МАТРИЦА

ТАКТИКИ

ТЕХНИКИ

MITRE ATT&CK

Разведка

Активное сканирование
- Сканирование блоков IP-адресов
- Поиск уязвимостей

Сбор информации об атакуемых пользователях
- Учетные данные
- Адреса электронной почты
- Имена сотрудников

Сбор информации об атакуемых узлах
- Конфигурация клиентов
- Прошивка
- Антивирусное обеспечение
- Программное обеспечение

Сбор информации об атакуемой организации
- DNS
- Свойства доменов
- IP-адреса
- Средства сетевой защиты
- Топология сети
- Доверенные сети

Сбор бизнес-информации об атакуемой организации
- Контрагенты
- Определение физического местоположения
- Изучение графика работы и режима поставок
- Определение ролей сотрудников

Фишинг с целью сбора сведений
- Целевой фишинг с вложением
- Целевой фишинг со ссылкой
- Целевой фишинг через сторонние сервисы

Поиск в закрытых источниках
- Покупка технических данных
- Поставщики информации об угрозах

Поиск технической информации в общедоступных источниках
- Сети доставки содержимого
- Цифровые сертификаты
- DNS-записи
- SEL с результатами сканирований
- WHOIS

Поиск на общедоступных сайтах
- Поисковые системы
- Социальные сети

Поиск на сайтах атакуемой организации

Подготовка ресурсов

Приобретение инфраструктуры
- Ботнет
- DNS-сервер
- Домены
- Сервер
- Виртуальный выделенный сервер
- Веб-сервисы

Компрометация учетных записей
- Учетные записи электронной почты
- Учетные записи соцсетей

Компрометация сторонней инфраструктуры
- Ботнет
- DNS-сервер
- Домены
- Сервер
- Виртуальный выделенный сервер
- Веб-сервисы

Разработка собственных средств
- Сертификаты подписи кода
- Цифровые сертификаты
- Эксплойты
- Вредоносное ПО

Создание учетных записей
- Учетные записи электронной почты
- Учетные записи соцсетей

Подготовка необходимых средств
- Сертификаты подписи кода
- Цифровые сертификаты
- Эксплойты
- Вредоносное ПО
- Инструменты
- Уязвимости

Размещение средств
- Подготовка теневой (drive-by) среды
- Установка цифрового сертификата
- Целевая ссылка
- Загрузка вредоносного ПО
- Загрузка инструментов

Закрепление

Манипуляции с учетной записью
- Добавление роли глобального администратора Office 365
- Дополнительные облачные учетные данные
- Выдача доп. прав учетной записи электронной почты Exchange
- Изменение авторизованных SSH-ключей

Задания BITS

Автозапуск при загрузке или входе в систему
- Активная установка
- Пакет аутентификации
- Модули и расширения ядра
- Объекты входа
- Драйвер LSASS
- Изменение списка свойств (plist)
- Мониторы портов
- Обработчики печати
- Перезапуск приложений
- Ключи запуска в реестре / Папка автозагрузки
- Поставщик поддержки безопасности (SSP)
- Изменение ярлыков
- Поставщики времени
- DLL-библиотеки, загружаемые с помощью Winlogon
- Записи автозагрузки XDG

Сценарии инициализации при загрузке или входе в систему
- Сценарий входа в систему (Mac)
- Сценарий входа в систему (Windows)
- Сценарий входа в сеть
- Сценарии RC
- Элементы автозагрузки

Расширения браузеров

Компрометация бинарных файлов клиентского ПО

Создание учетной записи
- Облачная учетная запись
- Доменная учетная запись
- Локальная учетная запись

Создание или изменение системных процессов
- Агент запуска
- Демон запуска
- Служба systemd
- Служба Windows

