HITCON 17

RURAL HOSPITAL INFORMATION TECHNOLOGY CONFERENCE

Malware Archaeology

# Defending Against Ransomware and what can you do about it

Michael Gough – Founder

MalwareArchaeology.com

# Who am I

- Blue Team Defender Ninja, Malware Archaeologist, Logoholic
- I love "properly" configured logs – they tell us Who, What, Where, When and hopefully How

**Creator of**

**"Windows Logging Cheat Sheet"**

**"Windows File Auditing Cheat Sheet"**

**"Windows Registry Auditing Cheat Sheet"**

**"Windows PowerShell Logging Cheat Sheet"**

**"Windows Splunk Logging Cheat Sheet"**

**"Malware Management Framework"**

- Co-Creator of "**Log-MD" – Log Malicious Discovery Tool**
  - **With @Boettcherpwned – Brakeing Down Security PodCast**
- @**HackerHurricane** also my Blog

MalwareArchaeology.com

LOG–MD

# The Problem or Challenge We all Face

# Europol experts

- "***Ransomware attacks have eclipsed most other global cybercrime threats***, with the first half of 2017 witnessing ransomware attacks on a scale previously unseen following the emergence of self-propagating 'ransomworms,' as observed in the WannaCry and Petya/NotPetya cases," write Europol experts in the agency's Internet Organized Crime Threat Assessment (IOCTA 2017)

# Costs and Growth

- The FBI believes the total cost of ransomware broke the ***$1 billion mark in 2016***
- Whatever the motivation, ***new ransomware increased by 54%*** in the second quarter of this year, according to McAfee.
- The number of total new ransomware samples has ***increased by 47%*** in the past four quarters.

# The Numbers

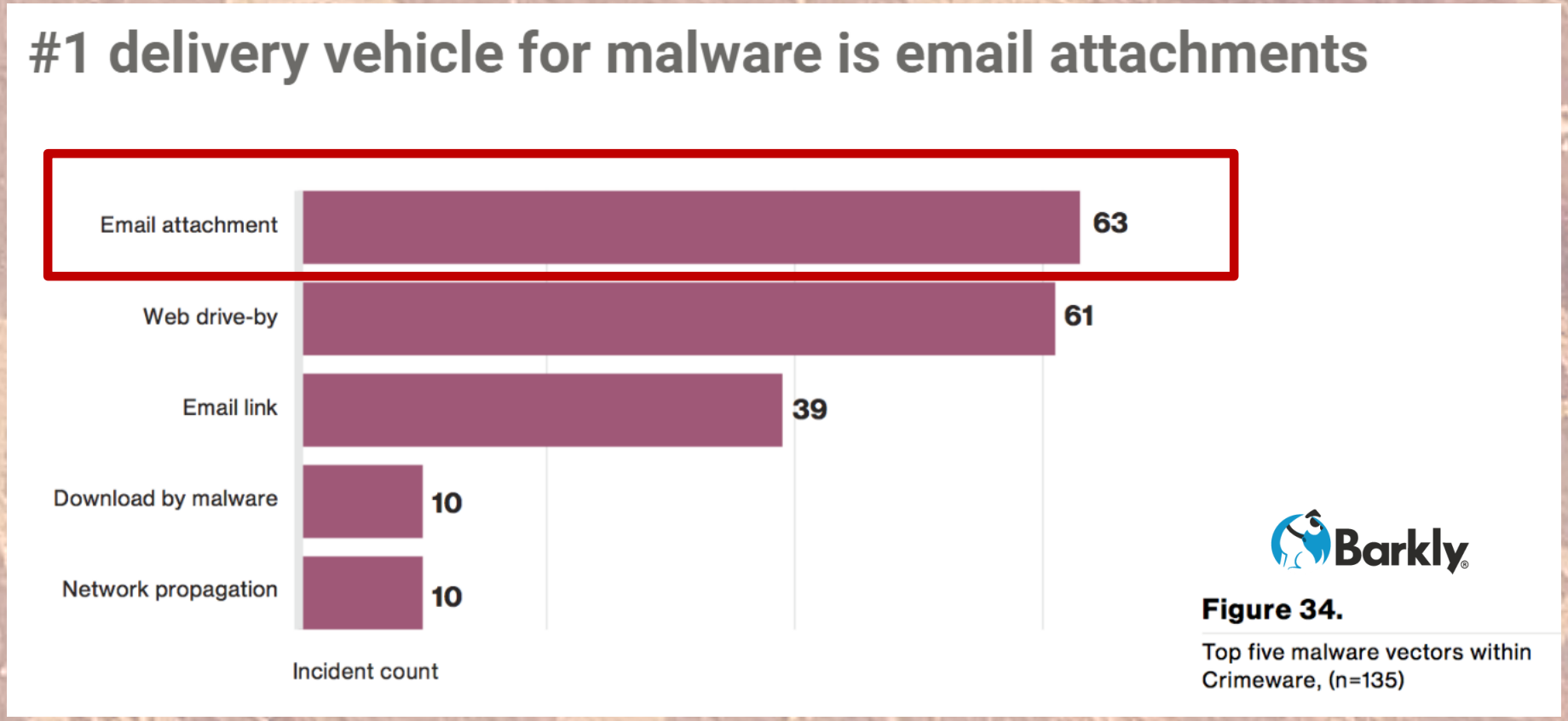
- ***80%*** of security pros view ransomware to be a ***moderate or extreme threat*** today. This is from a study of nearly 500 practitioners among the Information Security Community on LinkedIn, conducted by Cybersecurity Insiders and Crowd Research Partners.
- That survey showed that ***75%*** of organizations affected by ransomware have experienced up to ***5 attacks*** in the last year, and ***25%*** have been hit by ***6 or more attacks***.

