



RANSOMWARE



KATHY BELLEW – CYBER
SECURITY ANALYST

TRAVIS REDDICK – SYSTEM
ADMINISTRATOR

Silent Speaker (?)
JIM LONG – SYSTEM
ADMINISTRATOR

OBJECTIVES



Ransomware overview

Prevention

Discovery

Mitigation

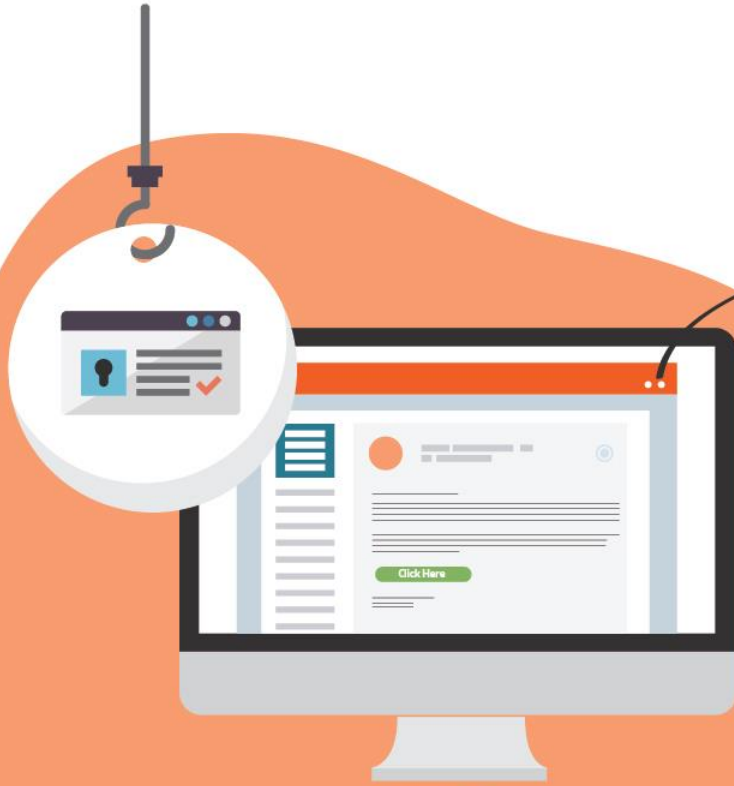
Recovery



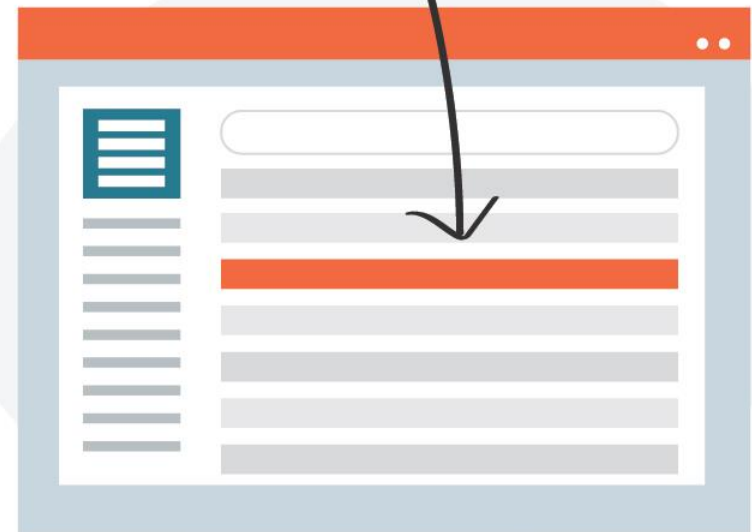
RANSOMWARE

ANATOMY OF AN ATTACK

LEVEL 1

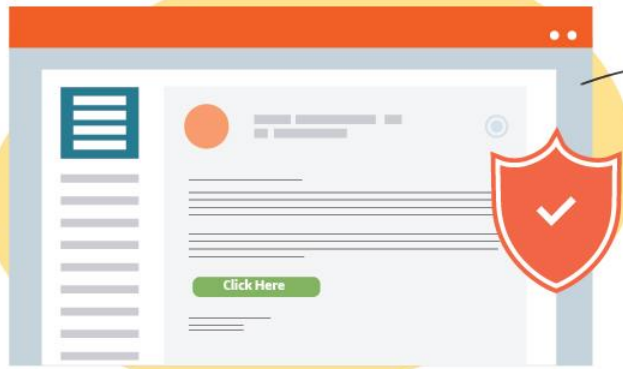


Attacker sends out a phishing email

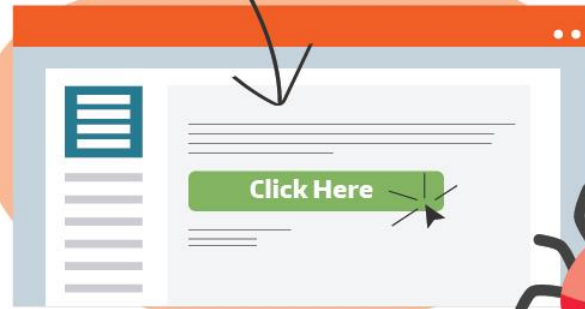


Bypassing the email spam filter, it lands in the user's inbox

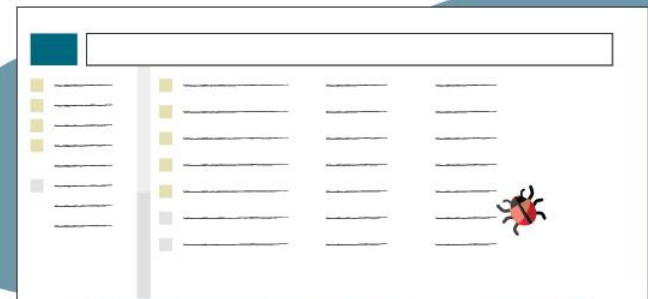
LEVEL 2



Anti-virus does not detect any problems with this email



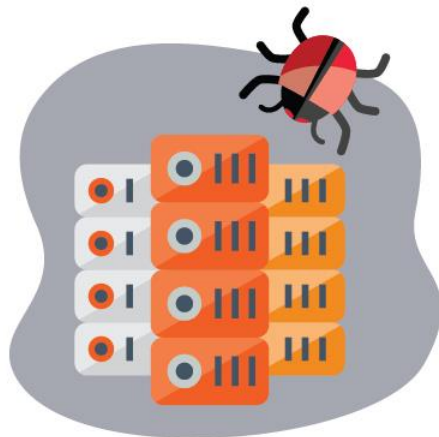
The user interacts with the malicious link or attachment



A copy of the malware is installed to the root drive, AppData or StartUp folders



