И.Б.БУРАЧЁНОК[1], Ф.П.ЦЫБУЛЬСКИЙ[2]

СПОСОБЫ ВЫЯВЛЕНИЕ ЦИФРОВОГО СЛЕДА В КОМПЬЮТЕРНОЙ СИСТЕМЕ

[1]*Учреждение образование «Полоцкий государственный университет имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь, заведующий кафедрой математики и компьютерной безопасности, кандидат технических наук, доцент*

[2]*Учреждение образование «Полоцкий государственный университет имени Евфросинии Полоцкой», г. Новополоцк, Республика Беларусь*

Расследование неправомерных действий с помощью средств информационных технологий предполагает вовлечение не только специалистов в области права, но и в области IT-наук. Исследование способов выявления цифрового следа (ЦС) в компьютерной системе (КС) и разработка новейших методов фиксации цифровых следов (ЦС) для работы в реалиях процесса эволюции и усложнения компьютерных систем являются актуальными.

Целью работы является исследование и анализ ценных цифровых следов, которые позволяют восстановить деятельность пользователя или вредоносного программного обеспечения (ПО) в КС.

Согласно проведенного анализа, основными компонентами, представляющими интерес для обнаружения ЦС являются внешние носители информации, такие как SSD и HDD и внутренняя энергозависимая память. Для структуризации ЦС была выбрана классификация А.Н. Колычевой [1], в которой выделяют 7 групп.

Первая группа – *файлы системного и прикладного программного обеспечения*. Например, для КС под управлением Windows можно получить перечень индексируемых программ с помощью утилиты "wmic" или графического интерфейса Windows.

Вторая группа – *файлы конфигурации программных приложений и операционных систем.* Если рассматривать ОС Windows, то она имеет иерархическую базу данных параметров – реестр. Наиболее информативным для выявления ЦС является набор

пользовательских и системных настроек, представленных в разделах реестра, таких как:

1. "HKEY_CURRENT_USER" (HKCU) – конфигурация учетной записи пользователя, которая хранится локально в файле ntuser.dat по пути "C:\Users\[user_name]" [2].

2. "HKEY_LOCAL_MACHINE" (HKLM) – конфигурации системы, устройств и драйверов для всех пользователей. "HKLM\CurrentControlSet\Control\TimeZoneInformation" – данные о временных зонах. "HKLM\System\CurrentControlSet\Services" – сведения о подключенных сервисах. Background Activity Moderator (BAM), сервис хранящий список записей SID с исполняемыми файлами в реестре по адресу "HKLM\SYSTEM\ControlSet00x\Services\bam\State\UserSettings\". Конфигурации драйверов – важные артефакты, представляющие собой ключи "HKLM\SYSTEM\DriverDatabase". Компонент ShimCache (AppCompatCache) обеспечивает обратную совместимость и хранит журнал по адресу "HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache" [2]. Список программ для автозапуска представлен в нескольких местах реестра, каждая ветвь реестра содержит приписку "run", например: "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run". Разделы HKLM хранятся локально по адресу "%SystemRoot%\System32\config". Эффективной программой для автоматизированного анализа реестра является FastIR Collector.

Третья группа – *файлы-журналы, создаваемые программным обеспечением в процессе работы*. "C:\ProgramData" и "C:\Users\[user_name]\AppData" – стандартные расположения записей ПО, однако существуют исключения. Примерами файла-журнала являются отчеты программы Windows Defender, они хранятся по адресу "C:\ProgramData\Microsoft\Windows Defender\Support". Журналы событий находятся по адресу "%SystemRoot%\System32\winevt\Logs". Они разделяются по назначению и сфере ответственности. К примеру, журнал "Microsoft-Windows-GroupPolicy%4Operational.evtx" хранит записи о сеансах групповой политики. Функционал допускается расширять при использовании утилиты "Sysmon". Управлять же журналами событий возможно через терминал с помощью утилиты "wevtutil".

Для примера, ОС Windows 10 управляет журналами Update Sequence Number (USN) – внутренними системными списками файлов NTFS. Новая информация записывается в конец потока журнала USN. Для каждого тома создается изолированный USN-журнал. Управление журналом USN осуществляется через утилиту "Fsutil". Подробный анализ предоставляется сторонним ПО "NTFS USN Journal parser".

