ссылка на гугл док

MITRE ATT&CK

Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge — «тактики, техники и общеизвестные факты о злоумышленниках») — основанная на реальных наблюдениях база знаний компании Mitre, содержащая описание тактик, приемов и методов, используемых киберпреступниками.

Информация в базе знаний Mitre Att&ck представлена в виде *матриц*. Каждая матрица представляет собой таблицу, в которой заголовки столбцов соответствуют *тактикам* киберпреступников, то есть основным этапам кибератаки или подготовки к ней, а содержимое ячеек — методикам реализации этих тактик, или *техникам*. Так, если *сбор данных* согласно Mitre Att&ck — это тактика атаки, то способы сбора, например *автоматический сбор* или *сбор данных со съемных носителей*, — это техники.

Матрицы Mitre Att&ck объединены в три группы:

- Enterprise — тактики и техники, которые злоумышленники применяют в ходе атаки на предприятия. В этой группе доступна как сводная матрица, так и отдельные матрицы, содержащие тактики и техники кибератак на конкретные операционные системы и облачные сервисы.
- Mobile — тактики и техники, которые злоумышленники используют в ходе атаки на мобильные устройства под управлением iOS и Android.
- ATT&CK for ICS — тактики и техники, которые используются в атаках на промышленные системы управления.

Применение Mitre Att&ck

Специалисты по информационной безопасности используют матрицы Mitre Att&ck для решения следующих задач:

- Анализ существующей защиты на предмет соответствия реальным угрозам и повышение безопасности инфраструктуры компании. С помощью матриц Mitre Att&ck можно определить, к каким техникам

уязвимы ресурсы организации, чтобы в перспективе устранить самые критичные проблемы.
- Своевременное реагирование на инциденты. С помощью матриц Mitre Att&ck можно установить, на каком этапе развития находится атака и какие меры необходимо принять в первую очередь.
- Расследование киберинцидентов. Матрицы Mitre Att&ck позволяют оперативно определить, на каком этапе обнаружена атака и где стоит в первую очередь искать следы вторжения.
- Атрибуция атак. По перечню техник, использованных злоумышленниками, можно определить вероятного исполнителя.
- Анализ деятельности киберпреступников. Матрицы Mitre Att&ck позволяют отслеживать эволюцию тактик и техник, которые применяют известные APT-группировки.
- Обмен информацией с коллегами. Единая структурированная система описания кибератаки позволяет специалистам из разных областей находить общий язык.

Таблица на русском: ссылка

Таблица на англ: ссылка

Тактики:

Reconnaissance (Разведка)

The adversary is trying to gather information they can use to plan future operations.

Techniques

- Active scanning

.001 Scanning IP Blocks
.002: Поиск уязвимостей
.003: Сканирование по списку слов

- Сбор информации об атакуемых узлах

Аппаратное, программное обеспечение, прошивка, конфигурация клиентов

- Сбор информации об атакуемых пользователях

Учетные данные, адреса эл. почты, имена сотрудников

- Сбор информации об атакуемой сетевой инфраструктуре

Способы обнаружения

- Сетевой трафик: Содержимое сетевого трафика
- Сетевой трафик: Поток сетевого трафика

- Скан интернета: Содержимое ответа

Меры противодействия

- Предкомпрометация
- Отключение или удаление компонента или программы

Resource Development(Подготовка ресурсов)

Противник пытается создать ресурсы, которые он мог бы использовать для поддержки операций.

Techniques

- T1650: Приобретение доступа
- T1583: Приобретение инфраструктуры(домены, DNS-сервер, виртуально выделенный сервер, сервер, ботнет, веб-сервисы, бессерверная инфаструктура, вредоносная реклама)
- T1584: Компрометация сторонней инфраструктуры

Способы обнаружения

- Доменное имя: Пассивные данные DNS
- Доменное имя: Регистрация домена

- Скан интернета: Метаданные ответа
- Доменное имя: Активные данные DNS
- Скан интернета: Содержимое ответа (VPS-servers)

Меры противодействия

- Предкомпрометация

- T1586: Компрометация учетных записей(учетные записи в социальных сетях, учетные записи эл. почты, облачные уч. записи)

Способы обнаружения

- Фиктивная личность: Социальные сети
- Сетевой трафик: Содержимое сетевого трафика

Меры противодействия

- Предкомпрометация

- T1587: Разработка собственных средств
- T1585: Создание учетных записей
- T1588: Подготовка необходимых средств
- T1608: Размещение средств

Первоначальный доступ(Initial Access)

Злоумышленник пытается проникнуть в вашу сеть.