Выполнение по событию
- Специальные возможности
- Модификация ключа AppCertDLLs
- Модификация ключа AppInit_DLLs
- Подсистема обратной совместимости приложений
- Подмена файловых ассоциаций по умолчанию
- Перехват COM-объектов
- Демон мониторинга событий emond
- Внедрение в IFEO
- Добавление LC_LOAD_DYLIB
- DLL-библиотеки, загружаемые с помощью Netsh
- Профиль PowerShell
- Экранная заставка
- Команда trap
- Изменение конфигурации командной оболочки Unix
- Подписка на события WMI

Внешние службы удаленного доступа

Перехват потока исполнения
- Переменная окружения COR_PROFILER
- Перехват поиска DLL-библиотек
- Загрузка сторонних DLL-библиотек
- Перехват поиска dylib-библиотек
- Перехват динамического компоновщика
- Недостатки разрешений для исполняемых файлов установщика
- Изменение переменной окружения PATH
- Перехват поиска программ
- Перехват поиска через не заключенный в кавычки путь
- Недостатки разрешений для файлов служб
- Недостатки разрешений для записей реестра, относящихся к службам

Внедрение кода в образ

Изменение процесса аутентификации
- Аутентификация на контроллере домена
- Аутентификация на сетевых устройствах
- DLL-библиотеки фильтров паролей
- Подключаемые модули аутентификации

Запуск приложения Office
- Надстройки
- Макрос в шаблоне
- Office Test
- Формы Outlook
- Домашняя страница Outlook
- Правила Outlook

Загрузка раньше ОС
- Буткит
- Прошивка компонентов
- BOOT/LOGIN
- Прошивка системы
- Загрузка по TFTP

Запланированная задача (задание)
- Утилита at (Linux)
- Утилита at (Windows)
- Задания оркестрации контейнеров
- Утилита cron
- Планировщик заданий Windows
- Таймеры systemd

Компонент серверного ПО
- Компоненты ВД
- Хранимые процедуры SQL
- Агенты транспорта Microsoft Exchange
- Веб-оболо

Передача управляющих сигналов в трафике
- Прослушивание портов

Существующие учетные записи
- Облачные учетные записи
- Учетные записи по умолчанию
- Доменные учетные записи
- Локальные учетные записи

Предотвращение обнаружения

Обход механизмов контроля привилегий
- Обход контроля учетных записей
- Запрос пароля суперпользователя для повышения привилегий
- Setuid и Setgid
- Sudo и кэширование sudo

Манипуляции с токенами доступа
- Создание процесса с помощью токена
- Создание токена и имперсонация
- Подмена родительского PID
- Внедрение в sIDHistory
- Кража токена и имперсонация

Задания BITS

Создание образа на узле

Деобфускация/декодирование файлов или информации

Развертывание контейнера

Прямой доступ к тому

Изменение доменной политики
- Изменение доверительных отношений между доменами
- Изменение групповой политики

Ограничения на исполнение
- Использование ключей на основе окружения

Эксплуатация уязвимостей для предотвращения обнаружения

Изменение разрешений для файлов и каталогов
- Изменение разрешений для файлов и каталогов (Linux и Mac)
- Изменение разрешений для файлов и каталогов (Windows)

Скрытие артефактов
- Правила скрытия электронной почты
- Скрытие файловых систем
- Скрытые файлы и каталоги
- Скрытые пользователи
- Скрытое окно
- Атрибуты файла NTFS
- Создание ветви ресурсов
- Запуск виртуальной машины
- Скрытие в скомпилированном VBA-коде

Перехват потока исполнения
- Переменная окружения COR_PROFILER
- Перехват поиска DLL-библиотек
- Загрузка сторонних DLL-библиотек
- Перехват поиска dylib-библиотек
- Перехват динамического компоновщика
- Недостатки разрешений для исполняемых файлов установщика
- Изменение переменной окружения PATH
- Перехват поиска программ
- Перехват поиска через не заключенный в кавычки путь
- Недостатки разрешений для файлов служб
- Недостатки разрешений для записей реестра, относящихся к службам