# The Numbers

- The study showed that ***39% of organizations*** say it takes them anywhere between ***several days*** to a ***few weeks to recover*** from a ransomware attack.
- This lack of resiliency and the fallout from attacks this year highlight ***the lack of accountability for instituting the basics of IT security*** within organizations, says James Carder, CISO of LogRhythm.

# Email is #1

- Phishing IS our worst enemy



# Ransomware

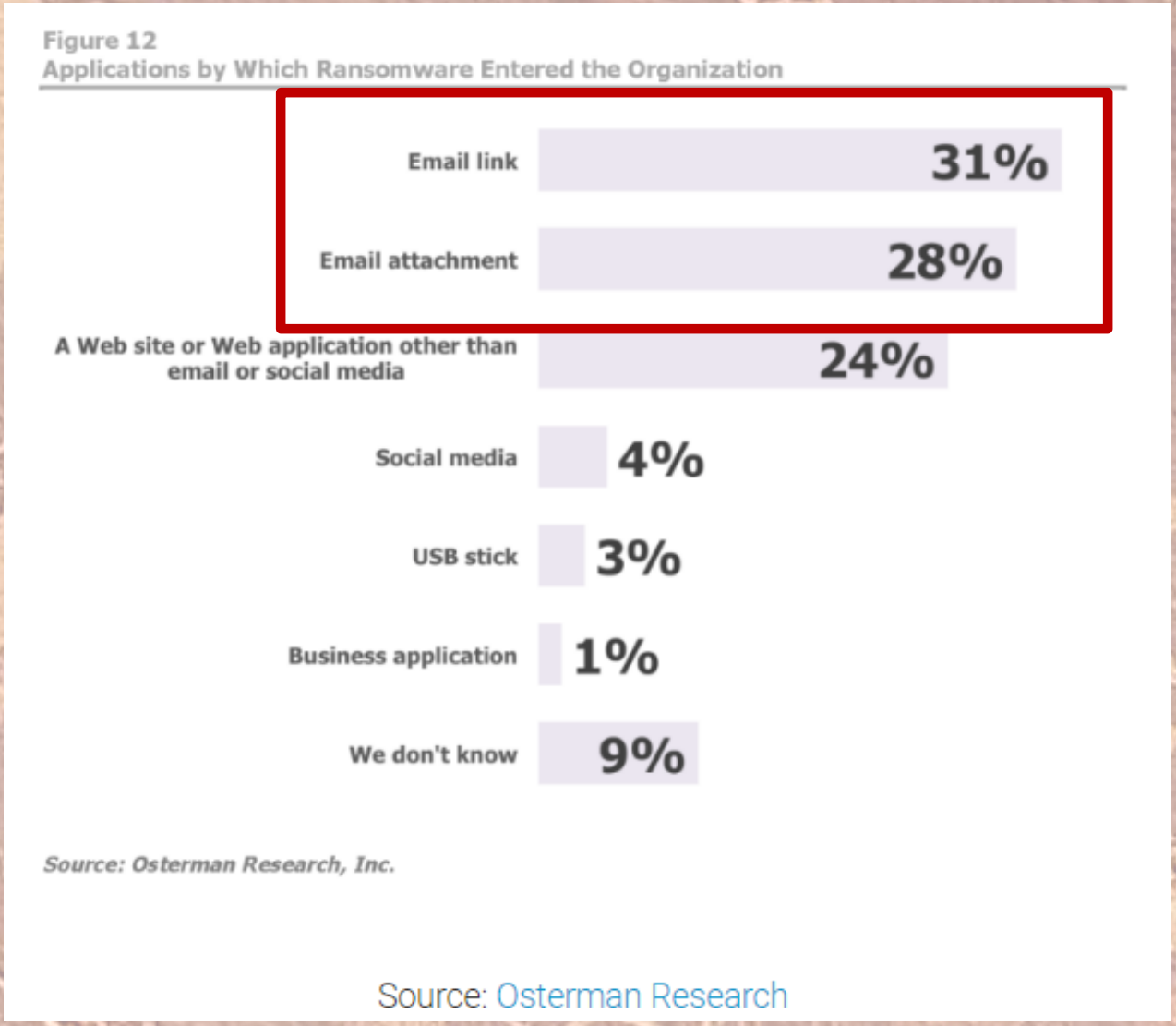


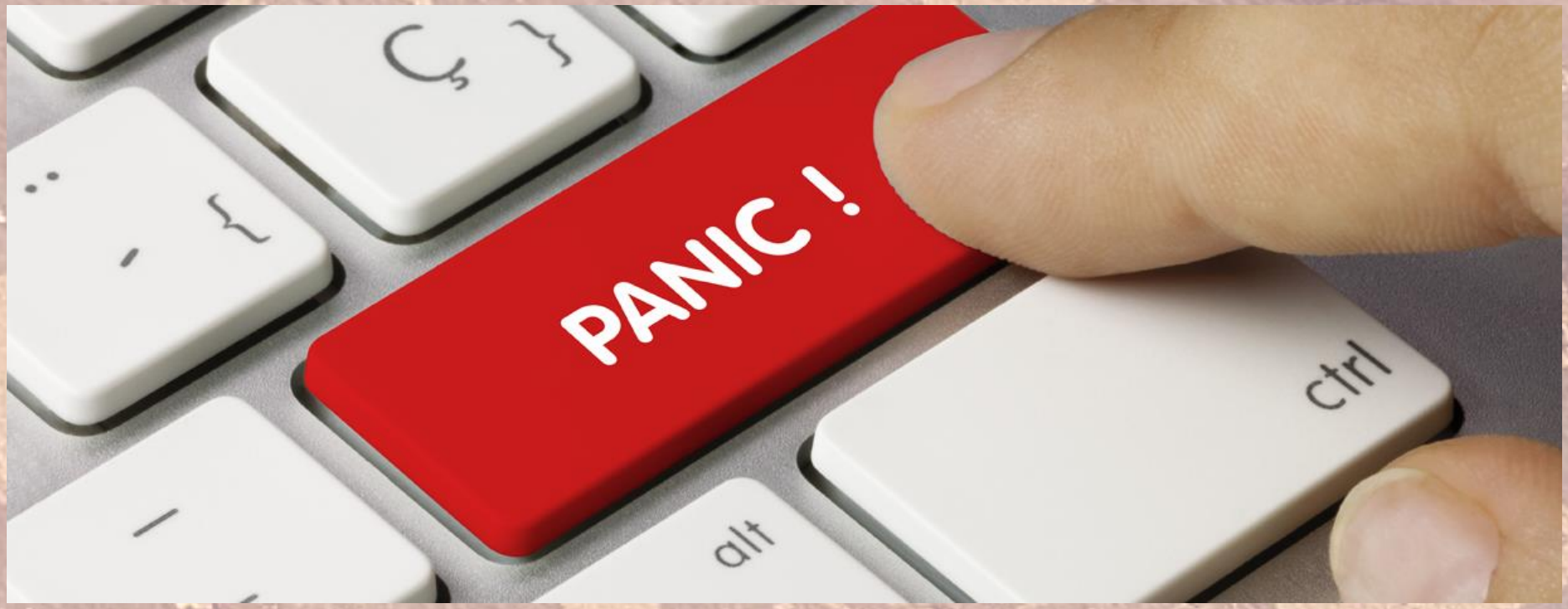
Figure 12
Applications by Which Ransomware Entered the Organization
Email link
31%
Email attachment
28%
A Web site or Web application other than email or social media
24%
Social media
4%
USB stick
3%
Business application
1%
We don't know
9%
Source: Osterman Research, Inc.
Source: Osterman Research

# Malicious Email

- Malicious Attachments
  - .js, .jse, .wsf, .wsh, .hte, .lnk, PS1, CMD, BAT, .vbs, .vbe, etc.
  - PDF, Word, Excel, etc.
- URL's in Email
  - Click ***HERE*** to see more
  - Then downloads the above file formats
  - Or sends you to a credential stealer webpage
- Encrypted emails
  - Same as above but protected with a password to bypass ***ALL*** security controls

# So what can we do?

# Don’t Panic



# Why does the criminals approach work?

# Understand WHY it works

- Email gateways do not block enough or anything
- Exchange and Outlook controls are seldom used
- Don’t forget users check personal email (Gmail, Yahoo, etc.)
- Yeah, executables are not allowed (.EXE)
- We do NOT do enough here and we should
- It’s FREE, your email gateway and Exchange server already have the capability