Techniques

- T1659: Внедрение контента

Способы обнаружения

- Сетевой трафик: Содержимое сетевого трафика
- Процесс: Создание процесса
- Файл: Создание файла

Меры противодействия

- Предкомпрометация

- T1189: Теневая (drive-by) компрометация

Способы обнаружения

- Сетевой трафик: Содержимое сетевого трафика
- Сетевой трафик: Создание сетевого подключения
- Журналы приложений: Содержимое журналов приложений
- Процесс: Создание процесса
- Файл: Создание файла

Меры противодействия

- Предкомпрометация
- Защита от эксплойтов
- Обновление ПО
- Изоляция и помещение в песочницу приложений
- Ограничения для веб-контента

- T1190: Недостатки в общедоступном приложении

Способы обнаружения

- Сетевой трафик: Содержимое сетевого трафика
- Журналы приложений: Содержимое журналов приложений

Меры противодействия

- Сегментация сети
- Управление привилегированными учетными записями
- Защита от эксплойтов
- Обновление ПО
- Изоляция и помещение в песочницу приложений
- Поиск уязвимостей

- T1133: Внешние службы удаленного доступа
- T1200: Подключение дополнительных устройств
- Фишинг

Выполнение (Execution)

Злоумышленник пытается запустить вредоносный код.

Techniques

- T1651: Средства администрирования облака

Способы обнаружения

- Сценарий: Выполнение сценария
- Процесс: Создание процесса
- Команда: Выполнение команд

Меры противодействия

- Предкомпрометация

- T1059: Интерпретаторы командной строки и сценариев

Способы обнаружения

- Сценарий: Выполнение сценария
- Процесс: Создание процесса
- Команда: Выполнение команд
- Процесс: Метаданные процесса
- Модуль: Загрузка модуля

Меры противодействия

- Предкомпрометация
- Подпись исполняемого кода
- Отключение или удаление компонента или программы
- Защита от выполнения
- Антивирус или ПО для защиты от вредоносных программ

- T1609: Средства администрирования контейнера

Способы обнаружения

- Процесс: Создание процесса
- Команда: Выполнение команд

- T1610: Развертывание контейнера

Закрепление (Persistence)

Злоумышленник пытается сохранить свои позиции.

Techniques

- T1098: Манипуляции с учетной записью
- T1197: Задания BITS
- T1547: Автозапуск при загрузке или входе в систему
- T1037: Сценарии инициализации при загрузке или входе в систему

Повышение привелегий (Privilege Escalation)

The adversary is trying to gain higher-level permissions.

Techniques

- T1548: Обход механизмов контроля привилегий
- T1548.001: Setuid и Setgid
- T1548.002: Обход контроля учетных записей
- T1548.003: Команда sudo и кэширование sudo
- T1548.006: Манипуляции с TCC
- T1134: Манипуляции с токенами доступа
- T1098: Манипуляции с учетной записью
- T1547: Автозапуск при загрузке или входе в систему

Предотвращение обнаружений (Defense Evasion)

The adversary is trying to avoid being detected.

Techniques

- T1548: Обход механизмов контроля привилегий
- T1548.001: Setuid и Setgid
- T1548.002: Обход контроля учетных записей
- T1548.003: Команда sudo и кэширование sudo
- T1548.006: Манипуляции с TCC
- T1134: Манипуляции с токенами доступа
- T1197: Задания BITS

- T1622: Предотвращение отладки

Получение учетных данных (Credential Access)

The adversary is trying to steal account names and passwords.

Techniques

- T1557: "Злоумышленник посередине"
- T1110: Метод перебора
- T1555: Учетные данные из хранилищ паролей
- T1212: Эксплуатация уязвимостей для получения учетных данных

Обнаружение (Discovery)

The adversary is trying to figure out your environment.

