One Page Checklist for Securing and Cleaning a Malware Infected Windows PC

Review and research all skill sets described below. To prevent immediate re-infection you may want to download/install *MBSA, WUA, MSE, PC Tools, MalwareBytes, Network Monitor, Snort, Sysinternals Suite, BotHunter, p0f or windump* first. This page is not domain administration relevant. This page does not describe malware or virus analysis. Recommended: **Microsoft Technet, Sysinternals, SRI** tutorials. Approximate tech labor time: 4 – 48 hours. Rev. 04.02.21010.001-RMF

Disconnect your machine from any network. Log in as a machine administrator.

- Remove all unused accounts and profiles. **'control sysdm.cpl' Select User profiles**
- Remove and/or properly configure all network shares. **'net share'**
- Configure auditing for professional versions per Microsoft's advice. **'control' Select Administrative Tools and Local Security Policy.**
- Review all event logs and take appropriate action **'eventvwr'**
- Clean-up your physical assets. Delete unnecessary folders and files, temporary directory contents, browser caches, old profiles, rebuild swap files. Remove file and folders from your desktops. Remove or disable suspected or infected restore points. Backup user data. Leave a minimum of 15% of each drive free.
- Clean up your SCM (*Service Control Manager*) profile. Disable unneeded services. **'mmc' Add Services**
- run *chkdsk /f* and *defrag* mercilessly. Reboot as necessary **'chkdsk /f' 'defrag'**
- Set up and configure Windows Firewall. Configure exceptions as necessary. **'mmc' Select Administrative Tools and Advanced Windows Firewall.**

Reconnect your computer to the internet.

- Install and run the latest *Microsoft Windows Updates* and *Malware Removal Tool*.

Reboot the PC.

- Install and run *PC tools Spyware Doctor* or *Microsoft Security Essentials*. Scan and remove virus/malware/exploits. Configure exclusions as needed.
- Install and run *Malwarebytes*. Scan and remove malware or dangerous configurations or files. Configure exlusions as needed.
- Plan, research and configure Security Templates . Deploy and test them as appropriate. **'mmc' Add Security Configuration; Analysis Add Security Templates**
- Research and configure file permissions as necessary. See tools at http://technet.microsoft.com/en-us/library/cc722416(WS.10).aspx
- Install and run *MBSA 2.1*. Follow recommendations as necessary and reasonable.
- Install and run *Sysinternals Suite* tools especially *autoruns.exe*. Remove unnecessary start up programs.

Reboot the PC if needed. Log in as an local administrator. Monitoring options:

- Run *Network Monitor* on the Local Machine. Run in promiscuous mode with conversations for all appropriate interfaces.
- Run *Procmon, Procexplorer, Sigcheck, AccessEnum* from *Sysinternals Suite.*
- Run *TCPView* and/or *TCPvcon* from *Sysinternals Suite.*
- Run *Snort* for Windows or (alternatively) **SRI's** *BotHunter.*
- Run *pOf, winpcap, windump.*

Run PC for 24 hours with maximum power and blank screen savers and network.

- Review and correlate all *Windows, Windows Firewall, network monitor, procmon, Snort, p0f, windump, BotHunter* output and logs.

Repeat steps from above as logging indicates. Look for successful and failed logins, unusual endpoints, snort signature detections, unsigned files, unusual object (svchost) requests. Optional: run **SRI's** *BotHunter* as needed. In this process, you are looking for outbound and inbound communication and connection attempts that seem suspicious – data transfers that you can not account for, processes that seem inexplicable, or unsigned files. You may or may not see logon attempts, registry changes, file creation, file access, file permission changes. You may need to correlate *Network Monitor* logs with network ingress and egress firewall logs. Additional info at:

- http://www.rmfnetworksecurity.com
- http://thinking-about-network-security.blogspot.com
- http://groups.google.com/group/small-business-threats