Changes are made to the registry to run the executable



The malware connects with the Command and Control server



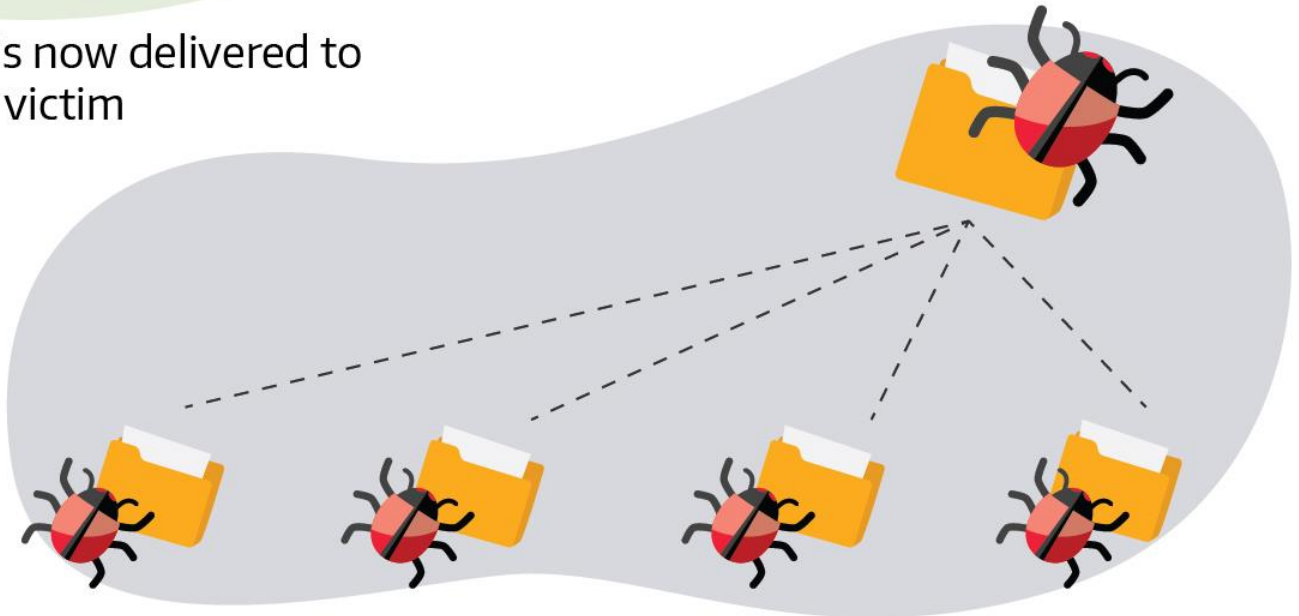
The executable runs and begins to encrypt data on the user's drive and shared drives

LEVEL 3



A ransom note is now delivered to the victim

Malware continues to spread across the network



EFFECTS

- System lock out
- Encrypted files
- Unresponsive system
- Spread
- Loss of data
- Money
- Time
- Reputation



PREVENTION

PREVENTION

- User training
- Host based
- 3rd party access
- Access controls
- Segmented access-flat network controls
- Host files
- Group policy
- Shared folders

PREVENTION

- Securing network applications
- Backups & shadow copies
- Images & virtual clones
- Wireless isolation
- GPO firewall rule, review after updates
- VPN
- Hardening
- Anti virus
- LAPS

