УДК 004.7

Плетеный Д.С.
студент магистратуры
2 курс, факультет «Отдел магистратуры»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Аленченко В.В.
студент магистратуры
2 курс, факультет «Отдел магистратуры»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Научный руководитель: Кузнецов Михаил Владимирович

МЕТОД АКТИВНОГО ПОИСКА УГРОЗ В ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ

Аннотация: *в статье рассматривается способ повышения информационной безопасности в корпоративной сети при использовании метода активного поиска угроз.*

Ключевые слова: *метод, активного, поиска, угроз, защита, доступ, безопасность, вредоносный, злоумышленники, сеть, предприятие.*

Annotation: *the article discusses a way to increase information security in a corporate network using the active threat search method.*

Key words: *method, active, search, threat, protection, access, security, malicious, attackers, network, enterprise.*

Активный поиск угроз - это метод, который позволяет выявлять те угрозы, которые программа не способна опознать как вредоносное действие. Поскольку

программы обеспечения безопасности в основном только предупреждает о подозрительных действиях, то данный метод укрепляет информационную безопасность от таких действий со стороны злоумышленника, который мог незаметно пробраться в защищаемую среду. Данный метод отличается от традиционных расследований и ответных мер, которые основываются на предупреждениях и предпринимаются после выявления вредоносной деятельности. Этот способ может показаться идеальным решением для профилактики безопасности, но все мы знаем, что идеального ничего не существует, и у любого метода поиска угроз есть свои недостатки. Но несмотря на это, такая процедура должна быть запланирована и регулярно проводиться, дабы усилить защиту корпоративной сети от вредоносных действий со стороны. Это всего лишь дополнительный инструмент обеспечения безопасности из множества других.

Обнаружение заранее неизвестных угроз будет являться важным событием для предприятия. Это поможет выявить в сети слабые места, которые возможно в последствии усилить и внедрить новую политику безопасности. В итоге результатом периодического активного поиска скрытых угроз будет являться значительное сокращение пространства для всевозможных вредоносных действий. Такие мероприятия позволяют заранее определить события, для которых можно инициировать различные предупреждения о возможном вредоносном поведении и определить необходимость в автоматизации данного метода для периодического повторения нужных действий по поиску угроз. В последствии эти наработки могут использоваться как дополнительные меры по активному поиску угроз, а также расширять функционал защиты.

Далее будут описаны тонкости и нюансы метода активного поиска угроз, а также объяснить, почему это весьма полезная инициатива, когда необходимо прибегать к данному методу и кто в организации будет им заниматься. Кроме этого, существует несколько дисциплин, непосредственно связанных с защитой от вредоносных действий, задачи которых пересекаются с задачами метода активного поиска угроз.

Метод активного поиска угроз является относительно молодой специализацией. Поэтому у данного метода есть схожесть с другими методами обеспечения безопасности. На деле многие специалисты, которые сегодня занимаются активным поиском угроз, имеют аналогичный опыт работы на других должностях. Далее будут приведены краткие сравнения метода активного поиска угроз с другими дисциплинами.

Реагирование на инциденты

Данная дисциплина наиболее всего схожа с методом активного поиска угроз. Обе дисциплины непосредственно работают с угрозами в корпоративной среде. Основное их различие заключается в реагировании на возможные инциденты: вы получаете сообщение о проникновении в сеть или попытке получения доступа к сети компании исходя из предупреждений системы безопасности, поведения самой сети, подключенных устройств или других фактов. При активном поиске угроз никаких свидетельств угрозы нет. Вы активно ищете возможную скрытую угрозу вместо того, чтобы сдерживать и пытаться устранить уже известную угрозу.

Тестирование на проникновение

Активный поиск угроз и тестирование на проникновение также имеют между собой некоторые сходства. Обе дисциплины предусматривают в себе поиск уязвимостей внутри сети. Как правило, тесты на проникновение обычно нацелены на поиск проблем с конфигурацией или заранее известных уязвимостей, которые позволяют получить доступ к сети предприятия или конфиденциальной информации. Однако при методе активного поиска угроз целью будет является не получение доступа к чему-либо, а выявление уже присутствующих в сети скрытых угроз, их подавление и разработка политик, которые позволят предотвратить такие угрозы в будущем.