Ослабление защиты
- Отключение облачного журналирования
- Отключение или перенастройка облачного межсетевого экрана
- Отключение или перенастройка системного межсетевого экрана
- Отключение или перенастройка средств защиты
- Отключение журналирования событий Windows
- Атака на понижение
- Повреждение журнала истории команд
- Блокировка сбора признаков активности
- Загрузка в безопасном режиме

Удаление признаков активности из системы
- Очистка истории команд
- Очистка системных журналов Linux или Mac
- Очистка журналов событий Windows
- Удаление файла
- Удаление подключений к общим сетевым ресурсам
- Изменение временных меток

Непрямое выполнение команд

Маскировка
- Двойное расширение у файла
- Недействительная подпись кода
- Имитация задачи или службы
- Подбор легитимного имени или расположения
- Переименование системных утилит
- Использование символа RLO
- Пробел после имени файла

Изменение процесса аутентификации
- Аутентификация на контроллере домена
- Аутентификация на сетевых устройствах
- DLL-библиотеки фильтров паролей
- Подключаемые модули аутентификации

Изменение облачной вычислительной инфраструктуры
- Создание облачного экземпляра
- Создание снапшота
- Удаление облачного экземпляра
- Отмена изменений облачного экземпляра

Изменение реестра

Изменение образа ОС
- Понижение версии образа ОС
- Внесение исправлений в образ ОС

Преодоление границ сети
- Изменение конфигурации NAT

Обфусцированные файлы или данные
- Добавление в бинарный файл незначащих данных
- Компиляция после доставки
- Внедрение данных в HTML
- Удаление индикаторов компрометации из вредоносных инструментов
- Упаковка ПО
- Стеганография

Загрузка раньше ОС
- Буткит
- Прошивка компонентов
- BOOT/LOGIN
- Прошивка системы
- Загрузка по TFTP

Внедрение кода в процессы
- Асинхронный вызов процедур
- Внедрение DLL-библиотек
- Внедрение в дополнительную память окна (EWM)
- Внедрение PE-образа
- Внедрение через файловую систему /proc
- Doppelgänging
- Внедрение в пустой процесс
- Системные вызовы ptrace
- Перехват выполнения потока
- Локальная память потока
- Перехват виртуального динамического общего объекта (VDSO)

Отраженная загрузка кода

Подсадный контроллер домена

Руткит

Выполнение через подписанные бинарные файлы
- Установщик профилей диспетчера подключений (CMSTP)
- CMSBaikn
- Панель управления
- Утилита InstallUtil
- Mavinject
- Консоль управления (MMC)
- Утилита msiexec
- Утилита odbcconf
- Утилиты Regsvcs и Regasm
- Утилита Regsvr32
- Rundll32
- Verclsid

Выполнение через подписанный сценарий
- Сценарий PubPrn

Нарушение работы средств контроля доверия
- Подпись исполняемого кода
- Изменение политики подписи кода
- Обход Gatekeeper
- Установка корневого сертификата
- Обход ограничений веб-меток безопасности (MOTW)
- Подмена поставщика доверия и SIP

Внедрение в шаблоны

Передача управляющих сигналов в трафике
- Прослушивание портов

Выполнение через доверенные утилиты разработчика
- MSBuild

Облачные инфраструктуры в редко используемых регионах

Использование альтернативных данных для аутентификации
- Токен доступа к приложению
- Управление жизненным циклом учетных данных
- Управляемый билет Kerberos
- Сессионные куки

Существующие учетные записи
- Облачные учетные записи
- Учетные записи по умолчанию
- Доменные учетные записи
- Локальные учетные записи

Обход виртуализации или песочницы
- Системные проверки
- Обход на основе времени
- Проверки активности пользователя

Понижение надежности шифрования
- Отключение аппаратного шифрования
- Сокращение ключевого пространства

Использование сценариев XSL

Перемещение внутри периметра

Эксплуатация удаленных служб

Внутренний целевой фишинг

Передача инструментов внутри периметра

Перехват сессии службы удаленного доступа
- Перехват сессии удаленного рабочего стола
- Перехват сессии SSH