- Even Outlook has rules that can be enabled

# Take-Away #1
# File Type Blocks

# Outlook Rules

- You REALLY need to enable these
- https://support.office.com/en-us/article/Blocked-attachments-in-Outlook-3811cddc-17c3-4279-a30c-060ba0207372

- Block these on your
  Email Gateway !!!

- Drop these PLEEEASE

Attachment file types blocked in Outlook

| File name extension | File type |
|---|---|
| .ade | Access Project Extension (Microsoft) |
| .adp | Access Project (Microsoft) |
| .app | Executable Application |
| .asp | Active Server Page |
| .bas | BASIC Source Code |

# RansomWare/Malware

- Most malware/ransomware comes in via email attachments
- Some by drive-by surfing
- Most infections are because users ***double-click*** the attachment
- Dropping these will result in **90%+** reduction
- Do whatever you can to reduce these malicious file types at the email gateway or email server

# What Gets By File Type Blocks?

# If we drop these, what is left?

- Encrypted messages
  - These emails will get by ALL security solutions because they can't inspect encrypted emails (It's Haaarrd)
- Emails with URL's
  - URL's are generally not malicious with new campaigns in the first few hours
- They use Cloud Storage too
- Users download and ***Double-Click***

# What gets by file type blocks?

- Documents that have URL's that convince the user to download the file that would have been dropped if it were an attachment
- Encrypted Word/Office Docs that have Macros or OLE objects that are scripts
- **NEW** – DDE Links in Word Docs
  - Auto opens a URL and downloads a malicious file
- If the a file gets in this way, then we have to address what happens when a user **clicks it**

