Написание этой книги было очень увлекательным и сложным путешествием, и я искренне благодарна своей семье, друзьям и коллегам – всем, кто верил в меня и поддерживал всеми возможными способами. Отдельное спасибо моему другу и коллеге Олегу, который одним прекрасным зимним днем предложил мне написать книгу, положив начало этому путешествию.

– Светлана Островская

Я благодарен команде издательства Packt за эту возможность и, конечно, Светлане, принявшей этот вызов, – словами не выразить, как я рад, что в моей команде есть такие талантливые люди.

– Олег Скулкин

Оглавление

Предисловие от издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте *www.dmkpress.com*, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу *dmkpress@gmail.com*; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в издании новой книги, заполните форму на нашем сайте по адресу *http://dmkpress.com/authors/publish_book/* или напишите в издательство по адресу *dmkpress@gmail.com*.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от непонимания текста и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу *dmkpress@gmail.com*, и мы исправим их в следующих тиражах.

Нарушение авторских прав

Пиратство в сети Интернет по-прежнему является насущной проблемой. Издательство «ДМК Пресс» очень серьезно относится к вопросам защиты авторских прав и лицензирования. Если вы знаете о незаконной публикации какой-либо из наших книг в сети Интернет, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу *dmkpress@gmail.com*.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Об авторах

Светлана Островская – ведущий консультант по компьютерной криминалистике и реагированию на инциденты в компании Group-IB, одной из глобальных лидеров в области предотвращения и расследования высокотехнологичных преступлений и онлайн-мошенничества. Помимо активного участия в реагировании на инциденты, Светлана имеет богатый опыт преподавания в различных регионах, включая Россию, страны СНГ, Ближний Восток, Африку, Европу и страны Азиатско-Тихоокеанского региона. Она является соавтором статей по информационной безопасности и компьютерной криминалистике, а также ряда учебных программ, в т. ч. по криминалистике оперативной памяти, криминалистике Linux, криминалистике Windows, реагированию на инциденты и проактивному поиску угроз.

Олег Скулкин – руководитель лаборатории цифровой криминалистики и исследования вредоносного кода в компании Group-IB. Олег более десяти лет занимался компьютерной криминалистикой и реагированием на инциденты, киберразведкой и исследованием угроз. Является автором и соавтором многочисленных публикаций, а также регулярно выступает на отраслевых конференциях. Сертифицирован GIAC GCFA (сертифицированный специалист по цифровой криминалистике) и GCTI (сертифицированный специалист по киберразведке).

О рецензентах

Рохит Тамма – старший руководитель программы, сотрудник Microsoft. Более 10 лет работает в области безопасности, занимался менеджментом и консультированием в области безопасности приложений и облаков, безопасности мобильных устройств, тестирования на проникновение и безопасного кодирования. Рохит является соавтором книги «Learning Android Forensics», изданной Packt, где рассказывает о различных способах компьютерно-технической экспертизы на мобильных платформах. Связаться с ним можно через аккаунт в Твиттере @RohitTamma.

Игорь Михайлов занимается компьютерно-технической экспертизой уже 21 год. За это время посетил множество семинаров и учебных курсов в ведущих компаниях (в т. ч. Guidance Software, AccessData и Cellebrite) и отделах КТЭ в государственных организациях в России. Обладает опытом и навыками проведения КТЭ, реагирования на инциденты, КТЭ сотовых телефонов, КТЭ уничтоженных устройств, КТЭ вредоносных программ, восстановления данных, анализа цифровых образов, КТЭ видеозаписей, анализа больших данных и т. д. Принимал участие в проведении нескольких тысяч компьютерно-технических экспертиз. В работе применяет передовые инструменты и методы глубокого анализа. Использует программы и оборудование для КТЭ от ведущих отраслевых компаний. Написал три пособия по КТЭ сотовых телефонов и реагированию на инциденты на русском языке. Был рецензентом книги «Windows Forensics Cookbook» Олега Скулкина и Скар де Курсье, изданной Packt.

Предисловие

Криминалистика памяти – эффективный метод анализа, применимый в различных областях, от реагирования на инциденты до анализа вредоносного ПО. Для опытного специалиста память – важный источник ценных данных. Криминалистика памяти дает информацию о контексте, в котором работал пользователь, позволяет находить следы вредоносных программ, а в некоторых случаях еще и дает возможность собрать все кусочки головоломки и раскрыть сложную целевую атаку.