Techniques

- T1087: Изучение учетных записей
- T1010: Изучение открытых приложений
- T1217: Изучение браузера

Перемещение внутри периметра (Lateral Movement)

The adversary is trying to move through your environment.

Techniques

- T1210: Эксплуатация уязвимостей в удаленных службах
- T1534: Внутренний целевой фишинг
- T1570: Передача инструментов внутри периметра
- T1563: Перехват сессии службы удаленного доступа
- T1563.001: Перехват сессии SSH

Сбор данных (Collection)

The adversary is trying to gather data of interest to their goal.

Techniques

- T1557: "Злоумышленник посередине"
- T1560: Архивация собранных данных
- T1123: Захват аудиоданных
- T1119: Автоматизированный сбор данных

Организация управления (Command and Control)

The adversary is trying to communicate with compromised systems to control them.

Techniques

- T1071: Протокол прикладного уровня
- T1092: Взаимодействие через съемные носители
- T1659: Внедрение контента
- T1132: Кодирование данных
- T1001: Обфускация данных

Эксфильтрация данных (Exfiltration)

The adversary is trying to steal data.

Techniques

- T1020: Автоматизированная эксфильтрация
- T1030: Ограничение размера передаваемых блоков данных
- T1048: Эксфильтрация по альтернативному протоколу
- T1041: Эксфильтрация по каналу управления
- T1011: Эксфильтрация через альтернативную сетевую среду

Деструктивное воздействие (Impact)

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Techniques

- T1531: Прекращение доступа к учетной записи
- T1485: Уничтожение данных
- T1486: Шифрование данных

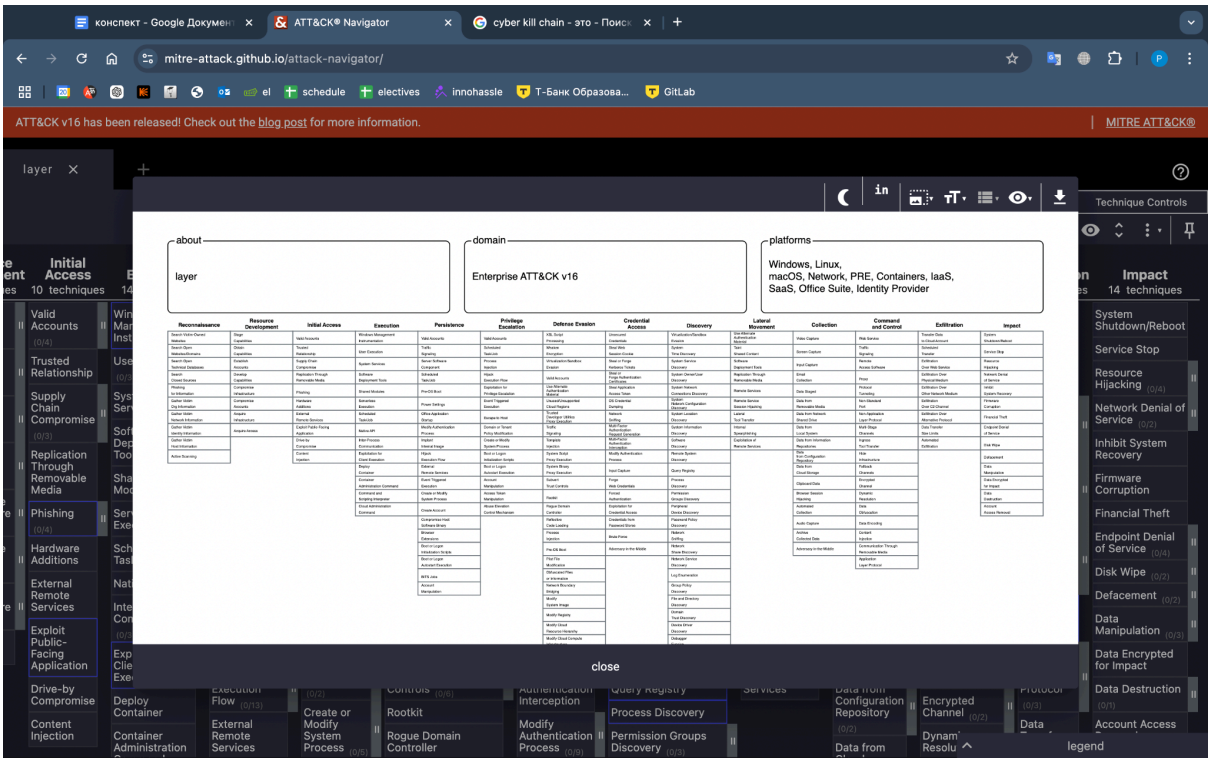
> **Ландшафт угроз** — это результат всестороннего анализа киберугроз, опирающийся на разведывательные данные, связанные с