USER TRAINING

- Phishing
- Security awareness
- Physical awareness
- Privacy

P
R
E
V
E
N
T
I
O
N

HOST BASED PREVENTION

- Patching
 - Firewall
 - Servers
 - Switches
 - End point
 - Wireless
- Anti-virus\anti-malware
- Auditing and monitoring
- Blackhole\Sinkhole DNS

P
R
E
V
E
N
T
I
O
N

Sinkhole/Blackhole DNS

- Available from MOREnet members using MOREnet connections
- Create your own Blackhole DNS
 - Windows DNS Sinkhole
 - <https://www.sans.org/blog/windows-dns-server-sinkhole-domains-tool/>
 - *Nix Blackhole DNS
 - <http://www.malwaredomains.com/bhdns.html>

P
R
E
V
E
N
T
I
O
N

Define Group Policy

- Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers.

Processing a Group Policy Object

- **L**
 - Local system policy is applied first
- **S**
 - Site policies are applied after the Local Policy
- **D**
 - Domain Policies are then applied
- **OU**
 - Organizational Units are applied last

P
R
E
V
E
N
T
I
O
N

GROUP POLICY OBJECTS - GPO

- Machine or User Policy
 - A computer policy applies to the computer itself and a user policy applies to the User logging in to the computer
 - Computer settings affect the computer and all users logging in to it
 - A user policy only applies to a specific user when they log into a computer, regardless of what computer it is

P
R
E
V
E
N
T
I
O
N

GROUP POLICY OBJECTS - GPO

What's the difference between Policies and Preferences?

- Group Policy Preferences provide better targeting, through item-level targeting and action modes.
- They enable you to deploy settings to client computers without restricting the users from changing the settings.
- It is a setting you would prefer the user takes on, but the user can still change it.

P
R
E
V
E
N
T
I
O
N

BLOCKING SOFTWARE WITH GROUP POLICY

- **Certificate:**
 - This allows the administrator to allow or disallow software dependent on the certificate associated with a software package.
- **Hash:**
 - Using the hash value for an application we can allow or deny the specific application. This prevents a user from being able to rename an application and then access it
- **Internet Zone:**
 - Specify whether to allow or deny applications from running when sites are within a specific Internet zone
- **Software path:**
 - Specify a location that users cannot launch applications

P
R
E
V
E
N
T
I
O
N

BLOCKING SOFTWARE WITH GROUP POLICY

Preventing users from running
programs using MD5 hash or the
path of the file name

P
R
E
V
E
N
T
I
O
N

GROUP POLICY OBJECTS - GPO

- White or Black list
 - White-Block all and allow only what is needed
 - Black-Allow all and only block specific paths

P
R
E
V
E
N
T
I
O
N

BLOCKING SOFTWARE WITH GROUP POLICY

- Prevent specific applications from being run by specific users or on computers
 - Reduce malware / spyware
 - Decrease use of unauthorized applications
- Restrict specific access to registry keys
 - Reduce malware / spyware
 - Increased Security

P
R
E
V
E
N
T
I
O
N

SOFTWARE RESTRICTION POLICIES

- Prevent access to these files
 - %windir%\system32\cmd.exe
 - %windir%\regedit.exe
- Restrict installation paths
 - %temp%
 - C:\temp
 - C:\windows\temp
 - C:\Users\%username%\Downloads
 - C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\
 - C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\

P
R
E
V
E
N
T
I
O
N

SOFTWARE RESTRICTION POLICIES..cont

- Mapped Drives: \\server\share
- Home Directory:
\\server\home\%username%
- External Drives: E:\, F:\
- %appdata%
- %localAppData%

P
R
E
V
E
N
T
I
O
N

Understanding and Using The Hosts File

- What is the hosts file?
- An ASCII text file that can be edited with a text editor
- It contains IP addresses separated by a space and then a domain name and performs a name to IP address mapping
- It was use to resolve URL to IP queries before DNS and has stayed. Can exists on windows, Mac, linux, and chrome
- On most devices the hosts file is examined first before DNS or the local cache

P
R
E
V
E
N
T
I
O
N

Why use Hosts File

- When you go to a site that's in your Hosts file, it will resolve the address a few milliseconds faster
- Where Hosts files really shine is by letting you block ads, spyware sites, malware sites, and tracking sites.