Авторы познакомят вас с основными концепциями криминалистики памяти, после чего постепенно перейдут к более сложным вопросам активного поиска угроз и исследования вредоносных программ с применением свободно распространяемых инструментов и фреймворков для анализа памяти. В книге принят практический подход и используются дампы памяти из реальных инцидентов. Это позволит лучше понять предмет и выработать навыки, необходимые для исследования и реагирования на инциденты, связанные с вредоносной активностью и сложными целевыми атаками. В книге затрагиваются вопросы внутреннего устройства Windows, Linux и macOS, а также обсуждаются методы и инструменты для обнаружения, исследования и активного поиска угроз с помощью криминалистики памяти.

Прочитав книгу, вы будете хорошо подкованы в вопросах криминалистики оперативной памяти и получите практический опыт использования необходимых техник и инструментов. Вы сможете самостоятельно создать и проанализировать дампы памяти, изучить действия пользователя, обнаружить следы бесфайловых вредоносных программ и установить действия, выполненные злоумышленниками.

Целевая аудитория

Эта книга ориентирована на специалистов по реагированию на инциденты и компьютерной криминалистике, на специалистов по кибербезопасности, системных администраторов, исследователей вредоносного ПО, студентов и энтузиастов, интересующихся исследованием оперативной памяти. Предполагается наличие базового понимания принципов работы вредоносных программ. Знание внутреннего устройства операционных систем будет полезным, но не является обязательным. В целом тем, рассмотренных в данной книге, будет вполне достаточно для начинающих.

Структура

В главе 1 «Зачем нужна криминалистика памяти?» объясняется, почему криминалистика памяти является неотъемлемой частью исследования многих современных компьютерных инцидентов. На реальных примерах описываются

основные цели и методы исследования, применяемые специалистами по компьютерной криминалистике и реагированию на инциденты (DFIR), а также обсуждаются проблемы, с которыми они сталкиваются в повседневной работе.

В главе 2 «Создание дампов памяти» вы познакомитесь с основными методами и инструментами получения дампов оперативной памяти и связанными с этим проблемами. Кроме того, вы узнаете о плюсах и минусах анализа памяти «вживую» и дампов.

В главе 3 «Создание дампа памяти в Windows» обсуждаются соответствующие инструменты и их подходы к работе с памятью Windows. Даются советы по выбору подходящего инструмента и рассматриваются примеры их работы.

Методики, рассматриваемые в главе 4 «Реконструкция пользовательской активности», во многих случаях имеют первостепенное значение, потому что позволяют лучше понять, что происходит. Описываются методы, основанные на анализе не только активных процессов и сетевых соединений, но и частей реестра Windows и файловой системы, находящихся в памяти.

В главе 5 «Поиск следов вредоносных программ и их анализ» речь идет о том, что современные вредоносные программы стараются оставлять как можно меньше следов на диске, и именно поэтому анализ памяти становится критически важным элементом исследования. Объясняется, как искать следы вредоносных программ в памяти процессов, в реестре Windows, в журналах событий и в частях файловой системы, находящихся в памяти.

В главе 6 «Альтернативные источники энергозависимых данных» отдается должное тому факту, что не всегда возможно создать дамп памяти для анализа, однако всегда есть шанс найти часть энергозависимых данных на диске. Рассматриваются альтернативные источники таких данных в Windows, а также инструменты и методы их анализа.

В главе 7 «Создание дампа памяти в Linux» демонстрируются основные различия между процессами создания дампов памяти в Windows и Linux. Описывается конфигурирование инструментов для Linux и примеры их применения.

Глава 8 «Реконструкция действий пользователя» посвящена процессу реконструкции действий пользователя в системах на базе Linux, который несколько отличается от такового в Windows. Описаны способы выявления действий пользователя по дампам памяти Linux.

Главной темой главы 9 «Обнаружение вредоносной активности» являются методы поиска следов вредоносной активности в системах на базе Linux и ее анализ.

В главе 10 «Создание дампа памяти в MacOS» рассматриваются инструменты создания дампа памяти macOS, так что в итоге вы будете знать о техниках снятия дампов памяти со всех популярных операционных систем.