Службы удаленного доступа
- Распространение COM-модель
- Протокол удаленного рабочего стола
- Общие SMB-ресурсы или ресурсы администраторов Windows
- SSH
- VNC
- Служба удаленного управления Windows

Распространение через съемные носители

Средства развертывания ПО

Заражение общего содержимого

Использование альтернативных данных для аутентификации
- Токен доступа к приложению
- Управление жизненным циклом учетных данных
- Управляемый билет Kerberos
- Сессионные куки

Сбор данных

«Злоумышленник посередине»
- Отравление ARP-кэша
- Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB

Архивация собранных данных
- Архивация с помощью специального метода
- Архивация с помощью библиотеки
- Архивация с помощью утилиты

Захват аудиоданных

Автоматизированный сбор данных

Перехват сессии браузера

Данные из буфера обмена

Данные из облачных хранилищ

Данные из репозиториев конфигураций
- Демон конфигурации сетевого устройства
- SNMP (демп MIB)

Данные из информационных репозиториев
- Репозиторий кода
- Confluence
- SharePoint

Данные из локальной системы

Данные с общих сетевых дисков

Данные со съемных носителей

Промежуточное хранение данных
- Промежуточное хранение данных (локально)
- Промежуточное хранение данных (удаленно)

Сбор электронной почты
- Правила пересылки электронной почты
- Сбор электронной почты (локально)
- Сбор электронной почты (удаленно)

Перехват вводимых данных
- Получение учетных данных через API
- Перехват данных с помощью подмены пользовательского интерфейса
- Регистрация нажатий клавиш
- Перехват данных на внешних веб-портал

Захват экрана

Захват видеоданных

Организация управления

Протокол прикладного уровня
- DNS
- Протоколы передачи файлов
- Протоколы электронной почты
- Веб-протоколы

Взаимодействие через съемные носители

Кодирование данных
- Нестандартное кодирование
- Стандартное кодирование

Обфускация данных
- «Мусорные» данные
- Имитация протокола
- Стеганография

Динамическое разрешение
- Расчет на основе DNS
- Алгоритмы генерирования доменных имен
- Быстрая смена IP-адресов для DNS-записи

Зашифрованный канал
- Асимметричное шифрование
- Симметричное шифрование

Резервные каналы

Передача инструментов из внешней сети

Отдельный канал для каждого этапа

Протоколы (кроме прикладного уровня)

Нестандартный порт

Туннелирование протокола

Прокси-сервер
- Домен-прокрытие
- Внешний прокси-сервер
- Внутренний прокси-сервер
- Цепочка прокси-серверов

ПО для удаленного доступа

Передача управляющих сигналов в трафике
- Прослушивание портов

Веб-служба
- Двусторонняя связь
- «Закладка» с данными
- Односторонняя связь

Эксфильтрация данных

Автоматизированная эксфильтрация
- Дублирование трафика

Ограничение размера передаваемых данных

Эксфильтрация по альтернативному протоколу
- Эксфильтрация по альтернативному протоколу с асимметричным шифрованием
- Эксфильтрация по альтернативному протоколу с симметричным шифрованием
- Эксфильтрация по альтернативному протоколу без шифрования (с возможной обфускацией)

Эксфильтрация через канал управления

Эксфильтрация через альтернативную сетевую среду
- Эксфильтрация через Bluetooth

Эксфильтрация через альтернативную физическую среду
- Эксфильтрация через USB

Эксфильтрация через веб-службу
- Эксфильтрация в облачное хранилище
- Эксфильтрация в репозиторий кода

Передача по расписанию

Перемещение данных между облачными учетными записями

Деструктивное воздействие

Прекращение доступа к учетной записи

Уничтожение данных

Шифрование данных

Манипуляции с данными
- Манипуляции с обрабатываемыми данными
- Манипуляции с хранимыми данными
- Манипуляции с передаваемыми данными