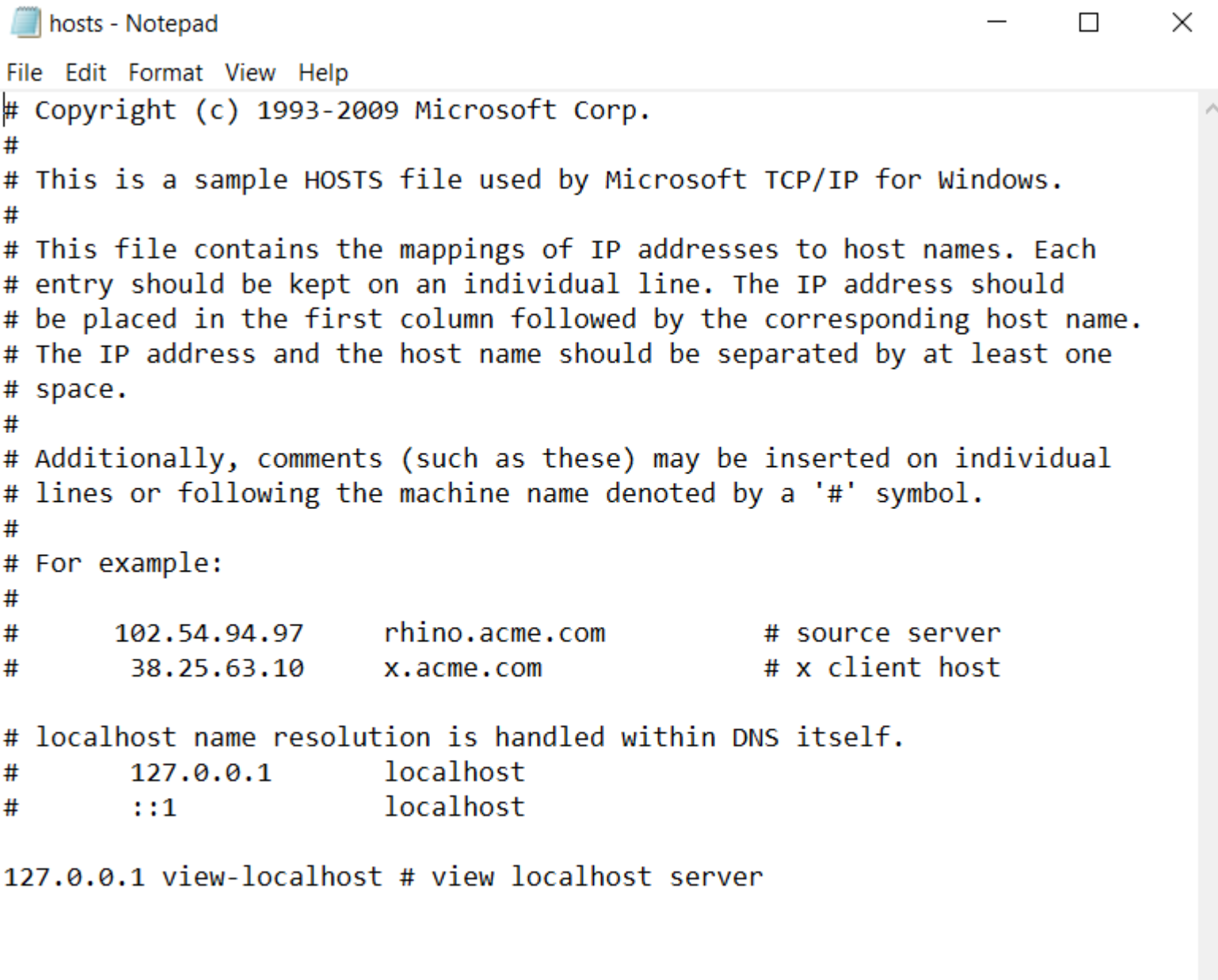
P
R
E
V
E
N
T
I
O
N

HOST FILES

- Deployed to every system via GPO

C:\windows\system32\drivers\etc

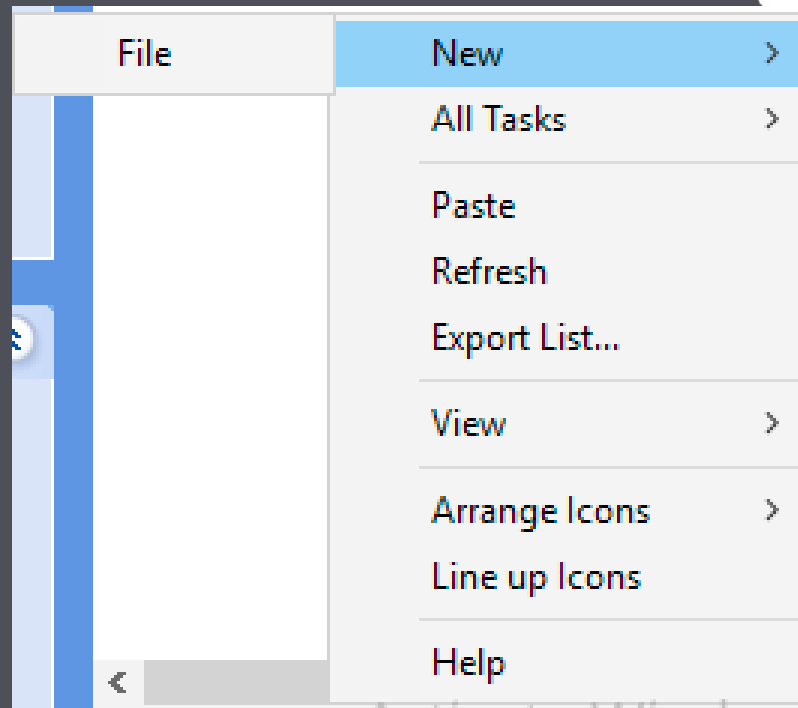
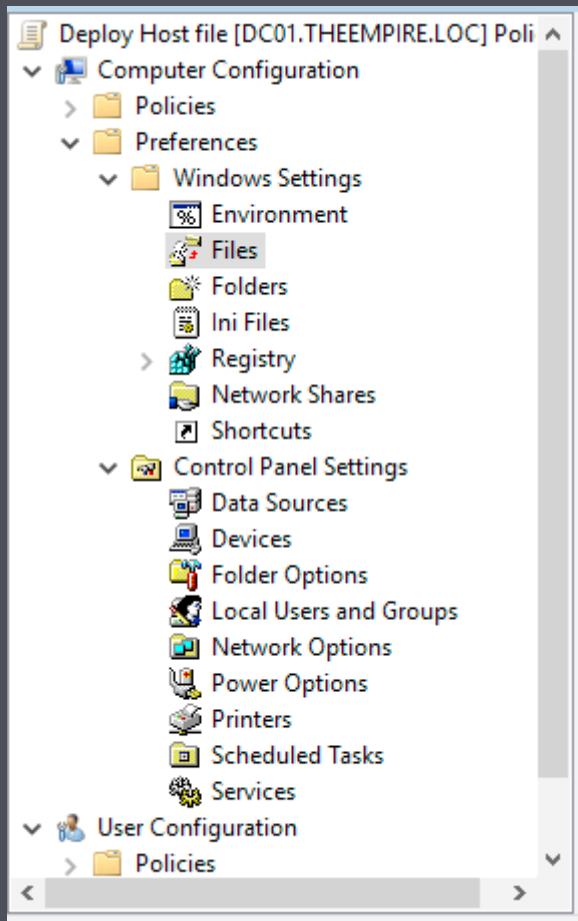
P
R
E
V
E
N
T
I
O
N



