Incident Response Logs and Locations

Type	File	Location
Remote Access	Ntuser.dat	C:\Users\usrprofile
	USRclass.dat	C:\ Users\ usrprofile\AppData\Local\Microsoft)Windows
	(Security events) *.evtx	C:\Windows\System32\ Winevt\Logs
	(Prefetch) *.pf	C:\windows\prefetch
	(Terminal Server) * bmc* bin	C:\ Users) usrprofile\AppData\Local\Microsoft\Terminal Server Client\Cache
	(Jumplists)	C:\Users\usrprofile\AppData\Roaming\Microsoft\ Windows\Recent AutomaticDestinations
	(Shimcache) SYSTEM (Hive)	C:\ windows\ System32\Config
	Amcache.hve	C:\Appcompat\Programs\
Remote Execution	Security Events (*.evtx)	C:\ Windows\ System32\Winevt\Logs
	System Events	C:\Windows\System32\Winevt\Logs
	(Shimcache) SYSTEM (Hive)	C:\ windows\ System32\ Config\System\CurrentControlSet\Services\PSexesvc
	Amcache.hve	C:\Appcompat\ Programs\
	NTUSER.dat	C:\ Users\ usrprofile
	(Prefetch) *.pf	C:\windows\prefetch
Scheduled Tasks	Security Events (*.evtx)	C:\ Windows\ System32\Winevt\Logs
	(Shimcache) SYSTEM (Hive)	C:\ windows\ System32\Config
	Amcache.hve	C:\Appcompat\Programs\
	(Prefetch) *.pf	C:\windows\ prefetch
	SOFTWARE Hive	C:\ Windows\System32\Config\Microsoft\ WindowsNT) CurrentVersion\Schedule\ Tashcache
	Microsoft-windows-Taskscheduler%4Maintenance.evtx	C:\ Windows\ System32\Winevt\Logs
Remote Access Mapping Network Shares	Security Events (*.evtx)	C:\Windows\System32\Winevt\Logs
	Microsoft-Windows-SmbClient%4Security.evtx	C:\Windows\System32\ Winevt\ Logs
	Ntuser.dat	Software\Microsoft\ Windows \ CurrentVersion\Explorer\Mountpoints2
Services	Security.evtx	C:\ Windows\System32\Winevt\Logs
	System.evtx	C:\Windows\ System32\Winevt\Logs
	SYSTEM Hive	C:\ Windows\ System32\Config\CurrentControlSet\ Services(New Service Creation)
	ShimCache SYSTEM (Hive)	C:\windows\System32\ Config
	Amcache	C:\Appcompat\Programs\
	Prefetch *.pf	C:\Windows\ Prefetch
WMIC	Security.evtx	C:\Windows\System32\Winevt\Logs
	Microsoft-Windows-WMI-Activity%40perational.evtx	C:\Windows\System32\ Winevt\Logs
	ShimCache SYSTEM (Hive)	C:\Windows\ System32\ Config
	Amcache	C:\AppCompat\ Programs
	Prefetch *.pf	C:\Windows\ Prefetch
	Look for Unauthorized changes	C:\Windows\ System32\ wbem\Repository
Powershell Remoting	Security.evtx	C:\Windows\System32\Winevt\Logs
	ShimCache (SYSTEM) Hive	C:\Windows \System32\Config