# Take-Away #2

# Block Macros

# PLEASE !!!!

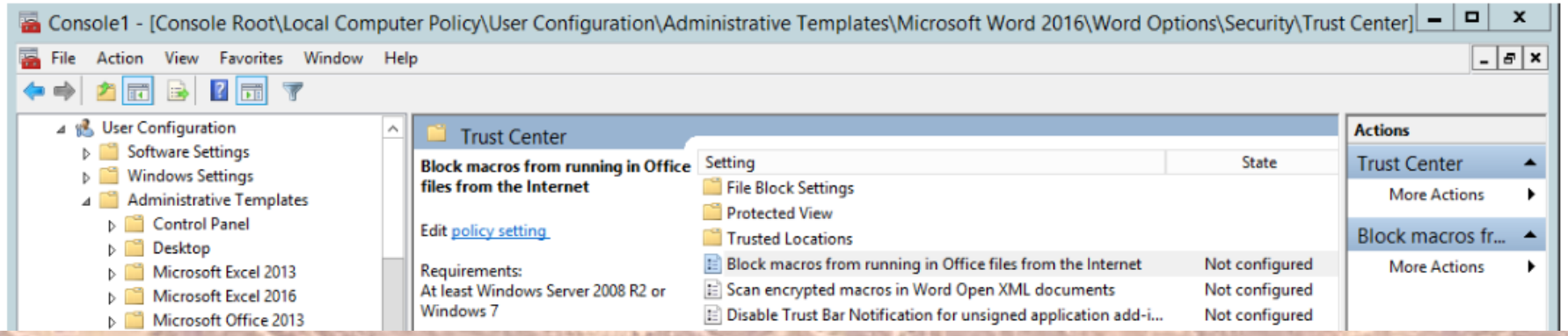
# Block Macros !!!

- For corporate users – Office 2013 or 2016 required

## Use Group Policy to enforce the setting, or configure it individually

Administrators can enable this feature for Word, Excel, and PowerPoint by configuring it under the respective application's Group Policy Administrative Templates for Office 2016. For example, to enable this setting for Word:

1. Open the Group Policy Management Console, right-click the Group Policy Object you want to configure and click **Edit**.
2. In the **Group Policy Management Editor**, go to **User configuration**.
3. Click **Administrative templates** > **Microsoft Word 2016** > **Word options** > **Security** > **Trust Center.**
4. Open the **Block macros from running in Office files from the Internet** setting to configure and enable it.



# Or tweak the registry

**Office 2016**

- HKCU\SOFTWARE\Policies\Microsoft\office\16.0\word\security
  HKCU\SOFTWARE\Policies\Microsoft\office\16.0\excel\security
  HKCU\SOFTWARE\Policies\Microsoft\office\16.0\powerpoint\security
  - In each key listed above, create this value:
    DWORD: blockcontentexecutionfrominternet  Value = 1

**Office 2013**

- HKCU\SOFTWARE\Policies\Microsoft\office\15.0\word\security
  HKCU\SOFTWARE\Policies\Microsoft\office\15.0\excel\security
  HKCU\SOFTWARE\Policies\Microsoft\office\15.0\powerpoint\security
  - In each key listed above, create this value:
    DWORD: blockcontentexecutionfrominternet  Value = 1

# #WINNING

- After adding these tweaks you will see this when you try and enable a macro and/or content

- You can unblock if truly needed and trusted, create an exception group

# There are More Than Macros

# More than Macros

- Macros account for a lot, but malwarians are morphing and evolving
- We blocked more than 6000 emails between June and Dec 2016
- They have moved to encrypted documents
- They have moved to documents with URL's
- They have moved to OLE objects in Word Docs
- They have moved to using Cloud Storage to retrieve documents
- **NEW** – They are using a DDE flaw to auto download URL's that have a file and get the user to click on the notification

# Why it Works

# Understand WHY it works

- Windows is Soooooooo broken
- The malwarians are taking advantage of the default configuration of Windows

- What happens when you ***Double-Click*** is the enemy
- Users have been trained to just **click it**
  - Click OK, click, click, click

# So how does it work?

- ***Clicking*** by users
- Yeah, Yeah, Yeah… User awareness training
  - It won't be enough

- How about this…
- Change what happens when users ***Double-Click*** a suspect file type
- Now there's a thought…