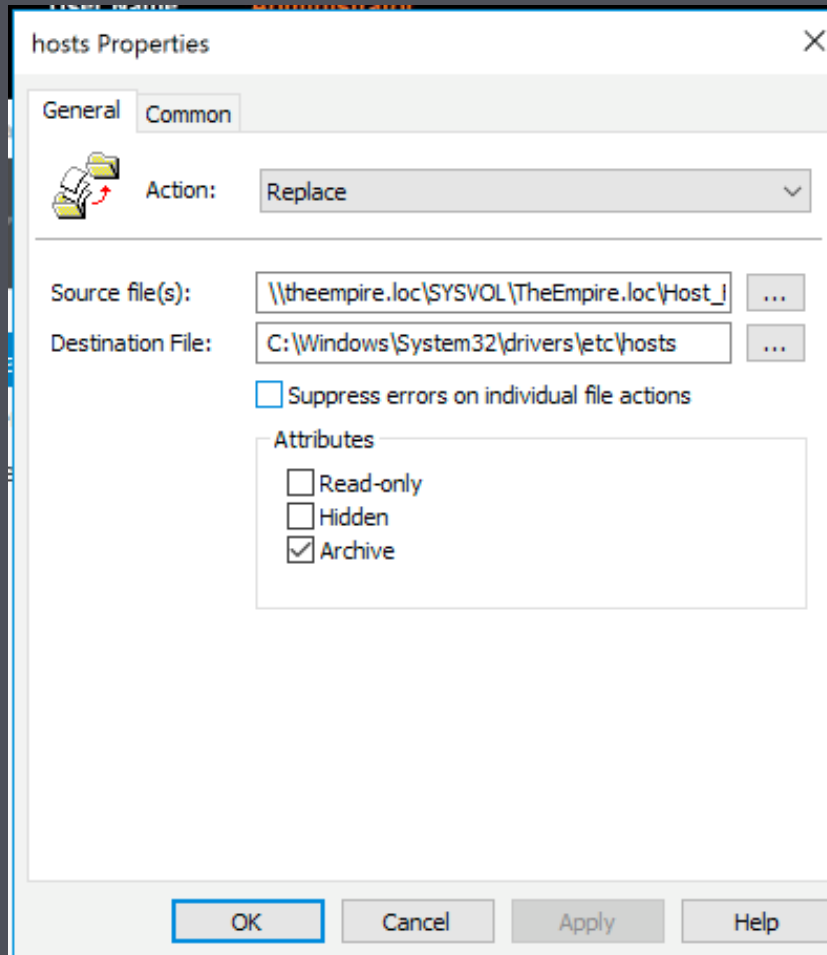
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#
127.0.0.1 view-localhost # view localhost server
```

Deploy Host File

P
R
E
V
E
N
T
I
O
N



Deploy Host File



P
R
E
V
E
N
T
I
O
N

Assigning Permissions

Permissions are privileges granted to users, groups or computers, enabling them to perform a task or access a resource.

Two sets of permissions that operate independently of each other are Share permissions and NTFS permissions.

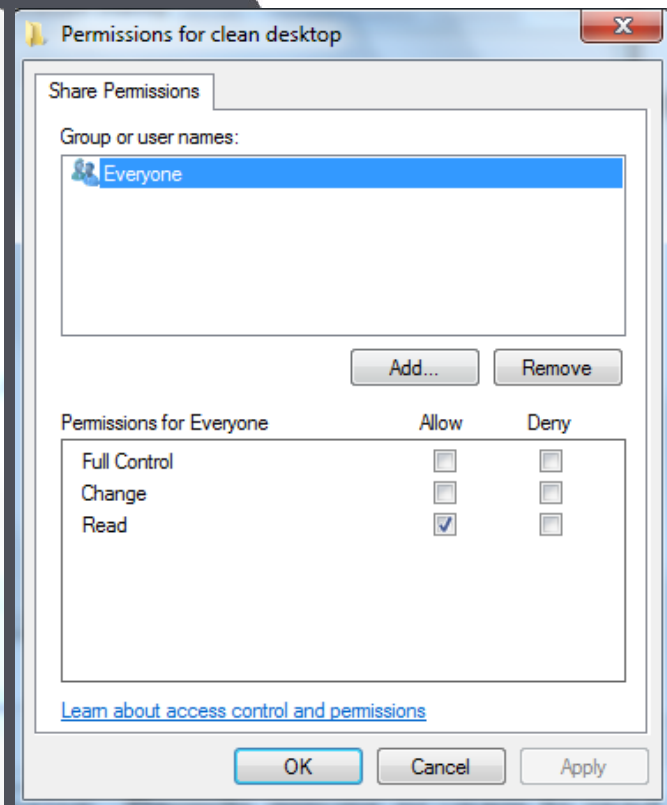
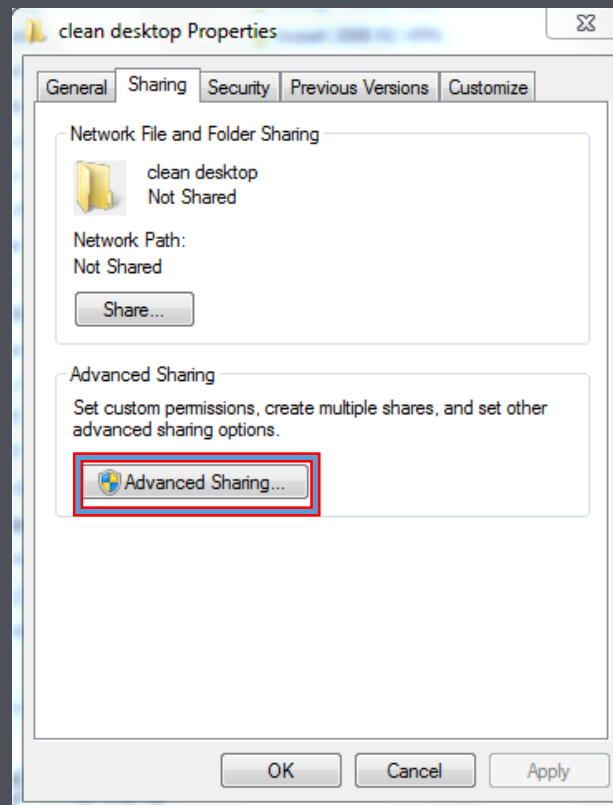
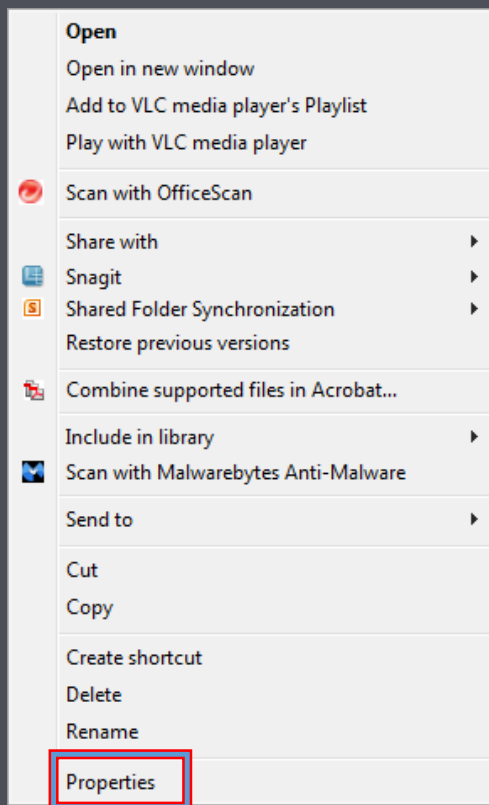
P
R
E
V
E
N
T
I
O
N

Assigning Permissions

- Share permissions - Designed to control access to folders over a network. Differ from the NTFS access permissions and are set through the Security tab
- NTFS - Control access to the files and folders stored on disk volumes formatted with the NTFS file system.
 - They are cumulative with the exception of permissions that are denied

Shared Files

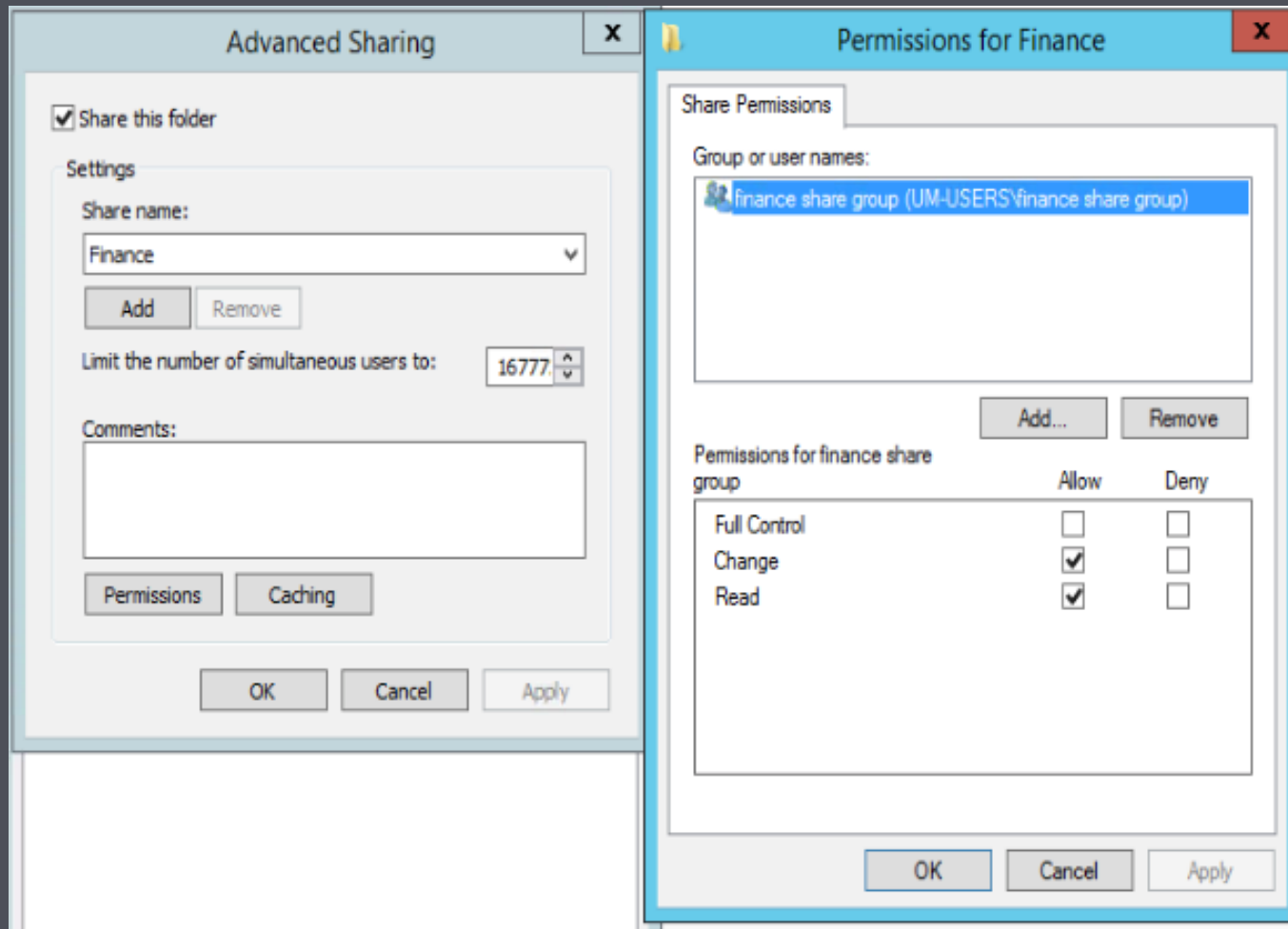
P
R



U
N

Shared Files Authenticated Users

P
R
E
V
E
N
T
I
O
N



Be better connected.

Shared Files

Considerations for Permissions

- Allowing and denying permissions.
 - How often do you review?
- Decide on a default way to grant access.
- Allow access through the share permissions or the NTFS permissions but not both.
- How will inheritance effective your system?
- Are there certain groups you want to implicitly deny?

P
R
E
V
E
N
T
I
O
N

3rd PARTY ACCESS

- Who has access?
- To what?

P
R
E
V
E
N
T
I
O
N

ACCESS CONTROLS

- Security templates
- Groups
- Restrictions