потенциальными злоумышленниками и их характеристиками. Этот анализ показывает наиболее релевантные угрозы для определенной отрасли, страны или конкретной организации.

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

link of project creation



Что такое цепочка Kill Chain

Kill Chain — это процесс с помощью, которого совершаются кибератаки. Модель «убийственной цепочки» описывает действия злоумышленников, включая самые ранние этапы атаки — шпионаж и планирование — до конечной цели.

Этапы цепочки Kill Chain

Цепочка Kill Chain состоит из семи звеньев. После прохождения всех этапов, злоумышленники начинают путь по цепи сначала, только уже в корпоративной сети. Нужно учитывать, что количество шагов при атаке может уменьшиться или увеличиться, например, когда дополнительным последним шагом становится удаление следов деятельности.

Основные этапы в традиционной цепи киберубиств:

1. Внешняя разведка (Reconnaissance). Злоумышленник выбирает цель и собирает информацию о ней: изучает специфику отрасли и данные о деятельности организации, выбирает методы и технологии для атаки.
2. Вооружение (Weaponization). На этом этапе выбирают, приобретают или создают самостоятельно средства для атаки. Оружием может стать не только вредоносное ПО, но и веб-приложения или различные уязвимости в файлах. Также злоумышленники могут создавать почтовые ящики, аккаунты в социальных сетях и фишинговые сайты.
3. Доставка полезной нагрузки (Delivery). Вредоносный контент попадает на устройство жертвы, например, когда она скачивает файл, заходит на поддельный сайт или использует зараженную флешку.
4. Заражение (Exploitation). Вредоносное ПО разворачивается на устройстве.
5. Установка (Installation). Программа внедряется в систему, маскируясь под другие процессы и открывает удаленный доступ. Может быть выполнена установка дополнительных утилит.
6. Получение управления (Command and Control). Злоумышленник получает доступ к устройству жертвы и отдает команды, какие именно действия должны быть совершены.
7. Выполнение целевого действия (Actions on Objectives). На последнем шаге выполняются вредоносные действия — кража информации, шифрование и подмена данных и т.д.

Diamond Model — это концептуальная структура, используемая в кибербезопасности для анализа и понимания киберугроз, вторжений или атак . Она использует четыре ключевых компонента: противник, жертва, инфраструктура и возможности.

База данных CVE

Common Vulnerabilities and Exposures (CVE) появилась в 1999 году по инициативе MITRE Corporation.

Каждая запись в CVE содержит:

- уникальный идентификатор (в формате CVE-ГГГГ-XXXX, где ГГГГ — это год обнаружения, а XXXX — порядковый номер)
- описание уязвимости
- ссылки на дополнительные источники
- информацию о затронутых версиях ПО
- дату обнаружения

Как работает система CVE

Процесс добавления новой уязвимости включает несколько этапов:

1. Обнаружение уязвимости исследователем: специалист находит брешь в безопасности и документирует ее
2. Подача заявки в CVE через CNA: исследователь обращается к одному из уполномоченных органов с описанием уязвимости
3. Проверка информации и присвоение идентификатора: CNA анализирует заявку, проверяет уникальность уязвимости и выдает CVE ID
4. Публикация в базе данных: после проверки информация становится общедоступной

CNA (CVE Numbering Authority) представляют собой организации, уполномоченные присваивать CVE-идентификаторы. В их число входят технологические гиганты вроде Microsoft, Apple и Google, а также научные институты и государственные организации. На 2024 год насчитывается более 200 CNA по всему миру.

