МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1Спец
_____ Кваша А. С.
(подпись)

Отчет защищен с оценкой

_____

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____

« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.

на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области киберпреступлений и методологии их защиты

- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1.Ознакомиться с понятием таргетированных кибератак.

2.Теоретически ознакомиться с видами и методами противодействия таргетированных кибератак.

3.На основе полученных знаний написать отчет по практике о проделанной работе.

Advanced Persistent Threat (Постоянная серьезная угроза). Таргетированные или целевые кибератаки.

Введение

Особенность целенаправленных атак заключается в том, что злоумышленников интересует конкретная компания или государственная организация. Это отличает данную угрозу от массовых хакерских атак – когда одновременно атакуется большое число целей и наименее защищенные пользователи становятся жертвой. Целенаправленные атаки обычно хорошо спланированы и включают несколько этапов — от разведки и внедрения до уничтожения следов присутствия. Как правило, в результате целенаправленной атаки злоумышленники закрепляются в инфраструктуре жертвы и остаются незамеченными в течение месяцев или даже лет – на протяжении всего этого времени они имеют доступ ко всей корпоративной информации.

Сложности классификации

Таргетированные или целевые атаки – атаки, направленные в отношении конкретных коммерческих организаций или государственных ведомств. Как правило, такие атаки не носят массовый характер и готовятся достаточно длительный период. Злоумышленники изучают информационные системы атакуемого объекта, узнают, какое программное обеспечение используется в тех или иных целях. Объектами атаки являются весьма ограниченные какими-либо рамками или целями конкретные информационные системы и/или люди. Вредоносное ПО специально разрабатывается для атаки, чтобы штатные антивирусы и средства защиты, используемые объектом и достаточно хорошо изученные злоумышленниками, не смогли обнаружить угрозу. Чаще всего это уязвимости нулевого дня и особые алгоритмы связи с исполнителями/заказчиками атаки.

Сложности при квалификации целевых атак - один из факторов, который не позволяет рассчитать даже их приблизительное количество.

Фазы целевой атаки

Подготовка – Выявление цели, сбор информации, разработка стратегии, разработка инструментов.

Проникновение – Техника обхода стандартных средств защиты, использование уязвимостей, социальная инженерия, комбинированные методы, инвентаризация сети.

Распространение – Закрепление, распространение, обновление, поиск ключевой информация и методов достижения цели.

Финал – Хищение ключевой информации, изменение данных, манипуляции с бизнес процессами, сокрытие следов, точка возврата.

Цели атак

Офис правления компании.

Часто аппаратура ненадлежащим образом защищена от физического повреждения.

НИОКР.

Обычно это отдел, требующий самого высокого уровня защиты, но зачастую он защищен не лучше, чем другие отделы.

Центры обработки данных

Представляют собой надежную среду для размещения частного облака. Проблемой является обеспечение безопасного функционирования многочисленных серверов, а также приложений, работающих на этих серверах.

Сеть поставщиков.

Из-за расширяющегося применения сетевых решений при работе с поставщиками возникают риски, связанные с тем, что относительно небольшие компании-поставщики, как правило, хуже защищены.

Облачные вычисления.

В основе своей использование внешнего облака безопасно. Проблемы связаны с тем, что уровень защиты данных зависит от законодательства и что возможен доступ со стороны спецслужб.

Производство.

Множество старых специализированных систем все чаще объединяется в сети, и их работу трудно отслеживать и контролировать. Атаки злоумышленников в этом случае могут привести к производственным потерям или даже к краху компании.

Базы данных

Обеспечивают безопасное хранение важной информации. Главная слабость – то, что в качестве «инструментов» для проникновения в базы данных взломщики могут использовать администраторов.

Конечная продукция

Активируемая с помощью информационных технологий. Растущий уровень использования сетевых решений для обеспечения функционирования конечной продукции облегчает проведение кибератак. Дистанционно контролируя устройства пользователей с целью провоцирования поломок, хакеры имеют возможность незаконно получать через эти устройства конфиденциальную информацию. В связи с этим компании может грозить потеря репутации и получение исков от пользователей, ставших жертвами мошенничества

Офисные сети.

Растущий уровень сетевого взаимодействия, предусматривающего объединение почти всех систем, предоставляет хакеру богатые возможности, если он сумеет проникнуть в сеть

Продажи.

Утечка маркетинговых планов, информации о ценах и клиентах подрывает репутацию компании и лишает ее конкурентных преимуществ.

Мобильные устройства.

Покупая смартфоны, доступные на коммерческом рынке, пользователи часто вводят в их память конфиденциальные данные, которые, как правило, без труда могут быть похищены хакерами. Самые испытанные и надежные концепции обеспечения безопасности могут оказаться бесполезными, если сотрудники компании используют собственные мобильные устройства для решения рабочих задач.