Дефейс
- Дефейс внешних систем
- Дефейс внутренних систем

Уничтожение диска
- Удаление содержимого диска
- Нарушение структуры диска

Точечный отказ в обслуживании
- Исчерпание ресурсов приложения
- Эксплуатация уязвимостей ПО
- Исчерпание ресурсов ОС
- Исчерпание ресурсов служб

Повреждение прошивки

Препятствование восстановлению системы

Сетевой отказ в обслуживании
- Прямое увеличение сетевого трафика
- Отраженное увеличение сетевого трафика

Несанкционированное использование ресурсов

Остановка службы

Завершение работы или перезагрузка системы

Выполнение

Интерпретаторы командной строки и сценариев
- AppleScript
- JavaScript
- Интерпретаторы командной строки сетевых устройств
- PowerShell
- Python
- Командная оболочка Unix
- Visual Basic
- Командная оболочка Windows

Команда администрирования контейнера

Развертывание контейнера

Уязвимости в клиентском ПО

Межпроцессное взаимодействие
- COM-модель
- Динамический обмен данными (DDE)

Нативный API

Запланированная задача (задание)
- Утилита at (Linux)
- Утилита at (Windows)
- Задания оркестрации контейнеров
- Утилита cron
- Планировщик заданий Windows
- Таймеры systemd

Общие модули

Средства развертывания ПО

Системные службы
- Утилита launchctl
- Диспетчер управления службами (SCM)

Выполнение с участием пользователя
- Вредоносный файл
- Вредоносный образ
- Вредоносная ссылка

Инструментарий управления Windows

Повышение привилегий

Обход механизмов контроля привилегий
- Обход контроля учетных записей
- Запрос пароля суперпользователя для повышения привилегий
- Setuid и Setgid
- Sudo и кэширование sudo

Манипуляции с токенами доступа
- Создание процесса с помощью токена
- Создание токена и имперсонация
- Подмена родительского PID
- Внедрение в sIDHistory
- Кража токена и имперсонация

Автозапуск при загрузке или входе в систему
- Активная установка
- Пакет аутентификации
- Модули и расширения ядра
- Объекты входа
- Драйвер LSASS
- Изменение списка свойств (plist)
- Мониторы портов
- Обработчики печати
- Перезапуск приложений
- Ключи запуска в реестре / Папка автозагрузки
- Поставщик поддержки безопасности (SSP)
- Изменение ярлыков
- Поставщики времени
- DLL-библиотеки, загружаемые с помощью Winlogon
- Записи автозагрузки XDG

Сценарии инициализации при загрузке или входе в систему
- Сценарий входа в систему (Mac)
- Сценарий входа в систему (Windows)
- Сценарий входа в сеть
- Сценарии RC
- Элементы автозагрузки

Создание или изменение системных процессов
- Агент запуска
- Демон запуска
- Служба systemd
- Служба Windows

Изменение доменной политики
- Изменение доверительных отношений между доменами
- Изменение групповой политики

Выход за пределы контейнера

Выполнение по событию
- Специальные возможности
- Модификация ключа AppCertDLLs
- Модификация ключа AppInit_DLLs
- Подсистема обратной совместимости приложений
- Подмена файловых ассоциаций по умолчанию
- Перехват COM-объектов
- Демон мониторинга событий emond
- Внедрение в IFEO
- Добавление LC_LOAD_DYLIB
- DLL-библиотеки, загружаемые с помощью Netsh
- Профиль PowerShell
- Экранная заставка
- Команда trap
- Изменение конфигурации командной оболочки Unix
- Подписка на события WMI

Эксплуатация уязвимостей для повышения привилегий

Перехват потока исполнения
- Переменная окружения COR_PROFILER
- Перехват поиска DLL-библиотек
- Загрузка сторонних DLL-библиотек
- Перехват поиска dylib-библиотек
- Перехват динамического компоновщика
- Недостатки разрешений для исполняемых файлов установщика
- Изменение переменной окружения PATH
- Перехват поиска программ
- Перехват поиска через не заключенный в кавычки путь
- Недостатки разрешений для файлов служб
- Недостатки разрешений для записей реестра, относящихся к службам