Важно отметить роль координированного раскрытия информации: исследователи обычно дают производителям ПО время на исправление уязвимости перед публичным анонсом. Этот период может длиться от нескольких недель до нескольких месяцев.

Система оценки CVSS

link
Common Vulnerability Scoring System появилась в 2005 году как ответ на потребность в стандартизированной оценке серьезности уязвимостей. CVSS определяет степень опасности по шкале от 0 до 10, где 10 означает максимальную угрозу.

Система использует три группы метрик:

Базовые метрики:

- вектор атаки (сетевой, локальный, физический)
- сложность атаки (высокая, средняя, низкая)
- требуемые привилегии
- необходимость взаимодействия с пользователем
- масштаб воздействия

Временные метрики:

- зрелость эксплойта
- доступность исправлений
- уверенность в оценке

Контекстные метрики:

- требования к конфиденциальности
- требования к целостности
- требования к доступности
- потенциальный ущерб для организации

SIGMA-правила

Sigma – это формат описания правил для обнаружения аномалий, с помощью которых Kaspersky Endpoint Agent анализирует данные внутренних событий и журналов событий. Правила, написанные в формате Sigma, называются Sigma-правилами. Каждое Sigma-правило хранится в отдельном YAML-файле.

Sigma-правила пишутся на языке YAML и имеют унифицированную структуру. Это позволяет специально созданным конвертерам формировать правила в синтаксисе различных SIEM-систем на основе Sigma-правил.

> **SIEM (Security information and event management, «управление событиями и информацией о безопасности»)** — класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.

Коллекция Sigma-правил – набор Sigma-правил, определяющих схожие события.

Структура Sigma-правила

Атрибут / Секция	Обязательный	Описание
`title`	Да	Название правила, указывающее на то, что оно обнаруживает. Максимальная длина 256 символов. Например: `title: Создание новой службы RAT`
`id`	Нет	Глобальный уникальный идентификатор правила. Например: `id: 929a690e-bef0-4204-a928-ef5e620d6fcc`

`status`	Нет	Статус правила. Возможные значения: `stable`, `test`, `experimental`, `deprecated`, `unsupported`. Например: `status: test`
`description`	Нет	Описание правила и вредоносной активности, которую можно обнаружить с его помощью. Максимальная длина 65 535 символов. Например: `description: Обнаруживает установку новой службы хост-программы Remote Utilities.`
`license`	Нет	Идентификатор лицензии согласно спецификации SPDX ID. Правило публикуется на условиях указанного типа лицензии.
`author`	Нет	Любой признак, указывающий на автора правила. Например, имя-фамилия, прозвище, идентификатор в социальной сети.
`reference`	Нет	Ссылка на источник, из которого было получено правило. Например, статья в блоге, технический документ.
`date`	Нет	Дата создания правила в формате ГГГГ/ММ/ДД.
`modified`	Нет	Дата в формате ГГГГ/ММ/ДД, когда был изменен один из атрибутов правила: `title`, `status`, `logsource`, `detection`, `level`.
`tags`	Нет	Тег для категоризации правила. Подробнее читайте по ссылке.
`logsource`	Да	В секции можно определить источник событий, в которых программа ищет аномалии. Основные атрибуты секции: `category`, `product`, `service`. Источники событий, которые поддерживает Kaspersky Endpoint Agent Подробнее читайте по ссылке.

`category`	Нет	Определяет категорию продуктов, в журналах событий которых программа ищет аномалии. Например: брандмауэр, интернет, антивирус или обобщенная категория.
		`logsource:`
		`  category: firewall`

`product`	Нет	Определяет программный продукт или операционную систему, в журналах событий которых программа ищет аномалии. Например:
		`logsource:`
		`  product: Windows`

`service`	Нет	Определяет службу, в журналах событий которой программа ищет аномалии. Например:
		`logsource:`
		`  service: AppLocker`

`definition`	Нет	Описание особенностей источника журналов событий, в которых программа ищет аномалии.
`detection`	Да	Секция содержит один или несколько критериев для поиска аномалий в журналах событий и условие срабатывания правила. В качестве критериев поиска могут быть списки, словари и их комбинация.