Интернет-магазины.

Для незаконного доступа под видом реально существующих покупателей и совершения мошеннических действий хакеры используют реквизиты кредитных карт и личные данные клиентов.

Телефонные звонки.

Эксплуатируя готовность людей помогать друг другу, злоумышленники могут использовать телефонные звонки как способ легкого получения нужной информации.

Сущность целевых атак

Попытки взлома имеют типовые особенности: атака была целевой и учитывала особенности процессов отправки и обработки сообщений в определенной платежной системе; вредоносный код в ряде случаев стандартными средствами антивирусной защиты не выявлялся, несмотря на актуальные антивирусные базы; зафиксированы также факты проникновения хакеров в локальные сети банков, чтобы, в том числе, с помощью попыток внедрения вредоносного кода через электронные сообщения.

Представители банков констатируют: если раньше мошенники предпочитали грабить клиентов, то теперь переключились на более крупную добычу, а именно – на сами финансово-кредитные учреждения.

Это более сложная процедура, но с точки зрения выгоды хакерам удобнее взламывать банки, где деньги лежат в одном месте. Они готовятся месяцами и в отношении конкретных банков и финансовых организаций. Это реальная угроза, от которой очень сложно защитится даже продвинутым в

плане информационной безопасности банкам. Злоумышленники достаточно хорошо изучили банковское ПО, АБС, средства защиты и так далее.

Целевые атаки идут бок о бок с социальной инженерией. DDoS-атаки никуда не исчезли, однако работать с ними гораздо проще, чем с вирусами, которые злоумышленники пишут для целенаправленных действий. Стандартные антивирусы не обнаруживают зловредных объектов, которые написаны для объекта атаки. Системы, которые позволяют фиксировать такие целевые атаки на конкретную финансовую организацию и выявлять риски на лету – это другой класс безопасности.

Методика целевых атак

Публично доступная информация о средствах проведения таргетированных атак и расследовании инцидентов позволяют говорить о разнообразии методов. Например, могут использоваться полностью автоматизированные методы, так и телефонные звонки.

Существенной проблемой становится безопасность смежных информационных систем – компаний-поставщиков (особенно разработчиков ПО, осуществляющих поддержку своего продукта) и клиентов. Доверенные отношения с ними могут быть использованы для обхода граничных средств защиты. Это значительно расширяет и без того сложный периметр защиты.

Уйти от попыток таргетированных атак жертве вряд ли удастся. Например, злоумышленник хочет получить доступ к внутренним ресурсам интересующей его компании. Для этой цели злоумышленник может инициировать множество целевых атак, на протяжении нескольких месяцев или лет. Все элементы атаки могут быть предварительно проверены на «заметность» для распространенных методов обнаружения. В случае неэффективности такие элементы модифицируются. Аналогично обновлению антивирусных баз могут обновляться и средства вторжения, в том числе и те, что уже функционируют в захваченной системе.

Подготовка может занимать месяцы, а активная фаза – минуты. Существует вероятность, что рано или поздно атака удастся. В конце концов

проблема нулевого дня уязвимостей актуальна всегда. Если есть информация, которая стоит 100 млн, то найдется кто готов потратить 50 млн на то чтобы ее украсть. Поэтому единственное что можно сделать – это быть готовым к компрометации и иметь инструменты для быстрого обнаружения атаки, ее пресечения и минимизации ущерба.

Установление организаторов

Большинство из таргетированных атак обнаруживается постфактум. Самой большой проблемой остается атрибуция – установление организаторов и исполнителей таких атак.

Для определения источника атаки необходимо учитывать множество факторов. Прежде всего, это анализ кода – в нем могут содержаться слова, косвенно указывающие на языковую или национальную принадлежность авторов. Например, русские слова, написанные латиницей, или ошибки, которые обычно свойственны именно русским авторам и т.д. Однако киберпреступники могут намеренно оставлять такие ложные следы, запутывая тем самым следствие.

Столь динамичное развитие этой угрозы говорит о том, что целевые атаки перестали быть уделом избранных: злоумышленники оптимизируют свои техники и инструменты, и это удешевляет и упрощает организацию вредоносной кампании, что, в свою очередь, способствует появлению новых игроков.

Методы защиты и предотвращения атак

Основными средствами защиты от целевых атак сегодня являются средства детектирования всевозможных аномалий (кода, команд, поведения и т.д.). При этом:

- Детектирование аномалий в рамках отдельно взятого компьютера, либо корпоративной ИС в целом, осуществляется с целью обнаружения реализуемых, а также частично, либо полностью реализованных атак.
- Обеспечивается возможность нейтрализации известных атак на ранних стадиях их осуществления .