- Segmented access- flat network controls

P
R
E
V
E
N
T
I
O
N

RECOMMENDED SECURITY TEMPLATE GUIDELINES

Use Online Guides as reference to create the security settings that best fit your organization.

- NIST
- SANS
- MICROSOFT
- INFOSEC
- EDUCAUSE

P
R
E
V
E
N
T
I
O
N

APPLICATION SECURITY

- Identify Applications
 - Finance
 - Student Information
 - Mission Critical Data
- Assess the Risk
 - Risks of running the application
 - Remote access
- Audit User Access
 - GPO-restricted groups
 - Who has access
 - Set appropriate controls
- Updates and patches

P
R
E
V
E
N
T
I
O
N

BACKUPS & SHADOW COPIES

- Regularly scheduled backups
 - Incremental and full
 - Off site backups
- NO BACKUP SHOULD BE CONSIDERED VALID UNTIL TESTED
- Enable Shadow Copies

P
R
E
V
E
N
T
I
O
N

IMAGES & VIRTUAL CLONES

Virtualized servers are vulnerable to attacks the same as physical.

However, malware is designed to know if it is in a virtual environment and can be coded to take advantage and cause different types of attacks.

P
R
E
V
E
N
T
I
O
N

IMAGES & VIRTUAL CLONES-KEYS TO SUCCESS

- Design your environment with security in mind
- Manage network and storage isolation
- Good patch management
- Disable non-used hardware and technologies in the environment
- Physical security

P
R
E
V
E
N
T
I
O
N

WIRELESS ISOLATION

- VLANs
- Segmentation

P
R
E
V
E
N
T
I
O
N

HOST BASED FIREWALL RULES End Points

- Allow Administrative process
 - Active Directory, WSUS, Anti-virus, Print Server & Trusted IPs
- Block ALL other inbound connections
- Block outbound RDP

P
R
E
V
E
N
T
I
O
N

HOST BASED FIREWALL RULES

Server

