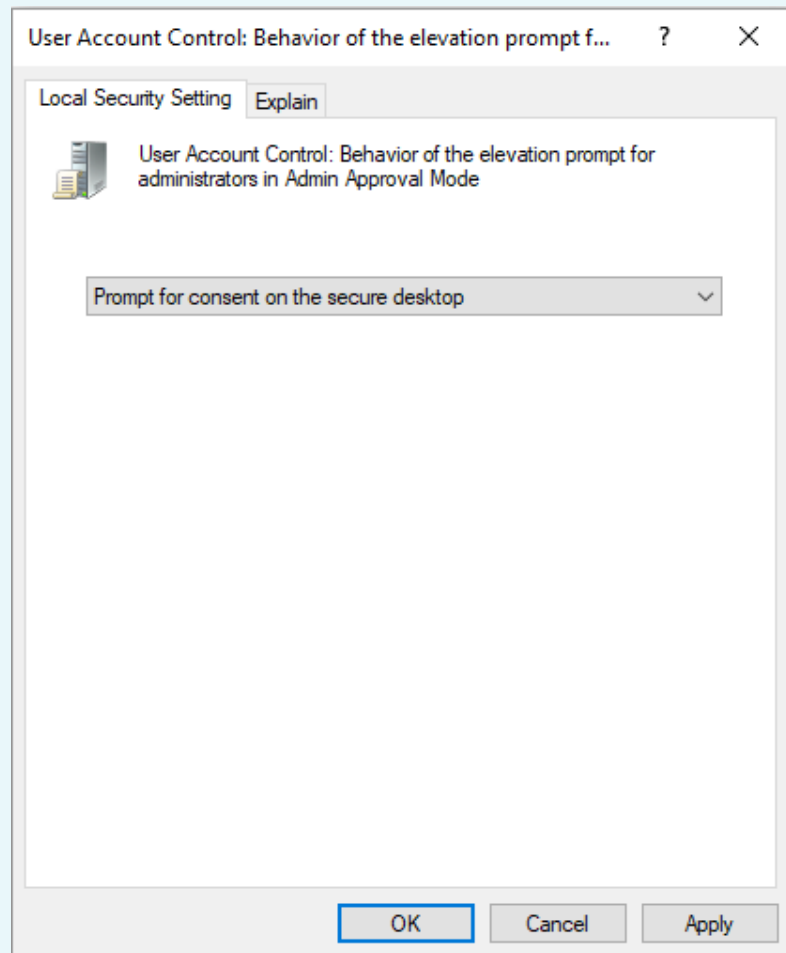
No settings defined.

Servers

c_ALLOS_ServerSecurity	
Scope	Details Settings Delegation
c_ALLOS_ServerSecurity	
Data collected on: 24.3.2017 15.06.49	
show	
Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Local Policies/User Rights Assignment	
Policy	Setting
Deny access to this computer from the network	XENONIA\G_Workstation_Admins, XENONIA\Domain Admins, NT AUTHORITY\Local account and member of Administrators group
Deny log on as a batch job	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Deny log on as a service	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Deny log on locally	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Deny log on through Terminal Services	XENONIA\Domain Admins, XENONIA\G_Workstation_Admins
Restricted Groups	
User Configuration (Enabled)	
No settings defined.	

PAW

- Management workstations
 - RSAT
 - Allowed to be used by Domain Admins or Server Admins
 - Hopefully not interactively
 - Prevented by AppLocker
 - UAC-elevation with authentication is recommended



DEMO

NIC



Implement Cool New Windows 10 Features

Device Guard

New Additions

- Deploy Managed Installer for Windows Defender Device Guard
 - <https://docs.microsoft.com/en-us/windows/device-security/device-guard/deploy-managed-installer-for-device-guard>
- Software list from ISG
 - <https://blogs.windows.com/business/2017/06/27/announcing-end-end-security-features-windows-10/>
 - <https://blogs.technet.microsoft.com/mmmpc/2017/10/23/introducing-windows-defender-application-control/>



New

Dashboard

All resources

Intune

Azure Active Directory

Resource groups

App Services

Function Apps

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Monitor

More services >

Endpoint protection

Windows 10 and later



Select a category to configure settings.

Application Guard
7 settings available >Windows Defender Firewall
43 settings available >Windows Defender SmartScreen
2 settings available >Windows Encryption
10 settings available >Windows Defender Exploit Guard
14 settings available >Windows Defender Application Co...
1 setting available >

OK

Windows Defender Application Control

Windows 10 and later



Choose additional apps that either need to be audited by, or can be trusted to run by application control code integrity policies. Windows components, all apps from Windows store are automatically trusted to run.

Applications will not be blocked when running in "audit only" mode. "Audit only" mode logs all events in local client logs. [Learn more about Device Guard deployment.](#)

Application control code integrity policies: ⓘ

Enforce ▼

Trust apps with good reputation: ⓘ

Enable ▼

Only Windows components, Microsoft store apps, and reputable apps as defined by the Intelligent Security Graph will be allowed to run.

