Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 1

habr.com/ru/articles/423405

Андрей Макеев

Ссылки на все части:

Часть 1. Получение первоначального доступа (Initial Access)
Часть 2. Выполнение (Execution)
Часть 3. Закрепление (Persistence)
Часть 4. Повышение привилегий (Privilege Escalation)
Часть 5. Обход защиты (Defense Evasion)
Часть 6. Получение учетных данных (Credential Access)
Часть 7. Обнаружение (Discovery)
Часть 8. Боковое перемещение (Lateral Movement)
Часть 9. Сбор данных (Collection)
Часть 10 Эксфильтрация или утечка данных (Exfiltration)
Часть 11. Командование и управление (Command and Control)

Получение первоначального доступа

Данной публикацией начинаю цикл постов, посвященных описанию основных техник, применяемых злоумышленниками на различных этапах осуществления хакерских атак.
Излагаемый материал будет свободным пересказом содержания матриц *Adversarial Tactics, Techniques & Common Knowledge (ATT@CK)* от компании *The Mitre*:

Автор не несет ответственности за возможные последствия применения изложенной информации, а также просит прощения за возможные неточности, допущенные в некоторых формулировках и терминах. Кстати, это моя первая попытка публикации на Хабре, поэтому надеюсь на справедливую критику в свой адрес.

Погружение в тему начнётся с самой объемной матрицы ATT&CK Matrix for Enterprise, которая описывает активные и наиболее опасные фазы атаки на корпоративную сеть:
— Получение первоначального доступа (Initial Access);
— Выполнение кода (Execution);
— Закрепление в атакуемой системе (Persistence);
— Повышение привилегий (Privilege Escalation);
— Обход защиты (Defense Evasion);
— Получение учетных данных (Credential Access);

— Обзор (Discovery);
— Горизонтальное продвижение (Lateral Movement);
— Сбор данных (Collection);
— Утечка (Exfiltration);
— Управление и контроль (Command and Control).

Цель злоумышленника на этапе получения первоначального доступа – доставить в атакуемую систему некий зловредный код и обеспечить возможность его дальнейшего выполнения.

Теневая загрузка (Drive-by Compromise), Drive-by download

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Суть техники состоит в открытии жертвой в браузере WEB-ресурса, на котором злоумышленником заранее подготовлены различные эксплойты браузеров и плагинов,
скрытые фреймы или вредоносные файлы Java, которые без ведома пользователя будут загружены в атакуемую систему.

Рекомендации по защите: Использование последних версий браузеров и плагинов и
применение антивирусного программного обеспечения. Microsoft предлагает использовать *Windows Defender Explloit Guard (WDEG)* и *Enhanced Mitigation Experience Toolkit (EMET)*. Имеет смысл так же рассмотреть целесообразность блокировки выполнения в браузере JavaScript.

Эксплоиты публичных приложений (Exploit Public-Facing Application)

Система: Windows, Linux, macOS
Описание: Техника предполагает использование известных багов, глюков и уязвимостей в программном обеспечении, имеющем открытые сетевые порты (web-серверы, сетевые службы SSH, SMB2, СУБД и т.п.). *ТОП 10 уязвимостей web-приложений* публикуется OWASP.

Рекомендации по защите: Использование брандмауэров, сегментирование сети с помощью DMZ, использование рекомендаций по безопасной разработке ПО, избежание проблем, задокументированных OWASP и CWE. Сканирование внешнего периметра на наличие уязвимостей. Мониторинг журналов приложений и траффика на предмет аномального поведения.

Аппаратные закладки (Hardware Additions)

Система: Windows, Linux, macOS

Описание: В дополнительные компьютерные аксессуары, сетевое оборудование и компьютеры могут быть встроены аппаратные дополнения для предоставления злоумышленникам начального доступа. В коммерческие и opensource-продукты могут быть встроены возможности скрытого сетевого подключения, реализации атак типа «человек по середине» для взлома систем шифрования, осуществления клавиатурных инъекций (keystroke injection), чтения памяти ядра через DMA, добавления новой беспроводной сети и т.п.

Рекомендации по защите: Применение политик контроля доступа к сети, таких как использование сертификатов для устройств и стандарта 802.1.x, ограничение использования DHCP только зарегистрированными устройствами, запрет сетевого взаимодействия с незарегистрированными устройствами, блокировка установки внешних устройств с помощью средств защиты хоста (Endpoint Security агенты для ограничения подключения устройств).

Распространение с помощью съемных медиа-устройств (Replication Through Removable Media)

Система: Windows
Описание: Техника предполагает исполнение вредоносной программы с помощью функции автозапуска в Windows. Чтобы обмануть пользователя «законный» файл может быть предварительно модифицирован или заменён, а затем скопирован на съемное устройство злоумышленником. Так же полезная нагрузка может быть внедрена прошивку съемного устройства или через программу первоначального форматирования носителя.

Рекомендации по защите: Отключение функций автозапуска в Windows. Ограничение использования съемных устройств на уровне политики безопасности организации. Применение антивирусного программного обеспечения.

Целевые фишинговые вложения (Spearphishing Attachment)

Описание: Использование вредоносных программ, прикрепленных к фишинговым электронным письмам. Текст письма, как правило, содержит правдоподобную причину почему получатель должен открыть файл во вложении.