- Block ALL inbound traffic
- Block inbound RDP
- Only allow trusted networks

P
R
E
V
E
N
T
I
O
N

VIRTUAL PRIVATE NETWORK-VPN

- Control access
 - Who?
 - Where?
 - What?

P
R
E
V
E
N
T
I
O
N

ANTI-VIRUS

Don't underestimate the importance of anti-virus, anti-malware and spam filtering

P
R
E
V
E
N
T
I
O
N

EMAIL

- Education
 - Spear phishing
 - Spoofing
- Port blocking – 25
- DKIM, SPF, DMARC

P
R
E
V
E
N
T
I
O
N

LOCAL ADMINISTRATOR PASSWORD SOLUTION – LAPS

Provides a solution to using a common local account with an identical password on every computer in the domain

P
R
E
V
E
N
T
I
O
N



DISCOVERY

DISCOVERY

- User reported
- System administrator
- Responding
- Source
- Scale
- File creation/ownership
- Logs

USER REPORTED

- Phishing email
- Strange behavior
- Unable to access files
- Unresponsive system

D
I
S
C
O
V
E
R
Y

SYSTEM ADMINISTRATOR

- Strange behavior
- Unable to access files
- Unresponsive system
- High CPU/memory usage
- Elevated permissions
- Encrypted files

D
I
S
C
O
V
E
R
Y

REPORTING

- Have a process in place for reporting
 - Who
 - What
 - Where
 - When

D
I
S
C
O
V
E
R
Y

SOURCE

- Origination
- Cause

D
I
S
C
O
V
E
R
Y

Be better connected.

SCALE

Identify affected devices
and users

D
I
S
C
O
V
E
R
Y

Be better connected.

FILE CREATION OWNERSHIP

Can help to identify point
of origination

D
I
S
C
O
V
E
R
Y



MITIGATION

MITIGATION

- Remove from network—do not reboot or log out
- Determine the scale and variant
- Determine attack vector



RECOVERY

INCIDENT RESPONSE PLAN

A DOCUMENTED PLAN WILL
ENABLE YOU TO PROCEED
THROUGH EACH OF THESE
PHASES WE DISCUSSED.