OK

Tools used to Deploy and Manage Device Guard

General guidance and blog resources were provided earlier to help prepare endpoints for Device Guard. You're likely to be using ConfigMgr and/or Microsoft Intune to manage Windows 10 PC's in the environment. The following table shows the roles and relationship of these and other tools, and the tasks they execute towards deploying and managing Device Guard:

	Group Policy	Configuration Manager	MDT / DISM	Intune	PowerShell	Packagelnspector.exe	SignTool.exe
Deploy hardware based security features (UEFI/Secure Boot, VBS)		●					
Configure hardware based security features (UEFI Secure Boot, VBS)	●						
Manage hardware based security features (UEFI/Secure Boot, VBS)		●					
Enable/Install Windows features (Hyper-V, Isolated User Mode)		●	●		●		
Configure Virtualization-based security features (for protection of KMC)	●						
Create Code Integrity policies					●		
Digitally sign Code Integrity policies							●
Deploy and Manage Code Integrity policies	●	●		●			
Version Control Code Integrity policies		●					
Create Catalog files						●	
Digitally sign Catalog files							●
Deploy and Manage Catalog files	●	●		●			
Version control Catalog files		●					

Controlled Folder Access



Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

Scan history

No threats found.

0 0
Threats found Files scanned

Quick scan

[Advanced scan](#)

Virus & threat protection settings

You are using the settings that Microsoft recommends.

Protection updates

Protection definitions are up to date.



Controlled folder access

Protect your files and folders from unauthorized changes by unfriendly applications.



On



[Protected folders](#)

[Allow an app through Controlled folder access](#)



Exclusions

Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.



[Add or remove exclusions](#)



Configure controlled folder access

Configure controlled folder access [Previous Setting](#)

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2016, Windows 10 Versi

Options: Help:

Configure the guard my folders feature

Disable (Default) ▾

Disable (Default)

Enable

Audit Mode

Enable or disable controlled applications.

Enabled:
Untrusted applications can
in protected folders, such as th

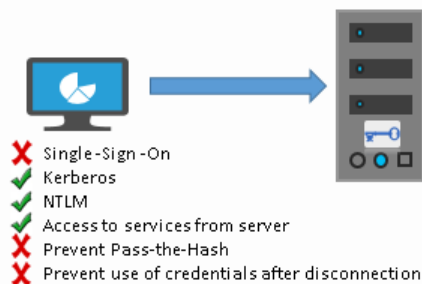
Disabled:

DEMO

NIC

Remote Credential Guard

Remote Desktop connection to a server without Windows Defender Remote Credential Guard



- Credentials sent to server
- Credentials are not protected from attackers on remote host
- Attacker can continue to use credentials after disconnection

🔑 = Credentials

Windows Defender Remote Credential Guard



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



- Credentials protected by Windows Defender Remote Credential Guard
- Connect to other systems using SSO
- Host must support Windows Defender Remote Credential Guard

Restricted Admin Mode



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

- Credentials used are remote server local admin credentials
- Connect to other systems using the host's identity
- Host must support Restricted Admin mode
- Highest protection level
- Requires user account administrator rights

 = Credential protection
 = Credentials

Support

- The Remote Desktop client device:
 - Must be running at least Windows 10, version 1703 to be able to supply credentials.
 - Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
 - Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
 - Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM. Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.

Support

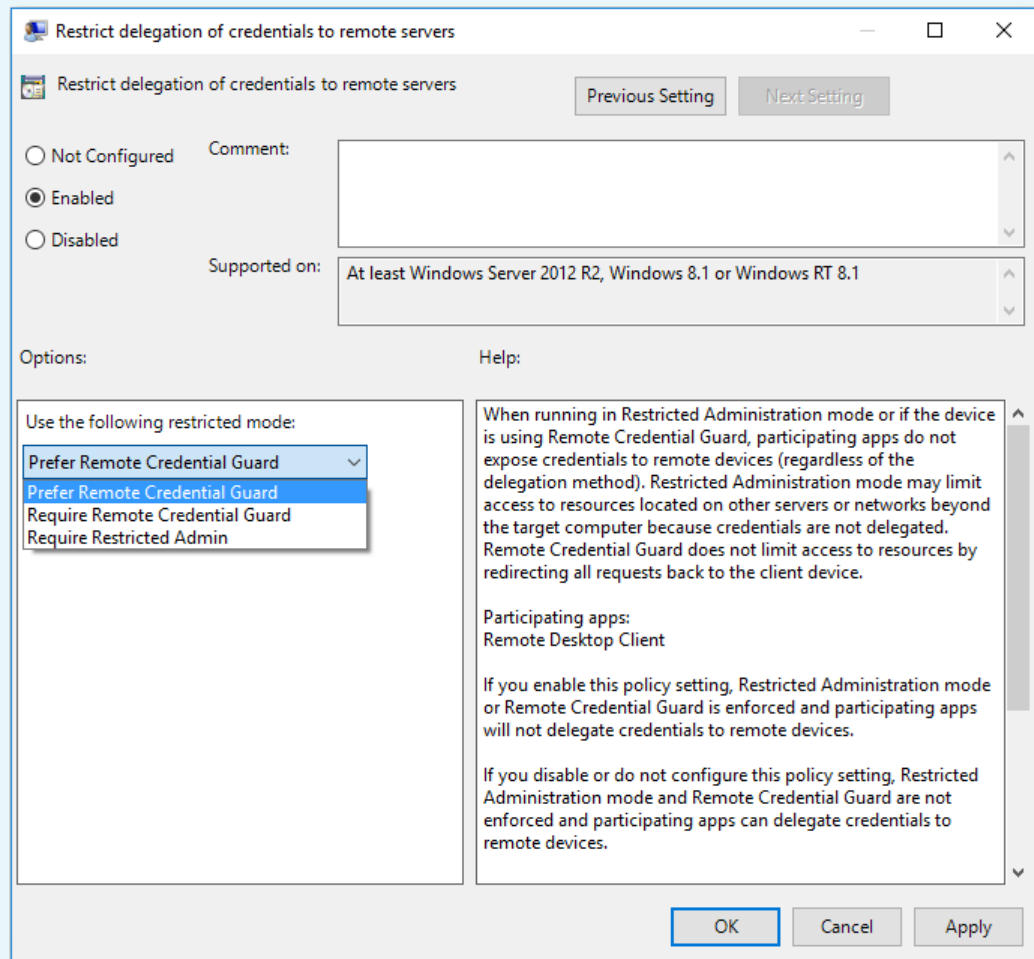
- The Remote Desktop remote host:
 - Must be running at least Windows 10, version 1607 or Windows Server 2016.
 - Must allow Restricted Admin connections.
 - Must allow the client's domain user to access Remote Desktop connections.
 - Must allow delegation of non-exportable credentials.