Глава 11 «Обнаружение и анализ вредоносной активности в macOS» посвящена исследованию действий пользователя, а также поиску и анализу следов вредоносной активности в памяти macOS.

Как извлечь максимум пользы из этой книги

Мы старались описывать все подробно и проводить читателя шаг за шагом по всему процессу. Поэтому вам понадобится только компьютер или виртуальная машина с установленными Windows и Linux.

Поскольку книга представляет собой практическое пособие, рекомендуется экспериментировать со всеми описанными в ней методами и инструментами – так вы сможете получить максимум пользы от прочтения.

Скачайте цветные изображения

Мы также предлагаем PDF-файл, содержащий цветные изображения всех снимков экрана и рисунков. Его можно скачать по адресу *https://static.packt-cdn.com/downloads/9781801070331_ColorImages.pdf*.

Условные обозначения

В этой книге применяется ряд условных обозначений.

`CodeInText`: код в тексте, имена таблиц баз данных, папок и файлов, расширения имен файлов, пути к файлам, URL, данные, вводимые пользователем. Например: «Для поиска таких процессов можно воспользоваться плагином `psscan`».

Входные данные и результаты команд выглядят так:

```
C:\WINDOWS\system32> wmic process list full
```

Полужирный: новые термины и важные определения, а также части пользовательского интерфейса, команды меню и текст в диалоговых окнах, например «**Living off the land** – популярный подход, заключающийся в том, что злоумышленник пользуется легитимными встроенными инструментами и пользовательскими программами для собственных целей».

> **Советы и важные замечания**
>
> Оформляются так.

Оставайтесь на связи

Мы всегда рады отзывам читателей.

Отзывы общего характера. Если у вас имеются какие-нибудь вопросы по этой книге, отправьте сообщение на адрес `customercare@packtpub.com`, указав в теме ее название.

Ошибки и опечатки. Мы тщательно проверяли содержимое книги, но какие-то ошибки все же могли проскользнуть. Если вы найдете в нашей книге ошибку, пожалуйста, сообщите нам о ней. Зайдите на страницу `www.packt.com/submit-errata`, выберите книгу, кликните по ссылке Errata Submission Form и введите описание ошибки.

Нарушение авторских прав. Если вы обнаружите незаконные копии наших изданий в любой форме в интернете, пожалуйста, сообщите нам адрес или название веб-сайта. Просим отправить ссылку на вызывающий подозрение в пиратстве материал по адресу `copyright@packt.com`.

Если вы хотите стать автором. Если вы являетесь специалистом по какой-то теме и хотели бы стать автором или соавтором книги, заходите на страницу `authors.packtpub.com`.

Поделитесь своими мыслями

После того как вы прочтете эту книгу, нам бы очень хотелось узнать, что вы думаете! Пожалуйста, перейдите по ссылке *https://packt.link/r/1-801-07033-4* и оставьте отзыв на странице этой книги на сайте Amazon.

Ваш отзыв важен для нас и всего технического сообщества, так мы сможем убедиться, что поставляем действительно высококачественные материалы.

Часть I

Основы криминалистики памяти

Из этой части вы не только узнаете о преимуществах криминалистики памяти, но и познакомитесь с основными понятиями, процессом создания дампов памяти и их анализа.

Часть I включает две главы:

- *главу 1 «Зачем нужна криминалистика памяти?»;*
- *главу 2 «Создание дампов памяти».*

Глава 1

Зачем нужна криминалистика памяти?

Мы живем в мире, где нет ничего более постоянного, чем переменное, и киберпреступления не являются исключением. Постоянно появляются новые методы атак, пишутся сотни вредоносных программ и тестируются на предмет обхода средств защиты. Сканеры неустанно ищут в сети уязвимые хосты и общедоступные сервисы. Вот почему так важно быть в курсе событий и иметь в своем арсенале всевозможные инструменты, чтобы противостоять злоумышленникам.

Так по какой же причине исследование памяти стало неотъемлемой частью многих *криминалистических экспертиз* и *реагирований на инциденты*? Каковы основные цели исследователя и какие методы применяют профессионалы? С какими проблемами они сталкиваются ежедневно? Ответы на поставленные вопросы вы найдете в этой главе.