Управление рисками

Метод управления рисками заключается в выявлении уязвимостей в сети, в оценке их серьезности, а также установлении приоритетов и последующем принятии необходимых мер по их устранению. Данная дисциплина может

включать в себя выявление источников угроз, а активный поиск угроз может помочь заполучить информацию для оценки рисков. Однако такие оценки, как правило, имеют гораздо больший охват, чем активный поиск угроз, и рассматривают все потенциальные уязвимости — как заранее известные, так и неизвестные.

Оценка компрометации

Оценка компрометации также схожа с активным поиском угроз. Данная дисциплина являет собой выявление возможного взлома сети компании неизвестными злоумышленниками и по сравнению с активным поиском угроз будет более масштабной. Для оценки компрометации в сети устанавливаются различные инструменты, которые выявляют любые признаки необычного поведения. Тем временем активный поиск угроз начинается с достаточно конкретной идеи или сценария и в дальнейшем сохраняет эту направленность.

Инвестиции в обнаружение скрытых угроз могут значительно повысить безопасность сети организации, если они были осуществлены заблаговременно. В современном мире существуют высококвалифицированные хакеры с хорошим финансовым обеспечением, которые могут быть нацелены на поиск уязвимостей и лазеек в сети предприятия и, к сожалению, не всегда возможно раскрыть все попытки злоумышленников даже с помощью самых лучших инструментов обеспечения безопасности. И для противодействия таким группам лиц и существует активный поиск угроз, круг задач которого предполагает обнаружение злоумышленников именно такого типа. Еще одно немаловажное преимущество активного поиска угроз заключается в том, что проведение таких мероприятий способствует более плотному изучению таких инструментов и методов, которые особенно необходимы при несанкционированных вторжениях или взломах. Вероятнее всего группа активного поиска угроз будет пересекаться с группой реагирования на инциденты, и различные методики активного поиска угроз будут способствовать членам этой группы совершенствовать свои навыки и значительно сократить время реагирования при возникновении реальных

случаев вторжения, соответственно, можно это рассматривать как практическую отработку нештатных ситуаций.

Создание группы активного поиска угроз достаточно сложно выполнимая задача, так как в ней необходимо объединить специалистов с разными навыками и опытом работы. Для крупного предприятия первый шаг может заключаться в выделении группе специалистов определенного временного интервала, например, длиною в месяц. Данная группа будет разрабатывать и реализовывать мероприятия по выявлению уязвимостей, а также вести отчетность о результатах исследований. В то же время, если рассматривать небольшое предприятие с малым количеством IT – специалистов, задача заметно усложняется. Для такого случая лучше воспользоваться услугами сторонних высоко квалифицированных специалистов. Такой вариант имеет как преимущества, так и недостатки. Преимущества - доступ к специалистам, имеющим знания и опыт, необходимые для активного поиска угроз. Но в то же время эксперты внешней группы активного поиска угроз не знают всех тонкостей и нюансы конкретной сети предприятия, как основной персонал. Для проведения мероприятий по активному поиску угроз требуется группа специалистов, владеющая следующими необходимыми навыками:

Знание основ защиты оконечных устройств и сетей

Это обязательное условие. В идеальном случае это опытные сотрудники центра информационной безопасности (SOC) или IT-отдела, которые отлично разбираются в проблемах информационной безопасности и имеют передовой опыт в данной области.

Понимание аналитики данных

Активный поиск угроз требует выделения характерных сигнатур из необработанных данных. Статистический анализ поможет выявить закономерности в таких данных. Визуализация данных также важна и для выявления различных отклонений, и для обмена информацией о них.