UNDERSTANDING THE
PROCESS WILL SAVE TIME,
MONEY AND MINIMIZE
DAMAGES.

RECOVERY

- Backups and snapshots
- Virtual-turn off and spin up new
- Virtual clones
- Verify clean prior to return to network
- Run AV scans on all network devices
- Change passwords
- Education & communication

RESOURCES

NIST- National Institute of Standards and Technology

- Guide to General Server Security

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistpecialpublication800-123.pdf>

- Detecting & Responding to Ransomware

<https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond>

- Identifying & Protecting Assets Against Ransomware

<https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect>

RESOURCES

- Microsoft -
<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>
- EDUCAUSE -
<https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program>

RESOURCES

- InfoSec

<https://www.infosec.gov.hk/english/technical/standards.html>

- SANS – SysAdmin, Audit, Network and Security

<https://www.sans.org/critical-security-controls/guidelines>

- MOREnet ftp

ftp://ftp.more.net/pub/S_P/Presentations/

RESOURCES

- GPO-Software restrictions -
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc507878\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc507878(v=technet.10)?redirectedfrom=MSDN)
- Creating an Application Whitelist
<https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/>

Where do I get the lists?

- MVPS Hosts
 - <http://winhelp2002.mvps.org/hosts.htm>
- hpHosts - powered by Malwarebytes
 - <https://hosts-file.net/?s=Download>



QUESTIONS



(800) 509-6673
www.more.net