# Take-Away #3

# Deny the Double-Click

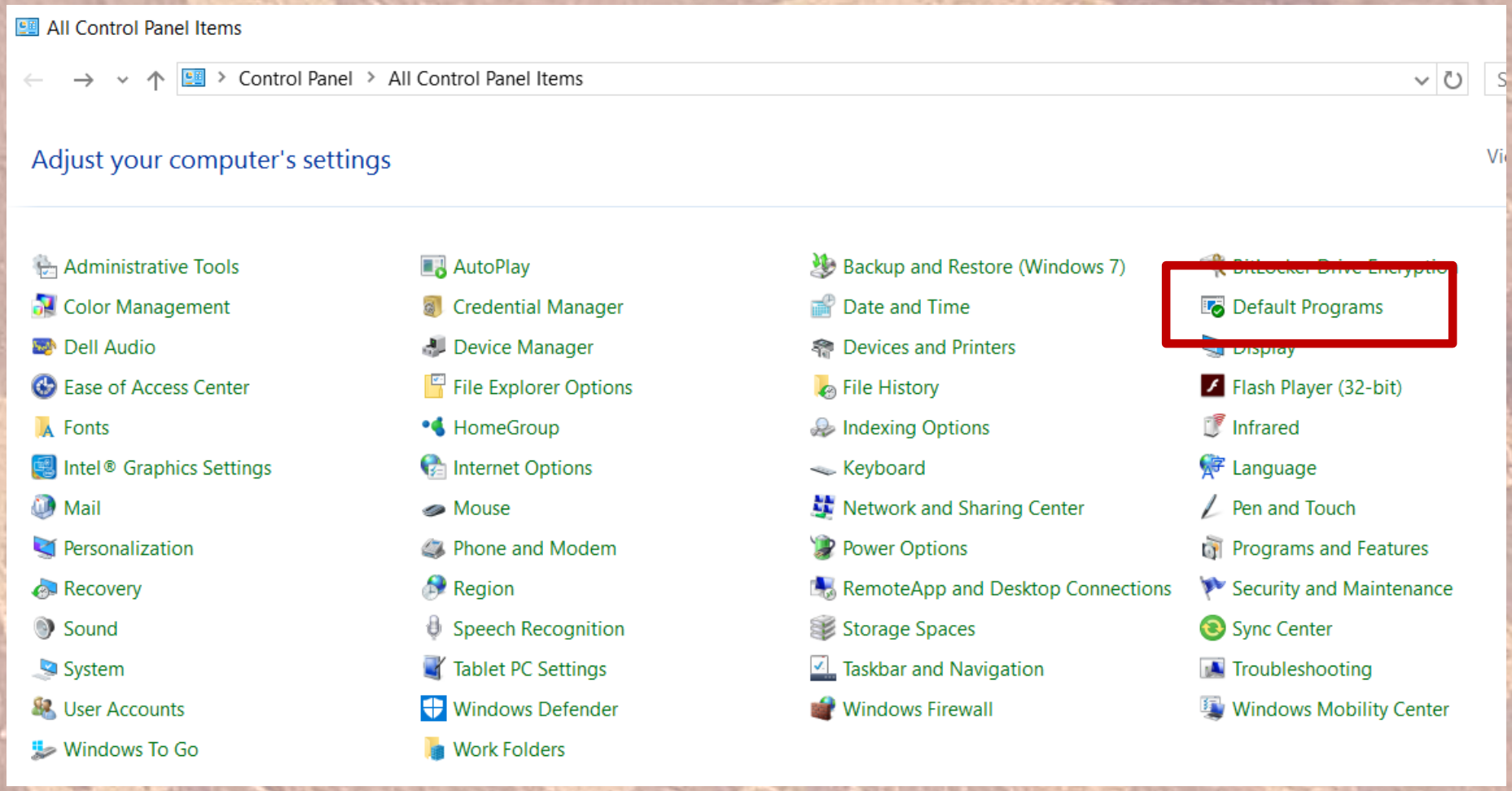
# Deny the Double-Click

- Windows allows by default the execution of a file type by double-clicking and launching the execution program (Boooooooo)
- So how about changing the dangerous file types that launch the interpreters to launching a simple editor?
- Yup, NOTEPAD to the rescue !!!!!
- Finally a good use for Notepad

# Deny the Double-Click

- This will NOT break the way these file types normally work.
- Cscript ‘Logon.vbs’ will work fine
- Double-Clicking ‘logon.vbs’ will just open Notepad
- You WILL need to convince IT, they haven’t played with this due to FUD and lack of experience
- Prove it by showing it works !

# Default Programs



# File Type

Control Panel > All Control Panel Items > Default Programs

## Choose the programs that Windows uses by default

Set your default programs

Make a program the default for all file types and protocols it can open.

Associate a file type or protocol with a program

Make a file type or protocol always open in a specific program.

Change AutoPlay settings

Play CDs or other media automatically

Set program access and computer defaults

Control access to certain programs and set defaults for this computer.

# Windows Based Script Host

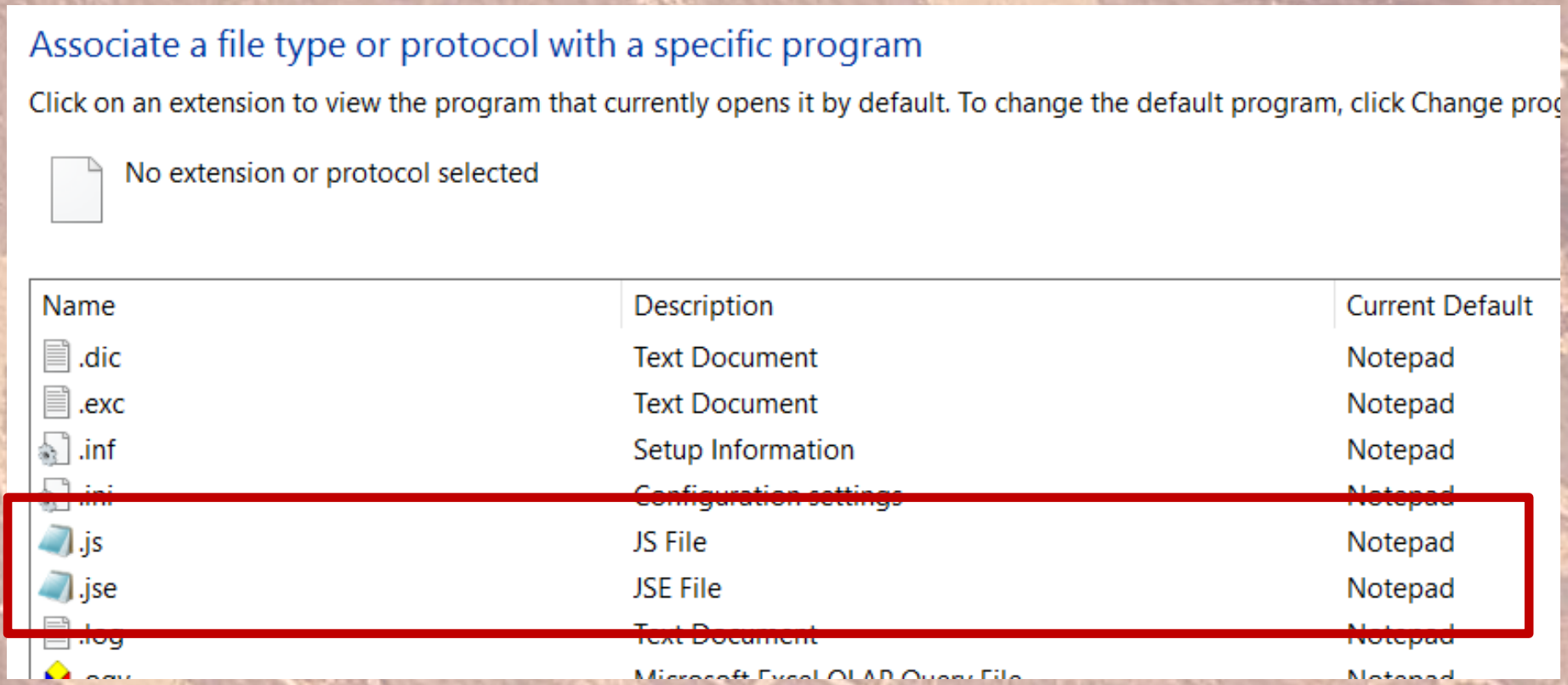
- Get rid of it, they use it to execute malware

