Артефакты Windows

Этап	Тип артефакта	Артефакт	Tool
Initial Access (Следы первичной компрометации)	**Факт открытия файлов**	NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU	RegRipper
		NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	RegRipper
		C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations	[C:\> JLECMD.exe -f <файл jump list>]
		C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\	[C:\> LECMD.exe -f <LNK файл>]
	История браузера	C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat - Internet Explorer	Esedatabaseview
		C:\%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles*.default\ - Firefox	DB Browser for SQLite
		C:\%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\ - Chrome	DB Browser for SQLite
	USB - устройства	C:\Windows\INF	USB Detective
		Amcache.hve	
		NTUSER.DAT	
		SOFTWARE, SYSTEM	
		Microsoft-Windows-Partition%4Diagnostic.evtx (ID 1006)	Windows Event Viewer, Event Log Explorer
	RDP bruteforce	Security.evtx (ID 4624, 4625, 4776, 4778, 4779, 4634, 4647)	Windows Event Viewer, Event Log Explorer
		Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx (ID 1149, 21, 22, 23, 24, 25, 39, 40)	
	Следы подключений по RDP	NTUSER.DAT|Software\Microsoft\Terminal Server Client\Servers	RegRipper
Execution (Следы запуска)	**Следы запуска**	C:\Windows\Prefetch	[C:\> PECMD.exe -f <prefetch файл>]
		SYSTEM|ControlSet001\Control\Session Manager\AppCompatCache	[C:\> AppCompatCacheParser.exe -f <AppCompatCache файл> --csv <директория вывода>]
		USRCLASS.DAT|Local Settings\Software\Microsoft\Windows\Shell\MUICache	RegRipper
		C:\Windows\appcompat\Programs\Amcache.hve	[C:\> AmCacheParser.exe -f <Amcache.hve> --csv <директория вывода>]
		NTUSER.DAT|Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	RegRipper
		HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}	Registry Explorer
		C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\L.<profile>\ActivitiesCache.db	[C:\> WxTCmd.exe -f <ActivitiesCache.db> <директория вывода>]

Этап	Тип артефакта	Артефакт	Tool
Persistence (Закрепление в системе)	**Run Keys**	NTUSER.DAT|Microsoft\Windows\CurrentVersion\Run	Registry Explorer
		NTUSER.DAT|Microsoft\Windows\CurrentVersion\RunOnce	
		SOFTWARE|Microsoft\Windows\CurrentVersion\Run	
		SOFTWARE|Microsoft\Windows\CurrentVersion\RunOnce	
	Startup Folders	C:\Users\<profile>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	FTK Imager
		C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup	FTK Imager
	Задачи (tasks)	C:\Windows\System32\Tasks\Task_Name	FTK Imager
		Microsoft-Windows-TaskScheduler%4Operational.evtx (ID 106, 140,141)	Windows Event Viewer, Event Log Explorer
	Службы (services)	Security.evtx (ID 4697)	Windows Event Viewer, Event Log Explorer
		System.evtx (ID 7034, 7035, 7036, 7040, 7045)	
	Logon Scripts	HKCU\Environment\UserInitMprLogonScript	Registry Explorer
	WMI Event Subscription	C:\WINDOWS\system32\wbem\Repository\OBJECTS.DATA	[C:\> wmi-parser.exe -i <OBJECTS.DATA> -o <директория вывода>]
Lateral Movement (Распространение по сети)	**Источник RDP соединения**	Security.evtx (ID 4648)	Registry Explorer
		Microsoft-WindowsTerminalServicesRDPClient%4Operational.evtx (ID 1024, 1102)	
		NTUSER.DAT|Software\Microsoft\Terminal Server Client\Servers	
		C:\Users\<profile>\AppData\Local\Microsoft\Terminal Server Client\Cache	[C:\> bmc-tools.py -s <Cache.bin> -d <директория вывода>]
	Назначение RDP соединения	Security.evtx (ID 4624, 4648, 4778, 4779)	Windows Event Viewer, Event Log Explorer
		Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx (ID 131, 98)	
		Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx (ID 1149)	
		Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx (ID 21,22,25)	
	Доступ к административным ресурсам	Security.evtx (ID 4648, 4624)	Windows Event Viewer, Event Log Explorer
		USRCLASS.DAT|Local Settings\Software\Microsoft\Windows\Shell\Bags	ShellBagsExplorer
		USRCLASS.DAT|Local Settings\Software\Microsoft\Windows\Shell\BagsMRU	
	PsExec. Источник	Security.evtx (ID 4648)	Windows Event Viewer, Event Log Explorer
		NTUSER.DAT|Software\SysInternals\PsExec\EulaAccepted	Registry Explorer
	PsExec. Назначение	Security.evtx (ID 4624, 4672, 5140)	Windows Event Viewer, Event Log Explorer
		System.evtx (ID 7045)	Windows Event Viewer, Event Log Explorer
		SYSTEM|CurrentControlSet\Services\PSEXESVC	Registry Explorer
		C:\Windows\psexecsvc.exe	Windows File Explorer
	WMI. Источник	Security.evtx (ID 4648)	Windows Event Viewer, Event Log Explorer
	WMI. Назначение	Security.evtx (ID 4624, 4672)	Windows Event Viewer, Event Log Explorer
		Microsoft-Windows-WMIActivity%4Operational.evtx (ID 5857, 5860, 5861)	Windows Event Viewer, Event Log Explorer

Memory Forensics

GROUP IB

	Создание дампа	[C:> DumpIt.exe /f D:\dump.raw] FTK Imager Lite(File>Capture Memory)
	VOLATILITY	
Общая информация	Профиль исследуемой системы	[vol.py -f dump.mem imageinfo]
	!Профиль необходимо использовать в каждой команде: --profile=<профиль>!	
	Список сетевых соединений	[vol.py -f dump.mem netscan] (connscan для WinXP)
	Дерево процессов	[vol.py -f dump.mem pstree]
Вредоносная активность процессов	Экспорт инжектированного вредоносного кода	[vol.py -f dump.mem malfind -D <директория вывода>]
	Экспорт DLL	[vol.py -f dump.mem dlldump -D <директория вывода>]
	Экспорт процесса	[vol.py -f dump.mem procdump -D <директория вывода> -p <pid процесса>]
	История команд cmd.exe	[vol.py -f dump.mem cmdscan] [vol.py -f dump.mem consoles] [vol.py -f dump.mem cmdline]
Исследование файлов	Информация о файлах	[vol.py -f dump.mem filescan > <имя файла>.csv]
	Исследование MFT	[vol.py -f dump.mem mftparser -D <директория вывода> --output=body --output-file= <имя файла>. csv]
	Экспорт файлов	[vol.py -f dump.mem dumpfiles -D <директория вывода>]
Исследование реестра	Экспорт файлов реестра	[vol.py -f dump.mem dumpregistry -D <директория вывода>]
	Значение ключа реестра	[vol.py -f dump.mem printkey -K «ключ реестра»]
Следы запуска	Userassist	[vol.py -f dump.mem userassist]
	Shimcache	[vol.py -f dump.mem shimcache]
	Shellbags	[vol.py -f dump.mem shellbags]