ANTCOLONY

Криминалистические артефакты Windows

Подсказки для системных администраторов

Разделы:

Registry Hives

Иерархические базы данных, в которых хранятся данные о конфигурации системы, приложения и пользователя

System Hives:
SYSTEM, SECURITY, SOFTWARE, SAM

System Hives Path:
%Systemroot%\System32\config\

User Hives:
NTUSER.DAT, USRCLASS.DAT

User Hives Paths:
\Users\\NTUSER.DAT, \Users\
\AppData\Local\Microsoft\Windows\USRCLASS.DAT

Интсрументы:
Regripper, Regedit (built-in), Registry Explorer

Registry Hive Mappings

SYSTEM	▶	HKLM\System
SOFTWARE	▶	HKLM\Software
SECURITY	▶	HKLM\Security
SAM	▶	HKLM\SAM

NTUSER.DAT	▶	HKEY_USERS\<SID>	▶ HKEY_CURRENT_USER
USRCLASS.DAT	▶	HKEY_USERS_Classes	▶ HKEY_CURRENT_USER \Software\ Classes

Разделы реестра конфигурации системы

Имя компьютера
HKLM\System\ControlSet###\Control\Computername\

Домен, Имя хоста, IP-адрес, DHCP-сервер
HKLM\System\ControlSet###\Services\Tcpip\Parameters\

Конфигурация файерволла
HKLM\System\ControlSet###\Services\Sharedaccess\Parameters\Firewallpolicy\

Привязка идентификаторов безопасности к пользователям
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\

Общие сетевые ресурсы
HKLM\System\ControlSet###\Services\Lanmanserver\Shares

Версия операционной системы и название продукта
HKLM\Software\Microsoft\Windows NT\Currentversion

Часовой пояс системы
HKLM\System\ControlSet###\Control\Windows

Пользователи, которые вошли в систему
HKLM\Software\Microsoft\Windows NT\Currentversion\Winlogon\Defaultusername, Altdefaultusername

Членство пользователей в группе Active Directory
HKLM\Microsoft\Windows\CurrentVersion\Group Policy\[USER_SID]\GroupMembership

USB-устройства хранения данных
HKLM\System\ControlSet###\Enum\USBSTOR\

Артефакты Совместимости Приложений

“Shim Cache” – содержит путь и время для файлов метаданных, которые выполнялись на системе

HKLM\SYSTEM\ControlSet###\Control\Session Manager\AppCompatCache\AppCompatCache

“Amcache” – содержит путь, время и хэш-метаданные SHA1 для файлов, которые запускались в системе

%Systemroot%\AppCompat\Programs\Amcache.hve

“Recent File Cache”– содержит путь к файлам, которые запускались в системе

%Systemroot%\AppCompat\Programs\RecentFileCache.bcf

Инструменты

Mandiant ShimCacheParser.py, AppCompatCacheParser, AmcacheParser, rfcparse.py

Общие разделы реестра автозапуска

Active Setup

HKLM\Software\Microsoft\Active Setup\Installed Components\
%APPGUID%

Библиотеки DLL AppInit

HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\AppInit_DLLs

Разделы запуска

HKLM\Software\Microsoft\Windows\CurrentVersion\Run, RunOnce

Службы и библиотеки DLL служб

HKLM\System\ControlSet###\Services\<Servicename>,<ImagePath>
HKLM\System\ControlSet###\Services\<Servicename>\Parameters,
<servicedll>

Расширения оболочки

HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions

UserInit

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit

ANTCOLONY

User Hive Registry Keys

Shellbags - Ключи в User Hive, которые отслеживают использование Explorer. Анализ может привести к получению метаданных доступного файла.

HKCU\Local Settings\Software\Microsoft\Windows\Shell\

Инструменты:
Shellbags.py, Shellbags Explorer

“Most Recently Used” or “MRU” keys

HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\RunMRU
HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\ComDlg32\ OpenSaveMRU

MUICache (недавно выполненные приложения)

HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\ MuiCache

Смонтированные тома и подключенные сетевые диски

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ MountPoints2\
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

Открытые документы

HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\ RecentDocs

Удаленный рабочий стол – история последнего доступа

HKCU\Software\Microsoft\Terminal Server Client\Default

TypedURLs (вводится вручную в Internet Explorer)

“HKCU\Software\Microsoft\Internet Explorer\TypedURLs” OR “… \TypedPaths” (Vista & later)

UserAssist (часто выполняемые приложения)

HKCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\UserAssist

Master File Table (MFT)

Сохраняет информацию о каждом файле и каталоге на томе NTFS

HKCU\Local Settings\Software\Microsoft\Windows\Shell\

Расположение:
\$MFT

Инструменты:
Acquire with FTK Imager, other raw disk access. Parse with MFT2CSV

INDX атрибуты

Содержит метаданные о файлах, хранящихся в каталоге.