В этой главе рассматриваются следующие темы:

- основные преимущества криминалистики памяти;
- цели и методы исследования;
- сложности исследования памяти.

Основные преимущества криминалистики памяти

Понятно, что читателю, выбравшему эту книгу, преимущества очевидны. Раз уж вы решили углубить свои знания в вопросах криминалистики памяти, то, вероятно, тому есть причины. Но давайте еще разок взглянем на наиболее типичные ситуации, когда исследование оперативной памяти может сыграть решающую роль (не только в компьютерной криминалистике и реагировании на инциденты, но и в анализе вредоносного ПО), – быть может, вы откроете для себя новые способы применения приобретенных знаний и навыков.

Без следов

В последние годы резко возросло количество атакующих, применяющих технику *Living off the land* и *бесфайловое* вредоносное ПО. Злоумышленникам больше не нужно удалять свои следы, вместо этого они стремятся их минимизировать и избежать обнаружения. Это значительно усложняет работу специалистов по информационной безопасности, поскольку использование злоумышленниками встроенных инструментов и отсутствие на диске вредоносных файлов, которые можно было бы просканировать, означает, что традиционные решения могут оказаться бесполезными. Отсутствие надлежащего логирования может сильно затруднить реконструкцию способов использования злоумышленниками инструментов двойного назначения, например различных интерпретаторов команд и скриптов, особенно в процессе постанализа. В таких случаях создание и анализ дампа памяти могут сыграть ключевую роль.

Обсудим каждый случай по отдельности.

Найди меня в памяти

Начнем с **вредоносных** программ, работающих исключительно в памяти. Сама идея не нова. Говоря о начале эпохи резидентных вредоносных программ, некоторые исследователи вспоминают *Maltese Amoeba*, вирус, впервые обнаруженный в 1991 году в Ирландии. Другие считают более правильным вести отсчет с червя *Code Red*, появившегося в 2001 году. Как бы то ни было, с начала XXI века бесфайловые атаки становятся все более популярными. Например, полезная нагрузка может быть внедрена в память посредством PowerShell, и этот способ получает очень широкое распространение. Многие вендоры в сфере кибербезопасности включили технику «Внедрение кода в процессы» (Process Injection) в десятку самых используемых техник матрицы *MITRE ATT&CK®* в 2020 году. Вот, например, 10 наиболее популярных техник, упомянутых в отчете *Red Canary 2021 Threat Detection Report*, доступном по адресу *https://redcanary.com/threat-detectionreport/techniques/*:

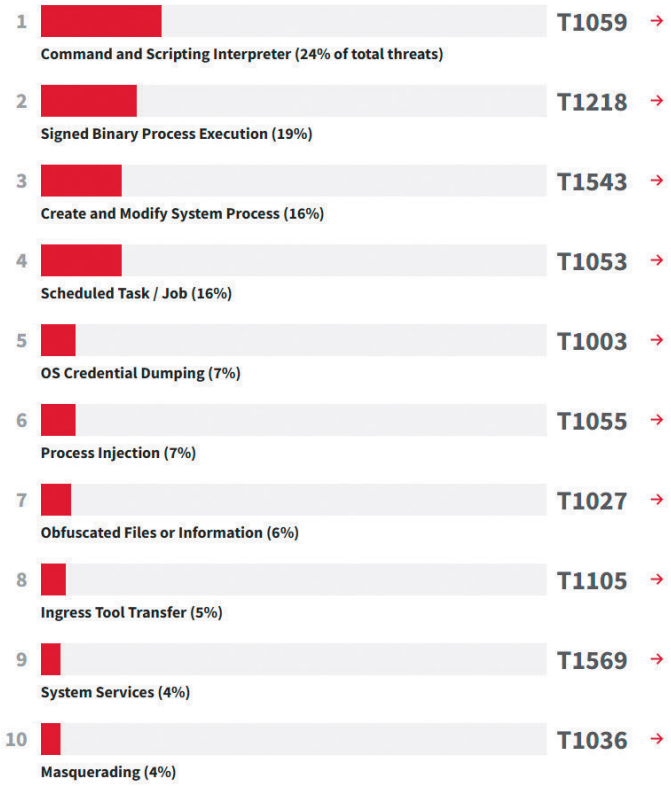

Рис. 1.1. Топ-10 техник матрицы MITRE ATT&CK 2020 года

Внедрение в пустой процесс (Process hollowing), внедрение DLL-библиотек (DLL injection), Doppelgänging и другие подтехники, связанные с внедрением кода в процессы, используются не только продвинутыми хакерскими группировками, финансируемыми государством, но даже операторами так называемого commodity malware.