| | | |
|---|---|---|
| .ms-windows-store-license | Windows Store License | LicenseManagerShellExt |
| .vbe | VBScript Encoded Script File | Microsoft ® Windows Based Script Host |
| .vbs | VBScript Script File | Microsoft ® Windows Based Script Host |
| .wsf | Windows Script File | Microsoft ® Windows Based Script Host |
| .wsh | Windows Script Host Settings File | Microsoft ® Windows Based Script Host |
| .accda | Microsoft Access Add-in | Microsoft Access |

- Consider .vbe, .vbs, .ps1 and .ps1xml too, but this is used in corporate environments
- This only affects double-clicking the file, not using the file properly (cscript Good_file.vbs)

# Change to Notepad

- Change ANYTHING that can execute a script to open Notepad



# So what happens?

- Users will open files that have been blocked, but got by either via an encrypted email or a URL in an email or attachment
- The user then downloads the malicious file type and double-clicks it… If it is one of the types that you have changed the File Association for, the malware script will FAIL !!!
- #WINNING

# Windows 10 upgrades

- Microsoft sometimes does full OS upgrades when they patch
- This will reset your File Association changes
- So use Group Policy (GPO) to set these
- If a standalone system (your home) then use a script I created that will set these and more
  - Create a scheduled task to run the script on logon to set them each time you begin work

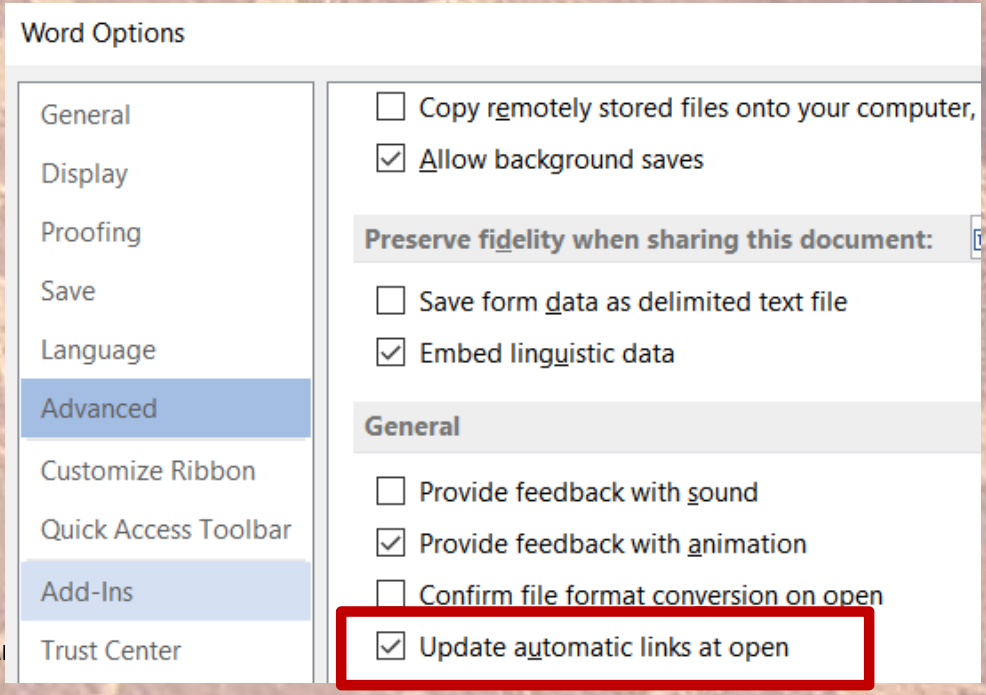
# Now What Can Get By?

# Take-Away #4

# Word DDE Attack

# DDE Links

- Word allows auto-execution of links to download content
- This is now being exploited HEAVILY !!!
- But easy to break!



# DDE Links

- Turn this off !!!!
- No need to automatically open links
- The user can right-click and manually update if it is an Excel Graph for example
- Disable using Group Policy
- Or the script from my website which also sets malicious file types to use Notepad
  - MalwareArchaeology.com\logging

# The 5%-10% that Can Get By

# What can still get by?

- Binaries (MZ, 4D5A, EXE)
- Yup, documents or emails that have URL's to a website or cloud storage will be allowed
- Browsers are doing a pretty good job of blocking .EXE downloads, or at least warning you
- The malwarians will use ZIP or 7Zip, Doc, or PDF files with or without passwords to get by the browser controls

# What can still get by?

- If a user gets an .EXE, then everything we have discussed thus far will not work, you can do:
  - Application Whitelisting - Complicated
  - Detect it and Respond – Logging and people
  - Next Gen Endpoint (EDR) protection - $$$$
- Maybe User Awareness can help as you can now focus the training since all the other ways they get in have been dealt with