Рекомендации по защите: Использование систем предотвращения сетевых вторжений (IDS) и антивирусов, предназначенных для сканирования и удаления вредоносных вложений в электронных письмах. Настройка политики блокирования неиспользуемых форматов вложений. Обучение пользователей правилам антифишинга.

Целевые фишинговые ссылки (Spearphishing Link)

Описание: Использование ссылок на загрузку вредоносных программ в электронных письмах.

Рекомендации по защите: Проверка URL-адресов в электронной почте может помочь обнаружить ссылки на известные вредоносные сайты. Использование систем предотвращения сетевых вторжений (IDS) и антивирусов. Обучение пользователей правилам антифишинга.

Целевые фишинговые сервисы (Spearphishing via Service)

Описание: В этом сценарии злоумышленники отправляют сообщения через различные службы социальных сетей, личную почту и другие службы, не контролируемые предприятием.
Злоумышленники могут использовать поддельные профили в соц. сетях, например, для отправки потенциальных предложений о трудоустройстве. Это позволяет задавать сотруднику-жертве вопросы о политиках и программном обеспечении в компании, заставлять жертву открывать вредоносные ссылки и вложения. Как правило, злоумышленник устанавливает первоначальный контакт, а затем отправляет вредоносное содержимое на почту, которую сотрудник атакуемой компании использует на рабочем месте. Если у жертвы не получается запустить вредоносный файл, то ему могут дать инструкцию по дальнейшим действиям.

Рекомендации по защите: Блокирование доступа к социальным сетям, сервисам личной электронной почты и т.п. Использование белых списков приложений, систем предотвращения сетевых вторжений (IDS) и антивирусов. Обучение пользователей правилам антифишинга.

Компрометация цепи поставок (Supply Chain Compromise)

Описание: Сценарий предполагает внедрение в программное обеспечение и компьютерное оборудование всевозможных эксплойтов, бэкдоров и других хакерских инструментов на этапе поставок в атакуемую компанию программного обеспечения и компьютерного оборудования. Возможные векторы атак:
— Манипуляции с инструментами и средами разработки ПО;
— Работа с репозиториями исходного кода;
— Манипуляции с механизмами обновления и распространения ПО;
— Компрометация и заражение образов ОС;
— Модификация легального ПО;
— Продажа модифицированной/контрафактной продукции законным дистрибьютером;
— Перехват на этапе отгрузки.
Как правило, злоумышленники сосредотачиваются на внедрении вредоносных компонентов в каналах распространения и обновления программного обеспечения.

Рекомендации по защите: Применение системы управления рисками в цепях поставок (SCRM) и системы управления жизненным циклом разработки ПО (SDLC). Использование процедур контроля целостности двоичных файлов ПО, антивирусное сканирование дистрибутивов, тестирование ПО и обновлений перед развертыванием, физический осмотр закупаемого оборудования, носителей с дистрибутивами ПО и сопроводительной документации с целью обнаружения фальсификаций.

Доверительные отношения (Trusted Relationship)

Описание: Злоумышленники могут использовать организации, которые имеют доступ к инфраструктуре предполагаемой жертвы. Зачастую, для связи с доверенной третьей стороной компании используют менее защищенное сетевое соединение, чем стандартный доступ в компанию из вне. Примеры доверенных третьих сторон: подрядчики ИТ-услуг, поставщики услуг безопасности, инфраструктурные подрядчики. Так же учетные записи, используемые доверенной стороной для доступа в сеть компании, могут быть скомпрометированы и использоваться для первоначального доступа.

Рекомендации по защите: Сегментация сети и изоляция критичных компонентов инфраструктуры, не требующих широкого доступа из вне. Управление учетными записями и разрешениями, используемыми сторонами доверительных отношений. Проверка политик безопасности и процедур организаций, работающих по контракту и требующих привилегированного доступа. Мониторинг деятельности, осуществляемой сторонними поставщиками и доверенными лицами.

Валидные учетные записи (Valid Accounts)

Описание: Злоумышленники могут украсть учетные данные определенного пользователя или учетную запись службы с помощью техник доступа к учетным данным, захватить учетные данные в процессе разведки с помощью социальной инженерии. Скомпрометированные учетные данные могут использоваться для обхода систем управления доступом и получения доступа к удаленным системам и внешним службам, таким как VPN, OWA, удаленный рабочий стол или получения повышенных привилегий в определенных системах и областях сети. В случае успешной реализации сценария злоумышленники могут отказаться от вредоносных программ, чтобы затруднить своё обнаружение. Так же злоумышленники могут создавать учетные записи используя заранее определенные имена и пароли для сохранения резервного доступа в случае неудачных попыток использования других средств.
Рекомендации по защите: Применение парольной политики, следование рекомендациям по проектированию и администрированию корпоративной сети для ограничения использования привилегированных учетных записей на всех административных уровнях. Регулярные проверки доменных, локальных учетных

записей и их прав с целью выявления тех, которые могут позволить злоумышленнику получить широкий доступ. Мониторинг активности учетных записей с помощью SIEM-систем.

В следующей части рассмотрены тактики, применяемые на стадии Выполнение кода (Execution).