- В отношении неизвестных угроз атак, к которым относятся угрозы целевых атак, детектирование аномалий неизбежно связано с ошибками первого (при поверхностном анализе событий) и второго (при глубоком анализе) рода. Неоднозначность аномалии является следствием более глубокого анализа, что исключает автоматизацию процесса. Задача детектирования аномалий в данном случае сводится не к защите информации, а к проведению соответствующего дальнейшего исследования по зарегистрированному факту реализации атаки, с целью максимально оперативной однозначной идентификации атаки.
- После однозначной идентификации аномалии, как атаки, в отношении этой атаки детектором аномалий уже реализуется защита информации.

Практически все поставщики имеют в своей линейке продукт, который позиционируется как средство защиты от таргетированных атак. Эффективность защиты от таргетированных атак не может всецело определяться только применяемыми техническими средствами.

Если говорить о технических средствах, то их эффективность будет рассматриваться сквозь призму поставленных компанией целей и задач, что лучше оценивать в рамках проведения пилотных проектов в конкретной среде. Подобно любым решениям продукты по защите от таргетированных атак имеют как свои сильные стороны, так и слабые.

Возможность оперативно реагировать на таргетированные атаки имеют центры мониторинга информационной безопасности. Такие центры могут комплексно анализировать состояние атакуемой системы через системы защиты информации; с помощью экспертов, сконцентрированных на анализе информационной безопасности в наблюдаемой системе; при мониторинге фактов компрометации и утечки информации; совокупном анализе крупных информационных систем. Это позволяет увидеть схожие признаки аномалий в различных сегментах информационной системы.

Технологии защиты от таргетированных атак были и раньше, но сейчас они выходят на новый уровень. В первую очередь речь идет о различных

инструментах для выявления аномалий – как на локальных компьютерах, так и на уровне сетевой активности. Задачей таких систем является поиск всего необычного, что происходит, а не поиск вредоносного года. Это объясняется тем, что во многих случаях атакующие могут вообще не использовать вредоносные программы.

Deception-ловушки

Новые средства появились и продолжают появляться. Однако их эффективность напрямую зависит от качества их настройки. Основными технологическими направлениями средств защиты являются:

- Песочницы, которые имитируют рабочие станции организации. В песочницах файлы, получаемые из интернета, запускаются и анализируются. Если запускаемый файл влечет за собой деструктивное воздействие, то такой файл определяется как зараженный;
- Анализ аномальной сетевой активности, который осуществляется путем сравнения текущей сетевой активности с построенной эталонной моделью сетевого поведения.
- Поведенческий анализ рабочих станций, также основанный на сравнении активности рабочих станций с эталонной моделью.

Что обеспечит Deception:

- Обнаружение в режиме реального времени целенаправленных атак и атак нулевого дня
- Защиту реальных ИТ-активов за счет переключения активности атакующих на «ловушки»
- Защиту ценных данных от «шифровальщиков»
- Сбор доказательств о действиях злоумышленников
- Отсутствие ложных срабатываний
- Не использует агентов и не оказывает влияния на работу пользователей и ИТ-сервисов

Результаты:

- Профиль злоумышленника

- Детализированные методы и инструменты, используемые во время атаки
- Углубленный анализ (какие цели преследуют хакеры, какую информацию они ищут)
- История и хронология взлома
- Источники происхождения злоумышленников на основе их IP-адресов и данных DNS

Ущерб от атак

Подсчитать реальный ущерб от таргетированных атак не представляется реальным: по данным ESET, 66% инцидентов системы безопасности остаются незамеченными многие месяцы. Именно под это и «заточено» сложное вредоносное ПО для целевых атак: кража данных происходит незаметно, в «фоновом» режиме.

Большое количество атак остается незамеченными. При обнаружении многие компании стараются скрыть факт инцидента и не предавать его огласке. В «Лаборатории Касперского» считают, что каждую неделю в мире становится известно как минимум об одной громкой целевой атаке. В реальности таких громких атак в неделю может происходить более ста.

Вывод

Из выше сказанного можно сделать вывод, что таргетированные атаки являются наиболее опасным деструктивным свойством ИТ-сферы и методы борьбы с ними очень индивидуальны, что и является одной из главных сложностей. Также сложность обнаружения таких атак заставляет очень скрупулезно подходить к ним, а в связи с тенденцией доступности инструментов атаки, делать это становится в разы сложнее.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился с сущностью целевых атак и методами защиты от них. Детально разобрано отличие целевых атак, а также их алгоритм действий. Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1) [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.tadviser.ru/index.php/Статья:APT_-_Таргетированные_или_целевые_атаки
2) [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://lib.itsec.ru/articles2/target/advanced-persistent-threat-rasstavlyaem-tochki-nad-i
3) [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://networkguru.ru/advanced-persistent-threat/
4) [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://cloudnetworks.ru/analitika/apt-ugrozy-i-kak-zashhititsya/
5) [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.securitylab.ru/blog/company/hlsec/252601.php