Сервис Windows Prefetch собирает информацию с помощью перехвата исполняемого файла и библиотек, с предварительно выделенным пространством на накопителе. Записи ведутся по адресу "%SystemRoot%\Prefetch". Получить доступ к просмотру журналов возможно с помощью сторонних программ, таких как WinPrefetchView.

При обработке критических ошибок в ОС Windows создаются слепки памяти, содержащие список процессов, Pid, адреса памяти и другую информацию. Наиболее интересны 3 вида создаваемых слепков: Minidump (до 256 КБ) хранится по адресу "%SystemRoot%\Minidump", kernel crash dump и Completely memory dump по пути "%SystemRoot%". Эти слепки содержат полную информацию о протекающих

процессах и состоянии ядра КС. ПО "WinDBG" позволяет анализировать дампы памяти.

Также отдельно следует отметить имеющиеся автоматизированные инструменты по поиску ЦС на носителях. Например, Kroll Artifact Parser and Extractor (KAPE) широко применяется в форензике [2]. KAPE исследует носитель, экономя время на этапах расследования. Belkasoft X Forensic – аналог, который помимо функционала поиска, имеет удобные инструменты анализа ЦС.

Четвертая группа ЦС – *источники информации, образующиеся в ходе деятельности пользователя,* в том числе их резервные копии и удаленные файлы. Метаданные фотографий, документов и файлов – ценная информация для специалиста в области кибербезопасности. Метаданные хранят сведения о времени и месте создания документа, устройстве и учетных записях пользователей. Для работы с метаданными рекомендуется использовать программное обеспечение FOCA.

Можно также предложить для применения утилиты: Encryption Analyzer, предоставляющую инструменты по расшифровке контейнеров и EzyZIP, позволяющую экспортировать файлы из защищенного архива .rar и .zip форматов.

Система NTFS, как и многие другие, не стирают сам удаляемый контент, а только точку входа к нему из таблиц доступа. Недавно удаленную информацию можно полностью восстановить с помощью программы "RecuperaBit" по явным сигнатурам файлов.

Пятая группа – ф*айлы, обеспечивающие аутентификацию и конфиденциальность пользователей.* Для поиска паролей и ключей от криптоконтейнеров полезны все инструменты, указанные выше. Информация может храниться в менеджерах паролей, таких как "KeePass", однако обычно такие данные тщательно скрываются пользователем.

Шестая группа – *информация, находящаяся в оперативной памяти или файле подкачки устройства.* Для работы с Random Acces Memory (RAM) необходимо предварительно сделать слепок состояния [3]. Особенность RAM в том, что информацию она хранит не цельно, а по фрагментам. ПО Belkasoft live Ram Capturer позволяет снимать слепки RAM памяти. Набор утилит Volatility анализирует созданные ранее дампы памяти на предмет ЦС.

Седьмая группа – и*нформация, полученная с помощью соответствующих радиоэлектронных или специальных технических средств.* Для перехвата сетевого трафика используются роутеры-анализаторы с установленным ПО, таким как WireShark или SiLK. Для извлечения и слежения за пользователем используются устройства "KeyGrabber"-ы и т.п. Для каждого случая может понадобиться уникальный инструментарий специалиста цифровой криминалистики.

В представленной статье приведен далеко не полный перечень способов фиксации ЦС. Однако любая активность в цифровом пространстве оставляет следы и приведенные в статье способы выявление ЦС в КС позволяют специалистам информационной безопасности и юриспруденции эффективно решать проблему сбора данных и их анализа и создавать более гибкие методики ведения криминалистического следствия и защиты информационных ресурсов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Колычева, А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: автореф. канд. юрид. наук: 12.00.12 / А. Н. Колычева. – М. : 2019. – 25 с.

2. Muhibullah, M. Windows Forensics Analyst Field Guide. Packt publishing, 2023. – 318 с.

3. Пантюхин, И. С. Снижение объема обрабатываемой информации в энергозависимой памяти при исследовании компьютерных инцидентов. / И.С. Пантюхин, Н.И. Белов, В.А. Катаева // Вопросы кибербезопасности, 2018. – № 2(26), – С. 70–76.