Врожденное любопытство

Активный поиск угроз совершенно не шаблонная процедура. Данный метод больше относится к творческому проявлению специальных знаний. Для него нужны определенное творческое мышление, а также способность сопоставлять несвязанные вещи и часто задаваться вопросом «Что было бы, если...». Одно из преимуществ активного поиска угроз для специалиста аключается в том, что данное занятие является увлекательным. Активный поиск угроз дает специалистам в IT-отделе передышку от повседневного реагирования на угрозы и возможность перейти в наступление. Такие динамичные задачи могут в дальнейшем способствовать удержанию специалистов, так как предоставляется возможность работать в области, где высококвалифицированных кадров найти проблематично.

Успешными операциями оказываются те, что тщательно были запланированы. Необходимо задать границы поиска, четкие цели и выделить определенное время. После тщательного анализа необходимо оценить меры по совершенствованию безопасности сети предприятия, а также создать сценарии обеспечения безопасности, которые позволят получить ожидаемый результат.

К тому же мероприятия активного поиска угроз будут своевременны, если найдутся основания предположить, что были замечены подозрительные операции. В качестве примеров приведем следующие операции:

-пользователь в конкретный день загружает избыточное количество данных, чем обычно;

-пользователь пытается войти в систему, к которой у него нет доступа;

-администратор подчищает журналы;

Такие примеры могут указывать на операции злоумышленника, который взломал какое-либо устройство. Это относительно несложный подход к началу активного поиска угроз. Существуют случаи, когда необходимость в активном поиске угроз возникает неожиданно. Как правило, такая потребность возникает в моменты поступления тревожных новостей из области информационной безопасности компаний, и руководство решает незамедлительно оценить состояние сети компании.

В конечном итоге ключом к поиску уязвимостей будут являться данные. Предварительно перед поиском угроз необходимо организовать надлежащую регистрацию данных, поскольку если проблематично отследить события в системах, возникают сложности с реагированием на происходящее. Выбор систем для изучения данных зависит от границ охвата поиска. Это могут быть как оконечные устройства в финансовом отделе, так и серверы. В определенных ситуациях могут потребоваться инструменты для мониторинга определенных типов трафика.

Ведение журналов регистрации может достаточно быстро исчерпать ограниченные ресурсы хранения данных, а работа с самими журналами может занять огромное количество времени у аналитической группы. Применение программного обеспечения для управления событиями и данными безопасности (SIEM) поможет заметно ускорить и упростить анализ журналов. В процессе первоначальных мероприятий активного поиска результаты покажут некоторый список вопросов, ответы на которые на основе имеющихся данных получить не удается возможным. При регулярности данных мероприятий станет более ясно, где следует вести журналы, дабы добиться положительных результатов.

Аналитик из области безопасности информации Дэвид Бьянко (David J. Bianco) разработал методику «пирамида боли» («pyramid of pain»), которая наглядно иллюстрирует способы усложнения работы для хакеров (рис.1). Каждый уровень данной пирамиды иллюстрирует различные подходы к данному вопросу, от простого до самого сложного. В основе данной пирамиды расположены хеш-коды. Файлы, содержащие в себе известные вредоносные хеш-коды, могут быть легко обнаружены, но при этом могут быть легко заменены злоумышленником. IP-адреса так же легко подлежат подмене, но для этого требуется немного больше работы как для поиска, так и для их подмены злоумышленником, следовательно они занимают меньший сегмент пирамиды. Домены немного сложнее, чем IP-адреса, сетевые артефакты еще сложнее и т.д. Цель активного поиска угроз — вычислить тактику, методы и процедуры (кратко ТМП), которыми пользуется хакер. Это и будет являться наиболее ценными

сведениями, поскольку злоумышленнику сложно их изменить. Их выявление является самой трудоемкой частью процесса, так как необходимо проводить сравнительный анализ точек данных из различных наборов данных и создания связей в первую очередь там, где эти связи не являются очевидными.

Рисунок 1. «Пирамида боли» Дэвида Бьянко

Сложность заключается в следующей идее: когда вы движетесь вверх по пирамиде, вы тем самым заставляете хакеров расходовать больше ресурсов на атаку сети предприятия, что значительно усложняет и увеличивает вероятность того, что они будут выявлены. Главная цель «пирамиды боли» заключается в том, что меняясь согласно ее принципам ваша сеть стала сложной для взлома настолько, что злоумышленникам придется отказаться от их намерений и перейти к другим целям.