Внедрение кода в процессы
- Асинхронный вызов процедур
- Внедрение DLL-библиотек
- Внедрение в дополнительную память окна (EWM)
- Внедрение PE-образа
- Внедрение через файловую систему /proc
- Doppelgänging
- Внедрение в пустой процесс
- Системные вызовы ptrace
- Перехват выполнения потока
- Локальная память потока
- Перехват виртуального динамического общего объекта (VDSO)

Запланированная задача (задание)
- Утилита at (Linux)
- Утилита at (Windows)
- Задания оркестрации контейнеров
- Утилита cron
- Планировщик заданий Windows
- Таймеры systemd

Существующие учетные записи
- Облачные учетные записи
- Учетные записи по умолчанию
- Доменные учетные записи
- Локальные учетные записи

Получение учетных данных

«Злоумышленник посередине»
- Отравление ARP-кэша
- Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB

Метод перебора
- Подстановка украденных учетных данных
- Взлом паролей
- Угадывание паролей
- Распыление паролей

Учетные данные из хранилищ паролей
- Учетные данные из браузеров
- Связка ключей
- Менеджеры паролей
- Память securityd
- Диспетчер учетных данных Windows

Эксплуатация уязвимостей для получения учетных данных

Принудительная аутентификация

Подделка учетных данных для веб-ресурсов
- Токены SAML
- Веб-куки

Перехват вводимых данных
- Получение учетных данных через API
- Перехват данных с помощью подмены пользовательского интерфейса
- Регистрация нажатий клавиш
- Перехват данных на внешних веб-портал

Изменение процесса аутентификации
- Аутентификация на контроллере домена
- Аутентификация на сетевых устройствах
- DLL-библиотеки фильтров паролей
- Подключаемые модули аутентификации

Прослушивание сетевого трафика

Получение дампа учетных данных
- Содержимое файлов /etc/passwd и /etc/shadow
- Кэшированные доменные учетные данные
- DCSync
- Секреты LSA
- Память процесса LSASS
- Файл ntds.dit
- Файловая система proc
- Диспетчер учетных записей безопасности

Кража токена доступа к приложению

Кража или подделка билетов Kerberos
- «Golden Ticket» AS-REP
- Золотой билет Kerberos
- «Серебряный» билет Kerberos

Кража сессионных куки

Перехват двухфакторной аутентификации

Незащищенные учетные данные
- История команд bash
- API метаданных облачных экземпляров
- API-контейнера
- Учетные данные в файлах
- Учетные данные в реестре
- Параметры групповой политики
- Закрытые ключи

Изучение

Изучение учетных записей
- Облачная учетная запись
- Доменная учетная запись
- Учетные записи электронной почты
- Локальная учетная запись

Изучение открытых приложений

Изучение закладок в браузерах

Изучение облачной инфраструктуры

Панель управления облачной службы

Изучение облачных служб

Изучение объектов облачного хранилища

Изучение контейнеров и их ресурсов

Изучение доверительных отношений между доменами

Изучение файлов и каталогов

Изучение групповой политики

Сканирование сетевых служб

Изучение общих сетевых ресурсов

Прослушивание сетевого трафика

Изучение парольной политики

Изучение периферийных устройств

Изучение групп разрешений
- Облачные группы
- Доменные группы
- Локальные группы

Изучение процессов

Запросы к реестру

Изучение удаленных систем

Изучение установленного ПО
- Изучение средств защиты

Изучение системы

Изучение местоположения системы
- Изучение системного языка

Изучение конфигурации сети
- Изучение интернет-соединений

Изучение сетевых подключений

Изучение владельца или пользователей системы

Изучение системных служб

Изучение системного времени

Обход виртуализации или песочницы
- Системные проверки
- Обход на основе времени
- Проверки активности пользователя

Матрица MITRE ATT&CK описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру.

ptsecurity.com