Turning it on

- You must enable Restricted Admin or Windows Defender Remote Credential Guard on the remote host by using the Registry.
 - Open Registry Editor on the remote host.
 - Enable Restricted Admin and Windows Defender Remote Credential Guard:
 - Go to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa.
 - Add a new DWORD value named **DisableRestrictedAdmin**.
 - Set the value of this registry setting to 0
 - Close Registry Editor.
 - Or:
 - `reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d 0 /t REG_DWORD`

Using it

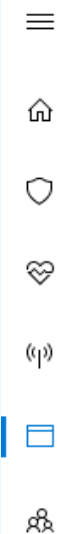
- Mstsc.exe /remoteGuard



More info

- <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/remote-credential-guard>

Exploit Guard (kind of EMET)



Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

System settings Program settings

Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

On by default

Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

On by default

[Export settings](#)

Exploit protection

See the Exploit protection settings for your system and p can customize the settings you want.

System settings Program settings

+ Add program to customize

ExtExport.exe
1 system override

ie4uinit.exe
1 system override

ieinstal.exe
1 system override

ielowutil.exe
1 system override

[Export settings](#)



Prepare for Forensics

Sysmon or 3rd party Cloud Services

- Sysmon is free but it doesn't itself have centralized logs or monitoring
- Advanced Threat Protection etc. from Microsoft
- Cylance etc.

Training, Training, Training

Training employees how to recognize and defend against cyber attacks is the most under spent sector of the cybersecurity industry — and yet it holds out the greatest hope for combating ransomware attacks.

91 percent of attacks by sophisticated cybercriminals start through email, according to Mimecast, a leading email security firm. Spear phishing attacks on employees are commonly used to infect organizations with ransomware.

“Training employees on security will immediately bolster the cyber defenses at most companies,” says Lawrence Pingree, a research director at Gartner, because most data breaches are based on “exploiting common user knowledge gaps to social engineer them to install malware or give away their credentials.”

Phishing identification training definitely bolstered Wells Fargo’s cyber defenses, notes Chief Information Security Officer Rich Baich. Through the use of various security awareness techniques, he says, workforce susceptibility to phishing declined by more than 40 percent.

Passwords

- New recommendations
 - <https://venturebeat.com/2017/04/18/new-password-guidelines-say-everything-we-thought-about-passwords-is-wrong/>
- Changes not as important anymore
 - Strong enough
 - **Different on different websites** (<https://haveibeenpwned.com>)
 - Password managers recommended

End User Training on Good Passwords

- For everyone
 - Minimum length of 8 characters (but don't advertise this)
 - Complexity required
 - Numbers
 - in the middle
- OR
 - at the beginning and end
- For important users like admins it's
 - Minimum length of 15 characters

End User Training on Good Passwords

- Show people <http://haveibeenpwned.com/> and teach to use different passwords on every site
 - Like
 - Flower10**Skype**Grows!
 - Flower10**Dropb**Grows!
 - Massively10Hard**IL**
 - Massively10Hard**PO**
 - Massively10Hard**BM**
 - **Even better, get a Password manager!**

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Blog: <http://blog.win-fu.com/>
- Free newsletter:
<http://eepurl.com/F-GOj>
- My trainings:
 - <https://win-fu.com/ilt/>
 - <https://win-fu.com/dojo/>



NIC