Мошенничество и киберпреступность

Дальневосточный федеральный университет

Школа естественных наук

Кафедра информационной безопасности

Бондарь А., Кваша А., Макаренко О.

Ключевые слова: Кибератаки, Тенденции киберпреступности, Таргетированный атаки, Вирусы,

Введение в проблему

В век информационных технологий все большую силу набирают различного рода киберпреступления. В цифровом мире крутятся очень крупные суммы и все больше злоумышленников претендуют на них. Так называемые киберпреступники становятся более лояльными между собой, что является следствием легкодоступности инструментов для атак. Благодаря этому, даже хакер-любитель может стать профессионалом - создать весомую проблему для бизнеса любого вида деятельности. Развитие тенденции качества и количества киберпреступлений становится большой проблемой для сферы безопасности.

Тагретированные атаки – в тихом омуте черти водятся

Такой вид кибератак, которой свойственно индивидуальный подход к каждой жертве, из этого и выливается особенности, а именно:

Сфокусированность - выбранная жертва всесторонне изучается профессиональной группой хорошо подготовленных специалистов, которые действуют не как грабители в переулке, а скорее как киллеры.

Многовекторность – высокая квалификация атакующих позволяет им сочетать методы нападения различной природы в поисках оптимального сценария проникновения.

Продвинутость, прогрессивность – злоумышленники могут комбинировать сложнейшее вредоносное ПО, использующее уязвимости нулевого дня, с элементарными приемами социальной инженерии и фишингом, физическим проникновением и другими тактиками.

Устойчивость, постоянство – термин «устойчивость» в аббревиатуре APT используется, чтобы описать трудности в устранении обнаруженных APT, а также намерение атакующих оставаться незамеченным в скомпрометированной системе в течение нескольких месяцев или лет.

Цели таких атак: Офис правления компании, НИОКР, Центры обработки данных, Сеть поставщиков, Облачные вычисления, Производство, Базы данных, Конечная продукция, Офисные сети, Продажи, Интернет-магазины, Телефонные звонки.

Атаке быть, вам не выиграть

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.

Deception-ловушки – главный инструмент борьбы

Технология Deception является наиболее эффективным способом обнаружения APT-атак, так как она использует тактику атакующих против них. Используя ловушки и приманки с высоким уровнем интерактивности, Deception обманывает злоумышленников, заставляя их раскрывать себя, тем самым закрывая те угрозы, с которыми не справились другие средства защиты. Используя такие приманки, как: учетные данные пользователей, серверы, сайты, вы можете обнаружить хакеров до того, как им станет доступна конфиденциальная информация.

Статистика или ее отсутствие

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.

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.

Противодействие мошенничеству и киберпреступности

Киберпреступность - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Типы киберпреступлений

· Мошенничество с электронной почтой и интернет-мошенничество

· Мошенничество с использованием личных данных

· Кража финансовых данных или данных банковских карт

· Кража и продажа корпоративных данных

· Кибершантаж

· Атаки программ-вымогателей

· Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)

· Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Вирусы-Шифровальщики

Программы-шифровальщики относятся к классу троянцев-вымогателей — это вредоносное ПО, которое вносит несанкционированные изменения в пользовательские данные или блокирует нормальную работу компьютера. Для расшифровки данных и разблокировки компьютера злоумышленники обычно требуют денежного перевода (выкупа).

Как защититься от шифровальщиков?

· Регулярно делать резервные копии данных, чтобы их можно было восстановить в случае инцидента.

· Использовать инструменты для автоматического обнаружения уязвимостей и установки исправлений.

· Своевременно обновлять приложения и операционные системы на всех устройствах.

· Не открывать подозрительные файлы или ссылки в электронных письмах.

· Установить на компьютер антивирус

· Скачивать программы только с сайта разработчика или с проверенных ресурсов.

Вирус-шифровальщик Netwalker

Netwalker — это быстро набирающая масштабы программа-вымогатель, созданная в 2019 году группой киберпреступников, известной как Circus Spider. На первый взгляд Netwalker действует, как и большинство других разновидностей программ-вымогателей: проникает в систему через фишинговые письма, извлекает и шифрует конфиденциальные данные, а затем удерживает их для получения выкупа. Но Netwalker способен на большее, чем просто удержание захваченных данных. Чтобы продемонстрировать серьезность своих намерений, Circus Spider публикует образец украденных данных в интернете, заявляя, что, если жертва не выполнит их требования вовремя, то в даркнет попадут и остальные данные. Circus Spider выкладывает

конфиденциальные данные жертвы в даркнете в защищенной паролем папке и публикует пароль в интернете.