Фреймворки

Другая сторона проблемы – использование многочисленных **постэксплуатационных фреймворков**, таких как Metasploit, Cobalt Strike или PowerShell Empire. Эти инструменты предлагают злоумышленнику широкий спектр средств генерирования разнообразных вредоносных полезных нагрузок и внедрения их в память.

Созданные специально для проведения атак, эти фреймворки позволяли сначала пентестерам и редтимерам, а затем и реальным злоумышленникам, в том числе не обладающим выдающимися навыками разработки вредоносного ПО, использовать самые разнообразные техники, практически не оставляя следов на диске. Например, полезная нагрузка Beacon, входящая в состав Cobalt Strike, имеет особые функции, позволяющие злоумышленникам выполнять команды и скрипты PowerShell через Windows API, не запуская при этом сам исполняемый файл powershell.exe.

Фреймворки наподобие Cobalt Strike стали настолько распространенными, что некоторые злоумышленники стали использовать их чаще, чем вредоносное ПО собственной разработки. Например, печально известная группа Evil Corp, которая, как полагают, стоит за громкими атаками с использованием шифровальщиков, включая атаку на Garmin, променяла бот Dridex на Beacon из Cobalt Strike в своих кампаниях *WastedLocker*.

Living off the land

Living off the land – очень популярный подход, при котором злоумышленники используют встроенные инструменты и уже установленные легитимные программы в своих целях. Большинство инструментов, например PowerShell или WMI, нужны системным администраторам для решения повседневных задач, поэтому трудно не только обнаружить злоумышленников, но и заблокировать используемый ими инструментарий.

Такой подход злоумышленники могут применять в рамках различных тактик. PowerShell можно использовать, чтобы скачать начальную полезную нагрузку с контролируемого злоумышленником сервера; такие программы, как `rundll32.exe` и `regsvr32.exe`, – для выполнения (Execution) и предотвращения обнаружения (Defense Evasion); **Ntdsutil** – для получения учетных данных (Credential Access), а **PsExec** и **WMIC** – для удаленного выполнения. Подобных примеров много, и если в ИТ-инфраструктуре нет продвинутых средств логирования, то шансы аналитика на извлечение подобной информации призрачны. Однако если вовремя создать дамп памяти, то его анализ может очень сильно помочь!

Важно также отметить, что во многих случаях на диске вы сможете найти только первую часть вредоносного файла, а следующие (их может быть несколько!) будут загружены с управляющего сервера непосредственно в память, так что при анализе образа диска, не имея дампа памяти, вы их даже не увидите.

Хуже того, в наши дни большинство вредоносных двоичных файлов упакованы, закодированы и зашифрованы, чтобы избежать обнаружения – но только не в памяти! Так что мы можем использовать такие инструменты, как PE-sieve, чтобы извлечь потенциально вредоносный код для последующего анализа. Конечно, в следующих главах мы покажем, как это делается.

На страже конфиденциальности

В последние годы тема конфиденциальности, или защиты частной жизни, приобрела дополнительную остроту. Тонны персональных данных, фотографий и сообщений каждый день поступают в сеть. Поставщики различных сервисов собирают информацию о нас, наших интересах и привычках, чтобы сделать свою работу более эффективной и полезной. В результате появились мессенджеры и браузеры с режимами конфиденциальности, файловые системы в памяти, менеджеры паролей и криптоконтейнеры.

Разумеется, конфиденциальность волнует всех, но киберпреступников особенно, потому что им есть что скрывать. Мы не раз видели, что представляющие интерес файлы на компьютере подозреваемого зашифрованы или хранятся в криптоконтейнере. В таких ситуациях выгрузка и анализ дампа памяти – ключ к любой двери, поскольку позволяют исследователю извлечь пароли и ключи, необходимые для дешифрирования.