В этом домашнем задании вы будете исследовать дамп оперативной памяти, снятый с компьютера жертвы — incident.mem. Для анализа можете использовать инструменты из папки Tools.  
В качестве Cheat Sheet используйте материалы из лекции.

**Порядок выполнения:**  
Загрузите [по ссылке](https://gibspace.group-ib.com/index.php/s/EPpRtDnnnECNqaR) все необходимые файлы из личного кабинета и распакуйте их. Используя доступные вам инструменты, найдите ответы на следующие вопросы.  
Пароль: GXspwwtCd9dTeM9

1. Когда был снят дамп? Запишите ответ в формате dd:mm:yy hh:mm:ss (UTC).

10:03:2019 13:06:28 UTC+0000

1. Назовите версию операционной системы, с которой был снят дамп. Например, Windows 10.

Windows 7

1. Напишите количество активных процессов.  
   46
2. Назовите родительский идентификатор процесса powershell.exe (PID).  
   3008
3. Имя процесса, «слушающего» порт 3389?

svchost.exe

1. Когда был запущен netscan.exe? Запишите ответ в формате dd:mm:yy hh:mm:ss (UTC).

10:03:2019 06:35:58 UTC+0000

1. Напишите имя процесса, командная строка которого содержит «Updater.bat».

conhost.exe

1. Назовите идентификатор процесса, который встречается в выводе плагина «malfind» 5 раз (PID).

3672

1. Назовите имя процесса, в который загружена библиотека «MSVCR80.dll».

Powershell.exe

1. Как осуществляется запуск файла «Updater» после перезагрузки? Укажите значение. (value) ключа реестра

C:\Users\Wilfred\AppData\Roaming\Identities\Updater.bat

В этом домашнем задании вам нужно проанализировать несколько файлов. Всё необходимое для выполнения заданий есть в облаке.  
В качестве Cheat Sheet используйте материалы из лекции.

**Порядок выполнения**  
Загрузите [по ссылке](https://gibspace.group-ib.com/index.php/s/mL2SAdYBNoWJR6j) все необходимые файлы из личного кабинета. Используя доступные вам инструменты, выполните задания и найдите ответы на вопросы.  
Пароль: MqTG3KyGPt2pNds

1. Изучите функцию main. Какое число будет выведено на экран в результате работы программы, содержащей в себе подобный код на языке ассемблера? Для вывода на экран используется функция printf. (Для этого проанализируйте файл asm\_1.txt)

0

1. Проанализируйте файл asm\_1.txt. Каким будет вывод программы, если следующие инструкции будут изменены? <https://drive.google.com/file/d/1SttaUFJBI7bs_d7mfUwrRoB7F_qc1GvA/view?usp=sharing>

0

1. Какие четыре WinAPI функции вызываются в программе? Перечислите названия функций через пробел в порядке их вызова в программе. (Проанализируйте файл asm\_2.txt)

GetComputerNameA CreateFileA WriteFile CloseHandle

1. Какое имя будет у текстового файла, создаваемого в программе? (Проанализируйте файл asm\_2.txt и ответьте на вопрос)
2. Что из списка не будет записано в создаваемый файл? (Проанализируйте файл asm\_2.txt и ответьте на вопрос)

* Имя пользователя
* Имя ключа реестра

1. Запишите полный путь исполняемого файла, который создается процессом WScript. Учитывайте, что файл будет исполняемым, его расширение будет не .exe. Проанализируйте отчет песочницы AnyRun (https://app.any.run/tasks/cd03ef11-f197-4aaa-9d7d-32dd20a7f7c4/). Данный отчет мы разбирали в рамках лекции, где выяснили, что это файл, который запускает полезную нагрузку с помощью WScript и regsvr32, а также внедряет код в контекст процесса iexplore.exe и может быть классифицирован как Ursnif.

C:\Users\admin\AppData\Local\Temp\PTgnTpO.txt

1. Запишите размер этого файла в килобайтах. Проанализируйте отчет песочницы AnyRun (<https://app.any.run/tasks/cd03ef11-f197-4aaa-9d7d-32dd20a7f7c4/>). Данный отчет мы разбирали в рамках лекции, где выяснили, что это файл, который запускает полезную нагрузку с помощью WScript и regsvr32, а также внедряет код в контекст процесса iexplore.exe и может быть классифицирован как Ursnif.