	Amcache	C:\AppCompat\Programs
	Prefetch (wmic.exe.xxx.pf)	C:\ Windows\ Prefetch
	Microsoft-Windows-PowerShell%40perational.evtx	
	Windows Powershell.evtx	
	Microsoft-Windows-WinRM%40perational.evtx	
	Registry SOFTWARE (Hive)	C:\windows\System32\Config Microsoft\Powershell\1\Shellids\Microsoft.powershell\executionPolicy
Recent File Access	*.lnk files	C:\Users\usrprofile\Appdata\Roaming\Windows\Recent
	Ntuser.dat (Registry)	\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps
WebCache	WebcacheV*.dat	C:\Users\usrprofile\AppData\Local\Microsoft\Windows\WebCache
Usn Journal Files	C:\$Extend	
	C:\MFT	
	C:\$LogFile	
ShellBags	Usrclass.dat (Explorer)	\Local settings\Software\Microsoft\ Windows\Shell
	Ntuser.dat(Desktop)	\Software\Microsoft\Windows\Shell \BagMRU and \Bags
Run Commands	Ntuser.dat	\Software\Microsoft\ Windows\CurrentVersion\Eplorer\RunMRU
Time Zone	SYSTEM (Hive)	C:\ windows\system32\ config
		SYSTEM\CurrentcontrolSet\controlxx\TimeZoneInformation
Network History	SOFTWARE (Hive)	Microsoft\Windows\WindowsNT\CurrentVersion\ NetworkList\Signatures\Unmanaged & Managed and …. \NIa\Cache
Browser Searches	WebCacheV*.dat	C:\users\usrprofile\Appdata\Local\Microsoft\Windows\Webcache\WebCacheV*.dat
	Places.sqlite	C:\users\usrprofile\appdata\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\
Persistence	SOFTWARE Hive	Software\Microsoft\Windows\CurrentVersion\Run
		Software\Microsoft\Windows\CurrentVersion\Runonce
		Software\Microsoft\Windows\CurrentVersion\ RunOnceEx
		Software\Microsoft\Windows\CurrentVersion\ RunServicesOnce
		Software\Microsoft\Windows\Active Setup\Installed Components
		Software\WOW6432Node\ Microsoft\ Active Setup\Installedcomponents
		Software\Microsoft\Windows\CurrentVersion\ Explorer\SharedTaskScheduler
	SYSTEM Hive	System\CurrentControlSet\Services
		C:\ProgramData\Microsoft\ Windows\Start Menu\Programs\Startup
		C:\Users\Usrprofile\AppData\Roaming\Microsoft\ Windows\start Menu\Programs \Startup
IIS Logs		C:\Windows\ System32\LogFiles\W3SVC1
		C:\Inetpub\ogs\logfiles\

Useful Incident Response Commands

WMIC

- Product - Lists all software
- Baseboard - Lists Machine information
- Netlogin - Gets network login info
- Nic - gets network interface card info
- Nicconfig - gets mac addresses, IP and Gateway info
- Netuse - network mapped drives
- Netlogin - gets network login information
- Os - gets running OS
- Process - gets running processes
- Service - gets running services
- Share - gets running shares
- Startup - gets startup programs and locations
- Sysdriver - system driver(s) information
- Timezone - Gets timezone
- Useraccount - gets user account information

Net view \\127.0.0.1 (look at file shares and make sure each has a defined purpose)

Net Session (Look at who has an open session with the machine)

Net Use (look at which sessions this machine has opened with other systems)

Nbstat - S (looks at NetBIOS over TCP/IP activity)

Netstat-anob (looks for unusual listening TCP and UP Ports and owning process ID ('b' shows executables & DLLS)

Netsh firewall show config (Checks Windows Firewall configuration)

Schtasks (lock for unusual scheduled tasks)

Msconfig (look at startup tab for programs to launch at startup)

Lusrmgr.ms (look for unusual accounts in the admin group)

Net localgroup administrators

Doskey / History (shows command prompt history)

Arp -a-v (Shows arp cache) IP's to MAC addresses)

Ipconfig /all (displays current TCP/IP configuration)

Sysinternal Commands

Autoruns - See what programs are configured to startup automatically when your system boots and you login.

DiskExt - Display volume disk-mappings.

Diskmon - This utility captures all hard disk activity or acts like a software disk activity light in your system tray.

EFSDump - View information for encrypted files.

Handle - This handy command-line utility will show you what files are open by which processes, and much more.

ListDLLs - List all the DLLs that are currently loaded, including where they are loaded and their version numbers.

Livekd - Use Microsoft kernel debuggers to examine a live system.

LogonSessions - List the active logon sessions on a system.

ProcDump - This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

Process Explorer - Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor - Monitor file system, Registry, process, thread and DLL activity in real-time.

PsGetSid - Displays the SID of a computer or a user.

Psinfo - Obtain information about a system.

PsList - Show information about processes and threads.

PsLoggedOn - Show users logged on to a system.

PsLogList - Dump event log records.

PsService - View and control services.

PsTools - The sTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

RAMMap - An advanced physical memory usage analysis utility that presents usage information in different ways on its several different tabs.

Streams - Reveal NTFS alternate streams.

Strings - Search for ANSI and UNICODE strings in binary images.

Sysmon - Monitors and reports key system activity via the Windows event log.

TCPView - Active socket command-line viewer.

VMMap - VMMap is a process virtual and physical memory analysis utility.

VolumeId - Set Volume ID of FAT or NTFS drives.

Whois - See who owns an Internet address.