# What can still get by?

- Lots of email is known bad
- Once a campaign is out for 4 hours or more, vendors start to add signatures to their advanced email filtering products to block known malicious emails
- Add these solutions to your email gateway AFTER you have implemented what is already recommended
  - FireEye
  - LastLine
  - Cisco AMP
  - Etc…
- If you add it first, you will tend to ignore the rest, which is best to do if you  REALLY want to reduce the threat

# Take-Away #5

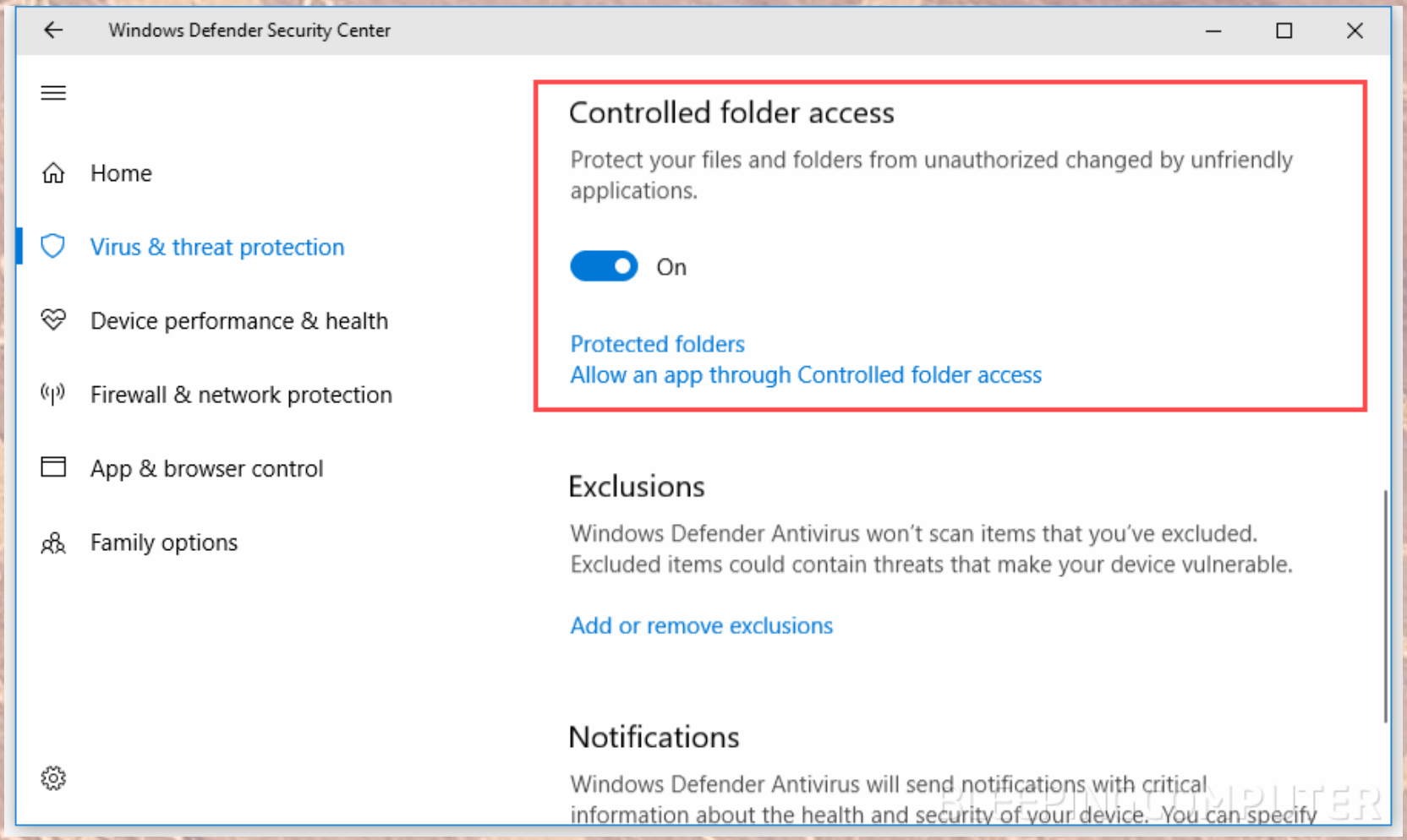
# New File Protection in Windows 10 - 1709

# New Feature in Windows 10

- Microsoft has now introduced ”***Controlled Folder Access”*** feature in its Windows Defender Security Center that is
- Available for Windows 10 Fall Creators Update (v1709)

- Basically folders that are protected with this wil be denied access to non-approved applications

