Limit access to Script Tools

CSC 4: Controlled Use of Administrative Privileges

Binary	Functions	Type
Atbroker.exe	Execute	Binaries
Bash.exe	Execute AWL bypass	Binaries
Bitsadmin.exe	Alternate data streams Download Copy Execute	Binaries
Certutil.exe	Download Alternate data streams Encode Decode	Binaries
Cmd.exe	Alternate data streams	Binaries
Cmdkey.exe	Credentials	Binaries
Cmstp.exe	Execute AWL bypass	Binaries
Control.exe	Alternate data streams	Binaries
Csc.exe	Compile	Binaries
Cscript.exe	Alternate data streams	Binaries
Dfsvc.exe	AWL bypass	Binaries
Diskshadow.exe	Dump Execute	Binaries
Dnscmd.exe	Execute	Binaries

Credit to LOLBAS Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

How is this thing configured?

CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	
Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	
Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.
Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

http://www.cisecurity.org/controls/