`список`	Нет	Список из значений какого-либо параметра из журнала событий, объединенных логическим ИЛИ. Например:
		`detection:`
		`  selection:`
		`  OriginalFileName:`
		`  - 'AnyDesk.exe'`
		`  - 'TeamViewer.exe'`
		`  condition: selection`

		Согласно условию, будут искаться совпадения `OriginalFileName='AnyDesk.exe'` ИЛИ `OriginalFileName='TeamViewer.exe'`.

`словарь`	Нет	Пары типа *параметр журнала событий - значение*. Соединены логическим И. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID: 517`
		`  condition: selection`
		
		Согласно условию, будут искаться совпадения EventLog='Security' И Event ID=517.

`комбинация списка и словаря`	Нет	Список, состоящий из значений параметров журнала событий и словарей. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  EventID:`
		`  - 517`
		`  - 1102'`
		`  condition: selection`
		
		Согласно условию, будут искаться совпадения EventLog='Security' И (Event ID=517 ИЛИ Event ID=1102)

`condition`	Да	Условие срабатывания правила. Например:
		`detection:`
		`  selection:`
		`  EventLog: Security`
		`  condition: selection`

`fields`	Нет	Строки из журнала событий, которые могут быть интересны аналитику для дальнейшего анализа события.

`falsepositives`	Нет	Список известных сценариев, которые могут привести к ложному срабатыванию правила. Например:
		
		`falsepositives:`
		`- Использование утилиты системными администраторами`

`level`	Нет	Показатель критичности аномалий, которые могут быть найдены с помощью правила. Возможные значения: `informational`, `low`, `medium`, `high`, `critical`.

Индикатор компрометации (Indicator of Compromise, IoC)

Индикатор компрометации (Indicator of Compromise, IoC) — в сфере компьютерной безопасности наблюдаемый в сети или на конкретном устройстве объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (то есть ее компрометацию). Такие индикаторы используются для обнаружения вредоносной активности на ранней стадии, а также для предотвращения известных угроз.

Что может быть индикатором компрометации

В качестве индикатора компрометации могут выступать:

- Необычные DNS-запросы.
- Подозрительные файлы, приложения и процессы.
- IP-адреса и домены, принадлежащие ботнетам или командным серверам вредоносного ПО.

- Значительное количество обращений к одному файлу.
- Подозрительная активность в учетных записях администраторов или привилегированных пользователей.
- Неожиданное обновление программных продуктов.
- Передача данных через редко используемые порты.
- Нетипичное для человека поведение на веб-сайте.
- Сигнатура или хеш-сумма вредоносной программы.
- Необычный размер HTML-ответов.
- Несанкционированное изменение конфигурационных файлов, реестров или настроек устройства.
- Большое количество неудачных попыток входа в систему.

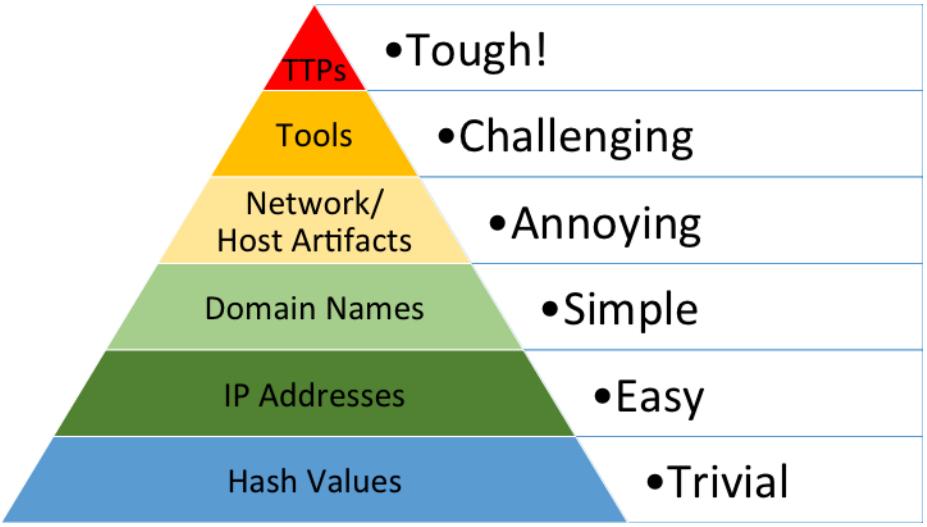
Выявление и применение индикаторов компрометации