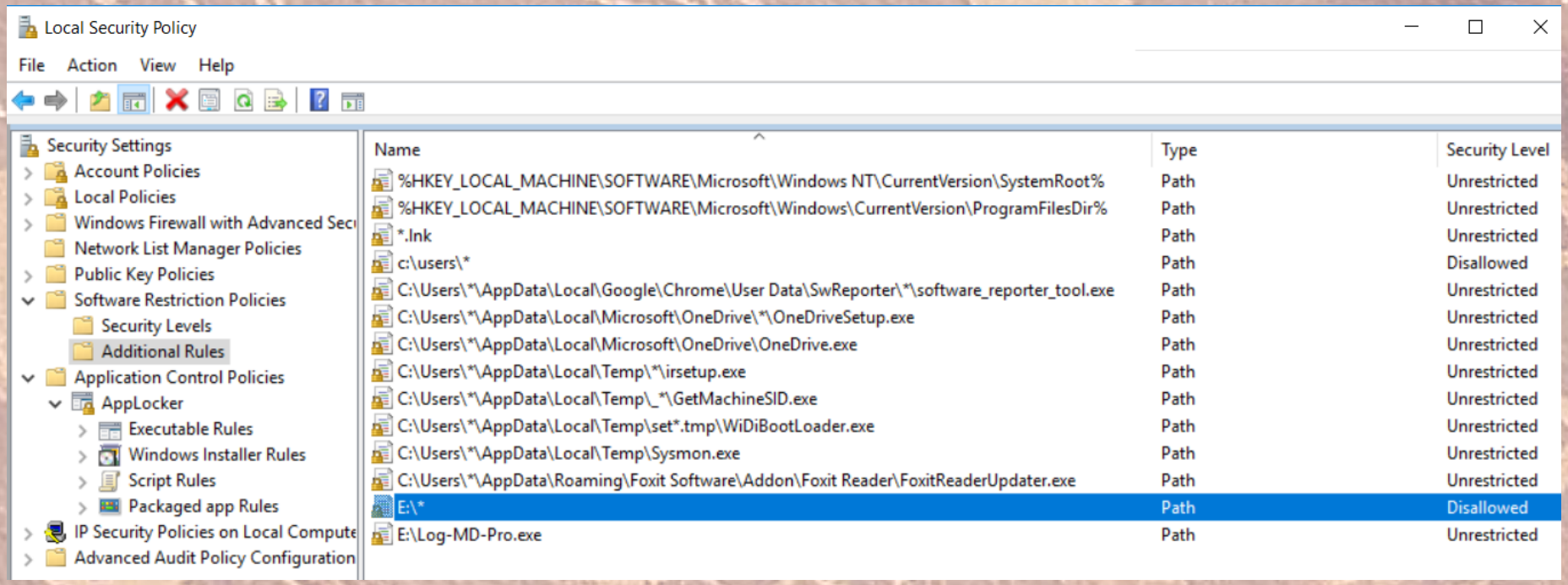
# New Feature in Windows 10



# Whitelisting

# Software Restriction Policies

- Block all executions from “C:\Users*”
- Block all USB executions from “E:*”



# Software Restriction Policies

- If you set to block like I do, then when you try to launch, install, or an update runs, it will fail
- Generates an Event ID 866 in the Application Log
- Copy the path that failed and create an exception if good and approved
- Be careful of over trusting generic paths
- Use a * to genericize an entry C:\Users*

# AppLocker

- ONLY works in Windows Enterprise versions
  - Boo Microsoft ;-(

- Has an Audit only mode (IDS) so can detect what would be blocked to allow you to tweak the policy before enforcing
- It does Dlls
- And it does Scripts

# User Awareness

# User Awareness

Teach them two things, and only 2 things

1. Don't open emails that have encrypted attachments AND have the ***<u>password in the body</u>*** AND contain a few words and not descriptive
2. ***Don't launch ANY .EXE files*** that you download from sources via email and links in emails or documents – EVER!

# Detection Options, Watch Incoming Email

# Alert on encrypted emails

- You heard me
- Setup an email alert to copy your InfoSec team on encrypted emails with attachments of:
  - Word
  - Excel
  - PDF
- Filter out the know good senders
- You will see campaigns coming in
- Tweak to prepend the subject with “Suspicious Email” once you made all your adjustments

# Malware/Ransomware Prevented

- If you do these simple things, which are all FREE, you will curb malware/ransomware infections by ***90-95% or more***
- This does not address malicious binaries .EXE files or .DLL files
- Whitelisting with Software Restriction Policies or AppBlocker will be needed for this

# What do we do with the attachments we receive?

# Evaluate them

- Splunk alerts looking at:
  - Same sender, multiple subjects or attachment names
  - Different senders same subject or attachment name
  - Encrypted Doc and XLS files
- Detonate them in a malware lab
- Obtain the artifacts to see who else might have open the ones that got through

# What do we use to quickly evaluate the malware?

# LOG-MD

## Discover it

- The Log and Malicious Discovery tool
- Audits your system and produces a report
- Also shows failed items on the console
- Helps you configure proper audit logging
- ALL VERSIONS OF WINDOWS (Win 7 & up)
- Helps you enable what is valuable
- Compares to many industry standards
- CIS, USGCB and AU standards and “Windows Logging Cheat Sheet”

# LOG-MD

## Discover it

Malware Archaeology

**Free Edition**

- Collect 1-7 days of logs
- Over 20 reports
- Full filesystem Hash Baseline
- Full filesystem compare to Hash Baseline
- Full system Registry Baseline
- Full system compare to Registry Baseline
- Large Registry Key discovery

# LOG-MD PROFESSIONAL

Malware Archaeology

- Over 25 reports
- Interesting Artifacts report
- WhoIS resolution of IPs
- SRUM (netflow from/to a binary)
- AutoRuns report with whitelist and Master Digest exclusions
- List of Locked files
- More Whitelisting
- Master-Digest to exclude hashes and files

# Resources

- Websites
  - **MalwareArchaeology.com**
  - **Log-MD.com** **The tool**

- The "***Windows Logging Cheat Sheet***"
  - **MalwareArchaeology.com**

- Script to set File Association, Break DDE and more
  - www.MalwareArchaeology.com\logging

# Questions?

- You can find us at:

- **@HackerHurricane**
- **@Boettcherpwned**
- **Log-MD.com**

- **MalwareArchaeology.com**
- **HackerHurricane.com (blog)**