334

1. Запишите MD5-хеш этого файла. Проанализируйте отчет песочницы AnyRun (<https://app.any.run/tasks/cd03ef11-f197-4aaa-9d7d-32dd20a7f7c4/>). Данный отчет мы разбирали в рамках лекции, где выяснили, что это файл, который запускает полезную нагрузку с помощью WScript и regsvr32, а также внедряет код в контекст процесса iexplore.exe и может быть классифицирован как Ursnif.

c10960e5f2ee8fa3fbca898000cc0938

1. С каким доменом производились коммуникации у вредоносного кода, внедрённого в процесс iexplore.exe? Проанализируйте отчет песочницы AnyRun (<https://app.any.run/tasks/cd03ef11-f197-4aaa-9d7d-32dd20a7f7c4/>). Данный отчет мы разбирали в рамках лекции, где выяснили, что это файл, который запускает полезную нагрузку с помощью WScript и regsvr32, а также внедряет код в контекст процесса iexplore.exe и может быть классифицирован как Ursnif.

f1.pipen.at

1. Укажите полный путь до исполняемого файла, закреплённого в ключе реестра «HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Test Update». Проанализируйте файл autoruns\_1.arn с помощью утилиты Autoruns (Autoruns\Autoruns.exe -> File -> Open).

c:\users\Администратор\appdata\local\temp\for\_sc.exe

1. Запишите имя службы, осуществляющей запуск файла «c:\users\Администратор\appdata\local\temp\for\_sc.exe». Проанализируйте файл autoruns\_1.arn с помощью утилиты Autoruns (Autoruns\Autoruns.exe -> File -> Open).
2. Что из списка реализует этот Powershell скрипт? Проанализируйте файл posh\_1.txt, который содержит в себе командную строку для подозрительного процесса Powershell. Необходимо декодировать Base64-закодированную строку.

* Скачивает файл с удалённого хоста
* Запускает скачанный файл
* Создаёт для скачанного файла службу
* Обходит политику исполнения Powershell
* Удаляет важные пользовательские файлы

1. С каким сетевым адресом происходит взаимодействие? Запишите URL-адрес.Проанализируйте файл posh\_1.txt, который содержит в себе командную строку для подозрительного процесса Powershell. Необходимо декодировать Base64-закодированную строку.
2. Какое имя будет у запускаемого файла? Проанализируйте файл posh\_1.txt, который содержит в себе командную строку для подозрительного процесса Powershell. Необходимо декодировать Base64-закодированную строку.

Выберите правильный, на Ваш взгляд, ответ для каждого вопроса:

1. Какая техника была использована атакующими для первичного проникновения? Напишите название техники на английском языке. В этом домашнем задании вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность — DNS запрос к ресурсу fmjstorage.com. Вам нужно:

* Проанализировать триаж-копию, снятую с компьютера, осуществившего эту сетевую активность.
* Найти следы атакующих.
* Проанализировать их действия.
* Предложить план действий по ликвидации и восстановлению.

Для анализа можете использовать инструменты из папки Tools. В качестве Cheat Sheet’а используйте материалы лекции. Загрузите все необходимые файлы по ссылке (<https://gibspace.group-ib.com/index.php/s/sxHWfz4NSbq5jLG>). Пароль: oJz7mi6qRxzEBQ4

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию. Постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

1. Как назывался файл, используемый атакующими для первичного проникновения? (Напишите полное название файла, включая расширение). В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке (<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>). Пароль: oJz7mi6qRxzEBQ4

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

1. Когда была запущена программа, которая использовалась для открытия этого файла? (dd:mm:yy hh:mm:ss UTC). В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке (<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>). Пароль: oJz7mi6qRxzEBQ4.

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

1. Какая программа запустилась после завершения MS Word? В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке(<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>). Пароль: oJz7mi6qRxzEBQ4

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

1. Какой ресурс использовался для загрузки полезной нагрузки? (URL). В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке(<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>). Пароль: oJz7mi6qRxzEBQ4.

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

1. Укажите полный путь до исполняемого файла, созданного после обращения к вредоносному ресурсу. В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке (<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>). Пароль: oJz7mi6qRxzEBQ4

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

1. Какие из файлов не были созданы вредоносным ПО? В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке (<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>). Пароль: oJz7mi6qRxzEBQ4

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

* episode1log.vbs
* LogScene2.cmd
* DW20.exe
* 00000000000000073701.dat
* SceneWar.exe

1. Какие действия по ликвидации и восстановлению обязательно следует предпринять? В рамках данного ДЗ вы попробуете провести реагирование на инцидент. 18 июня в 14:34 UTC+3 средствами защиты была задетектирована подозрительная сетевая активность – DNS запрос к ресурсу fmjstorage.com. Вам необходимо проанализировать триаж-копию, снятую с компьютера, осуществившего данную сетевую активность, найти следы атакующих, проанализировать их действия и предложить план действий по ликвидации и восстановлению. Для анализа вы можете использовать инструменты, расположенные в папке Tools. В качестве Cheat Sheet’а вы можете использовать материалы лекции. Загрузите все необходимые файлы по ссылке (<https://gibspace.group-ib.com/s/sxHWfz4NSbq5jLG/authenticate/showShare>) Пароль: oJz7mi6qRxzEBQ4

Распакуйте их. Используя доступные вам инструменты, проанализируйте полученную триаж-копию, постарайтесь понять, какие действия были осуществлены атакующими и, основываясь на ваших находках, составьте план по ликвидации и восстановлению.

* Остановка вредоносных процессов
* Отключение и удаление функций или служб
* Удаление файлов
* Смена пароля пользователя
* Удаление задач планировщика
* Удаление учётных записей
* Изменение ключей реестра