Индикаторы компрометации, связанные с конкретной угрозой, выделяются при анализе этой угрозы. Например, если кибербразведка обнаружила новое вредоносное ПО, в отчете о нем будут приведены такие IoC, как хеши файлов, адреса командных серверов и так далее.

В дальнейшем индикаторы компрометации используются для активного поиска угроз в инфраструктуре организации. Обнаружение IoC в системе указывает на то, что, вероятно, на нее уже ведется кибератака и необходимо принять меры реагирования.

Индикаторы компрометации также добавляют в базы данных пассивных средств мониторинга и антивирусного ПО, чтобы своевременно выявлять и блокировать попытки проникновения. Например, с помощью сигнатур вредоносной программы защитное решение распознает ее и запрещает ей запускаться на устройстве.

Пирамида боли



Каждая ступень пирамиды характеризует различные типы индикаторов компрометации, которые могут быть использованы для поиска следов атакующего. Ширина ступени отражает количество индикаторов, а ее цвет и расположение по высоте — степень неудобств или «боли», которые могут быть причинены атакующему при детектировании или блокировании его индикаторов.

Например, блокировка IP-адресов или доменных имен C2 не доставит атакующему много неудобств, т. к. IP-адреса могут быть легко изменены, а новые домены — зарегистрированы. Вместе с тем блокировка специфичных утилит, используемых атакующим, способна причинить немало неудобств, т. к. для обхода такой защиты потребуется либо серьезно переработать уже имеющийся в его распоряжении инструмент, либо разработать или купить новый, что довольно затратно и неприятно. И наконец, TTPs (тактики, техники и процедуры), используемые атакующим, могут быть обнаружены посредством разработки детектирующих правил. Такой подход доставит атакующему максимально много «боли», т. к. это вынудит его либо изменить свои техники, несмотря на то что это может быть очень сложно, а зачастую даже невозможно, либо отступить.

Теперь, когда мы познакомились с пирамидой боли, рассмотрим, какие подходы к Threat Hunting существуют в настоящее время:

IoC-based — первые четыре ступени пирамиды. Поиск следов атакующего ведется по специфичным индикаторам, например по хеш-суммам известных хакерских инструментов, таких как Mimikatz или Empire, или по специфичным доменным именам командных центров атакующего. Менее волатильные индикаторы — специфичные ключи реестра, изменяемые malware или строки User-Agent.

Tools-based — предпоследняя ступень пирамиды боли, включающая детектирование по признакам, характерным для специфичных инструментов. Например, командные строки, которые мы можем получить из событий запуска процессов, или атрибуты VERSIONINFO исполняемых файлов, поставляемые EDR-решениями, в том числе уже ранее упомянутым Sysmon.

TTPs-based — верхняя ступень пирамиды боли с тактиками, техниками и процедурами. Допустим, что для lateral movement и закрепления в системе атакующий использует технику удаленного выполнения кода T1035 — Service Execution. Опытный охотник за угрозами исследует эту технику, определяет телеметрию, необходимую для разработки детектирующего правила, и при помощи инструментов выполняет проактивный поиск следов использования данной техники в защищаемой инфраструктуре.

Common Vulnerability Scoring System

Common Vulnerability Scoring System (**CVSS**) — открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью понять приоритет её исправления.

Оценки рассчитываются по специальным формулам на основе нескольких метрик и приблизительно оценивают простоту внедрения эксплойта и его влияние на компьютерную систему. Результатом расчета являются три числовые оценки (*Base Score*, *Temporal Score* и *Environmental Score*), каждая из которых может принимать значение от 0 до 10, где 10 выражает максимальную опасность.