Сферы, атакуемые Netwalker:

· образование

· здравоохранение

· производство;

· управление бизнесом;

· управление потребительским опытом и качеством обслуживания;

· электромобили и решения для накопления электричества;

· образование;

Как работает Netwalker?

· 1: Проникает в систему

· 2: Шифрует данные

· 3: Вымогательство, шантаж, использование данных в личных интересах злоумышленников

Советы по защите от программы-вымогателя Netwalker:

· Выполнять резервное копирование важных данных на локальные хранилища данных;

· Убедиться, что копии критически важных данных хранятся в облаке, на внешнем жестком диске или устройстве хранения;

· Защитить свои резервные копии и убедиться, что данные невозможно изменить или удалить из системы, в которой они хранятся;

· Установить и регулярно обновлять антивирусное программное обеспечение на всех компьютерах;

· Использовать только безопасные сети и избегайте общедоступных сетей Wi-Fi. По возможности используйте VPN;

· Использовать двухфакторную аутентификацию с надежными паролями;

· Регулярно обновлять компьютеры, устройства и приложения.

Любые информационные и технические новации значительно расширяют сферу киберпреступности.

В отличие от других видов экономической преступности, киберпреступность в настоящее время является наиболее быстрорастущим сегментом, что связано с увеличением численности пользователей компьютеров, подключенных к глобальной сети Интернет, постоянным повышением уровня профессионализма киберпреступников, устойчивым развитием и совершенствованием информационных технологий. Любые информационные и технические новации значительно расширяют сферу киберпреступности и создают условия для повышения эффективности хакерских атак, поэтому киберпреступность растет более быстрыми темпами, чем все другие виды преступности.

Так, уровень киберпреступности повысился с 24% в 2014 г. до 32% в 2016 г., заняв вторую позицию среди видов экономической преступности в мире, опередив отмывание денег, коррупцию и другие составляющие.

Очевидность совершения преступных действий не всегда явная, могут совершаться совершенно скрытно.

Киберпреступления ввиду их относительной ненаказуемости, а также высокой доходности являются достаточно привлекательным видом деятельности. Риски и издержки при совершении киберпреступлений равны рискам и издержкам при осуществлении легальной трудовой деятельности (производственный травматизм, монотонность трудовой деятельности, стрессы, риск сокращения и т.д.). Распространение интернета привело к устранению национальности киберпреступности, сделало ее подлинно интернациональной. Хакер может иметь гражданство одной страны, находиться на территории другой и при этом работать через сервер, расположенный в третьей стране.

Очевидность совершения преступных действий не всегда явная, могут совершаться совершенно скрытно, в результате пострадавшая сторона узнает

об этом через достаточно большой промежуток времени. Место нахождения преступника и факт совершения преступных действий, сбор доказательств являются затруднительными для правоохранительных органов, осуществления процессуальных действий.

Продолжительность самих атак при этом варьируется в достаточно большом временном интервале: от нескольких секунд до суток и месяцев.

Достаточно легкой жертвой киберпреступности являются предприятия малого и среднего бизнеса

Рост киберпреступности связан преимущественно не с крупными предприятиями, а именно с предприятиями МСБ. Такие предприятия в силу малого бюджета, отсутствия квалифицированных кадров, пробелов в познаниях сотрудников не могут на должном уровне обеспечить качественную информационную безопасность.

Для больших компаний, в отличие от малого и среднего бизнеса, защита конфиденциальной информации, интеллектуальной собственности имеет принципиально важное значение для успешного ведения бизнеса и требует разработки комплексной стратегии безопасности, исходя из целей деятельности компании.

Интернет-банкинг по-прежнему остается одним из лидеров в перечне киберпреступлений.

Электронные технологии, с одной стороны, снизили себестоимость оказываемых услуг, с другой стороны, расширение применения данных

технологий увеличило возможности киберпреступников в совершении незаконных финансовых операций, что повысило риски обеспечения финансовой безопасности в банках. Преступники обогащаются за счет кибер-шантажа, вымогательства, снятия денежных средств со счетов клиентов банка.

Распространению киберпреступности в банковской сфере способствует использование банками устаревших технологий, не способных противостоять преступникам.

Заключение

Киберпреступность прошла фазу становления, «детства» и перешла на принципиально новый уровень, включающий вымогательство, промышленный шпионаж, таргетированные атаки.

Изменился и сам хакер: из любителя превратился в профессионала, являющегося частью криминального бизнеса. Киберпреступники наносят значительный ущерб как отдельным гражданам, организациям, предприятиям, так и всей национальной экономике при минимальном для себя риске.

Злоумышленники идут на несколько шагов вперед, увеличивая отрыв от систем безопасности компаний. Решение же проблемы киберпреступности состоит не в подстраивании компаний под существующие тенденции, а в активной разработке информационной безопасности стратегии предприятий на опережение.