В определенных случаях действия по активному поиску угроз основаны на исследованиях или отчетах о недавно обнаруженных уязвимостях. В настоящее время распространенной практикой является указание в данных исследованиях индикаторов компрометации (ИК), которые могут быть использованы другими заинтересованными сторонами. Точки данных, как правило, состоят из IP - адресов, URL - адресов, доменов, хеш - кодов файлов или других ИК, составляющих угрозу. Один из простых способов начать мероприятия активного поиска угроз - изучение журналов систем на наличие ИК. Для начала будет

достаточно использование инструментов командной строки или простых сценариев. Применение SIEM (Security information and event management) – еще один способ быстрого поиска ИК в журналах. Кроме этого также существуют более совершенные средства обеспечения безопасности сети, которые заметно упрощают активный поиск угроз, предоставляя возможность копировать и добавлять ИК на панель мониторинга, дабы отслеживать их появление в среде.

При освоении вышеперечисленных действий можно приступать к углубленному изучению журналов и начать поиск других возможных ИК. В таком случае потребуются навыки анализа данных. Использование статистических моделей, таких как кластеризации или распределения частот, может помочь выявить какие-либо отклонения. Главной целью является подъем к вершине «пирамиды боли» и определение тактики, методов и процедур (ТМП) злоумышленника.

Свежие новости об информационной безопасности могут в себе содержать много полезной информации для активного поиска угроз. В качестве примера можно рассмотреть процессы в Windows, в которых недавно были обнаружены критические уязвимости, из-за которых следовало бы проверить подозрительную активность, непосредственно связанные с этими процессами. Изучение отчетов работников о необычном поведении систем также немаловажно при данных аналитических методах.

Подозрительная активность может является неплохой отправной точкой, но ее не так просто зафиксировать. Для этого приходится приложить достаточно много усилий. Основные виды деятельности, на которые стоит обратить внимание, перечислены ниже:

-длительные сетевые подключения, из которых могут следовать утечки данных. Фильтрация надежных источников поможет вычислить подозрительные соединения.

-пиковые нагрузки центрального процессора, а также процессы, которые их создают. Данное действие может свидетельствовать о майнинге криптовалют

или протоколировании процессов с целью кражи информации. Фильтрация известных процессов поможет выявлять такие случаи.

-заранее запланированные задачи. В данном случае злоумышленники могут добавить собственные задачи с целью запустить определенные вредоносные действия. Анализ любых возможно подозрительных задач поможет выявить случаи вредоносного воздействия.

Любые случаи необычного поведения являются объектами углубленного анализа и поиска первоисточников. Тем не менее при оценке выявленных аномалий необходимо соблюдать осторожность. Как правило потому, что не все необычные действия предполагают собой злые умыслы. Обязательно нужно сопоставлять полученные результаты с прочими источниками данных.

Вывод

Важными аспектами активного поиска угроз являются выяснение путей их проникновения в сети предприятий и принятие мер по предотвращению атак в будущем. Важно выявлять уязвимости внутри инфраструктуры предприятия. Правильно выполненная кампания по активному поиску угроз может выявить неправильно сконфигурированный сервер или нарушение политики безопасности, которое в обязательном порядке необходимо устранить. Иногда хорошо выполненные мероприятия активного поиска угроз могут не выявлять уязвимости. Однако это будет значить то, что для организации в ближайшем будущем нет повода волноваться за сохранность конфиденциальных данных.

Использованные источники:

1. Отчет Cisco по информационной безопасности за 2018 год [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf
2. Threat Hunting Report [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/pdfs/cybersecurity-series-2019-threat-hunting-ru.pdf

3. Блог Cisco в России и СНГ [Электронный ресурс]. URL: https://gblogs.cisco.com/ru/
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: учебное пособие. - М.: ДМК Пресс, 2012. - 592 с.
5. Калашников С.К. История «болезней» VPN // Журнал сетевых решений, 2013. - № 11.