Расположение:
$I30 files (a.k.a. “INDX” файлы) внутри каждого каталога

Инструменты:
Получить данные с помощью FTK Imager или другого инструмента для доступа к сырому диску.
Анализировать с помощью INDXParse.py

Инструментарий управления Windows

WMI может обеспечить сохранение вредоносных программ и записывать доказательства их выполнения

Расположение:
%systemroot%\System32\wbem\Repository\OBJECTS.DATA

Инструменты:
https://github.com/fireeye/flare-wmi/tree/master/python-cim

История браузера

Internet Explorer 10 & 11
C:\Users\\AppData\Local\Microsoft\Windows\WebCache

Google Chrome
C:\Users\\AppData\Local\Google\Chrome\User Data

Mozilla Firefox
C:\Users\\AppData\Roaming\Mozilla\Firefox\ Profiles\

Запланированные задачи

“SchedLgU.txt” Log: история запланированных задач, которые ранее выполнялись в системе
%systemroot%\tasks\SchedLgU.txt, Microsoft-WindowsTaskScheduler%4Operational.evtx

“.job” путь к файлу:
%systemroot%\tasks*.job

Инструменты
Текстовый редактор для «SchedLgU.txt», шестнадцатеричный редактор или «jobparser.py» для файлов «.job»

Предварительная выборка

Кэшированные данные для файлов, которые ранее выполнялись в системе.

Расположение:
%systemroot%\prefetch*.pf

Инструменты:
WinPrefetchView, strings

Распространенные местоположения аудио- и видеожурналов

McAfee:
%allusersprofile%\McAfee\DesktopProtection*.txt

Symantec:
: %allusersprofile%\Symantec\Symantec EndpointProtection\Logs\AVMan.log

Trend Micro:
HKLM\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\

Sophos:
C:\ProgramData\Sophos\Sophos Anti-Virus\logs\sav.txt

Windows Defender:
C:\ProgramData\Microsoft\Windows Defender\ Support*.log

Журналы событий

Встроенный в Windows механизм ведения журнала

HKCU\Local Settings\Software\Microsoft\Windows\Shell\

Ключевые журналы:
Журналы приложений, безопасности, системы, служб терминалов для подтверждения доступа по протоколу RDP (Microsoft-Windows-TerminalServices-LocalSessionManager, Microsoft-WindowsTerminalServices-RemoteconnectionManager);

Расположение:
%systemroot%\System32\winevt\Logs*.evtx

Инструменты:
Event Viewer (built-in), Microsoft Log Parser, Event Log Explorer (commercial)

Типы входа в Windows

Тип	Код
Interactive	2
Network Logons	3
Batch	4
Service	5
Unlock	7
NetworkCleartext	8
NewCredentials	9
RemoteInteractive	10
CacheInteractive	11

Коды журнала событий Windows

Сообщение статуса	Windows Vista/2008+
Scheduled Task Registered	106
Remote Desktop Auth Succeeded	1149
Audit Logs Clearedz	1102
Powershell Scriptblock contents	4104
Powershell Scriptblock start	4105
Powershell Scriptblock stop	4106
Network Logons	4624
Logon Using Explicit Credentials	4648
New Process	4688
Process Exit	4689
Scheduled Task Created	4698
Scheduled Task Deleted	4699
Scheduled Task Updated	4702
Service Start / Stop Control	7035
Service Running / Stopped	7036
Service Installation	7045

ANTCOLONY

Временные метки Windows

	$STD_INFORMATION			
	Modified	Accessed	Created	Entry Modified
Rename				X
Local Move				X
Volume Move		X		
Copy		X	X	
Access				
Modify	X			X
Create	X	X	X	X
Delete				

	$FN_NAME			
	Modified	Accessed	Created	Entry Modified
Rename	X			X
Local Move	X			X
Volume Move	X	X	X	X
Copy	X	X	X	X
Access				
Modify				
Create	X	X	X	X
Delete				