Кибертерроризм

написано Александр Астахов | 10 июня, 2023

> *«Рассмотрим следующий сценарий… В один прекрасный день террористическая организация заявляет о том, что они отключат Тихоокеанскую Северо-западную электрическую сеть на 6 часов, начиная с 16.00. Затем они выполняют обещанное. Эта же группа затем заявляет, что они отключат основную телекоммуникационную магистральную линию связи между Восточным и Западным побережьем США на полдня. Затем они выполняют обещанное, несмотря на все наши усилия этому помешать. Затем они угрожают вывести из строя систему управления воздушным трафиком города Нью-Йорк, заставляя приземляться все самолеты, отводя в сторону входящий трафик, и выполняют обещанное. Далее следуют другие угрозы, которые тоже успешно приводятся в исполнение, демонстрируя возможности наших врагов успешно атаковать критичную сетевую инфраструктуру. Наконец террористы угрожают парализовать сервисы электронной коммерции и кредитных карт на неделю путем использования нескольких сотен тысяч похищенных идентификационных номеров в миллионах поддельных транзакций в случае, если их требования не будут удовлетворены. Вообразите, какую панику и всеобщий хаос это вызовет».*
>
> *Отрывок из письма к Президенту США от лица 50 ученых, компьютерных экспертов и представителей американских разведслужб*

Что делает этот сценарий интересным и волнующим, так это то, что все упомянутые события уже происходили ранее, хотя и не в одно и то же время и не все по злому умыслу. Все это происходило как изолированные события, распределенные во времени. Некоторые – в результате технических неполадок, другие были результатом неудачных экспериментов, а некоторые из них – в результате осуществления реальных кибератак. Важен тот факт, что все эти события могут быть осуществлены в

результате кибератак.

Цитируемое письмо было написано уже много лет назад, когда кибератаки еще не были столь массовым явлением как сейчас. В наши дни средства массовой информации ежедневно публикуют информацию о десятках и сотнях компьютерных инцидентов, начиная с крупных утечек данных и заканчивая ограблениями банков через Интернет. В России ежегодно совершаются десятки тысяч компьютерных преступлений, а многие «некомпьютерные» преступления также не обходятся без использования компьютеров и реализации информационных угроз. Кибер-преступность ежегодно наносит ущерб государствам и бизнесу по всему миру на миллиарды долларов и имеет тенденцию к значительному росту.

В таком потоке информации недолго утонуть, поэтому позволим себе сделать небольшой экскурс в историю, чтобы читатель смог получить более структурированное представление о ландшафте современных кибер-угроз. Подробная антология кибератак приведена в Приложении № 2.

Официальный отсчет истории кибер-преступности начинается в начале 70-хх годов. В 1971 году телефонный фрикер Джон Дрейпер обнаружил, что забавный свист, упакованных в коробки зерновых хлопьев мог быть изменен, для генерации тонального звука с частотой в 2600 герц. Она совпадала с частотой, используемой телефонными компаниями, для указания того, что магистральная линия была доступна для маршрутизации нового запроса. Направление свиста в приемник телефонной трубки разъединяло один конец магистрали, позволяя войти в режим оператора (полезная функция для обслуживающего персонала, а также для фрикеров).

Коробка с хлопьями, положившая начало кибер-преступности

«Проблема состояла в том, что телекоммуникационные компании позволяли таким си

гнал ам попадать в полосу частотли ни и связи, благодаря чему пользователи могли со

здавать, а также «передавать» эти сигналы. Хотя большинство из этого было переме

щественно вне полосы передачи сигналов, проблема все еще существует для многих старых

коммутаторов, как в некоторых штатах США, так и в ряде мест за границей», — гово

рит Маддж, хакер, перекваливировавшийся в компьютерного исследователя в ВВ

N
Технологиях.
В результате фрикер получает возможность осуществлять бесплатные

телефонные звонки и другие противозаконные действия.

Данный эпизод считается прародителем компьютерного хакинга. Дрейпер продолжал создавать «синие коробки», способные к репродуцированию других тонов, используемых телефонной компанией и позволяющих их пользователям делать бесплатные междугородные звонки. Деятельность Дрейпера была освящена в статье журнала «Эсквайр» в 1971 году, которая возбудила интерес творческого дуэта по имени Стив Джобс и Стив Возняк, который самостоятельно начал выпускать «синие коробки». Позднее они основали компанию Apple.

В 1988 году Роберт Т. Моррис, 23-летний студент Корнельского

университета, написал некий программный код как часть научно-исследовательской работы, нацеленной на определение размера Интернет. Код предназначался для заражения компьютеров, но только с той целью, чтобы увидеть, сколько существовало подключений в Интернет. Однако, из-за ошибок, допущенных при программировании, все это закончилось использованием уязвимости в ОС Unix и быстрым распространением с многократным заражением множества хостов и выводом их из строя.

Робер Моррис — создатель первого сетевого червя

Этот случай рассматривается как момент появления первого ко

мп
ью
те
рн
го
че
рв
я,
ра
сп
ро
ст
ра
ня
ющ
ег
ос
я
че
ре
з
Ин
те
рн
ет
,
и
по
ло
жи
вш
ег
о
на
ча
ло
эп

ох
е
вр
ед
он
ос
но
го
пр
ог
ра
мм
но
го
об
ес
пе
че
ни
я.
Че
рв
ь
Мо
рр
ис
а
та
кж
е
бы
л
пе
рв
ым
ки
бе

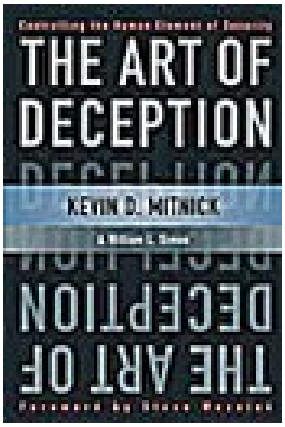
р-
ин
ци
де
нт
ом
,
по
лу
чи
вш
им
за
ме
тн
ое
вн
им
ан
ие
со
ст
ор
он
ы
СМ
И
и
су
де
бн
ой
си
ст
ем
ы.
В

1990 Морис был приговорен американским окружным судом к трем годам условного за

ключения, 40 часам общественных работ и штрафу в размере 1005 долларов.

В 1995 году начал отбывать свой пятилетний срок Кевин Митник, являющийся волей судьбы, пожалуй, самым знаменитым хакером в

истории. В течение двух с половиной лет он взламывал компьютерные системы и крал конфиденциальную информацию у крупных американских корпораций, включая Motorola и Sun Microsystems.



Книга Кевина Митника «Искусство взлома»

Этот случай впервые поместил хакера в центр общественного внимания.

Действия Митника наглядно проиллюстрировали концепцию социального инжиниринг

а
–
ис
по
ль
зо
ва
ни
е
ма
ни
пу
ля
ци
и
и
об
ма
на
вм
ес
то
те
хн
ич
ес
ки
х
по
дх
од
ов
дл
я
по
лу
че

ния несанкционированного доступа к компьютерным системам.

Освободившись из мест заключения Кевин Митник встал на путь исправления. Сейчас он руководит собственной компанией и консультирует организации по всему миру по вопросам обеспечения информационной безопасности. Его книга «Искусство взлома» в увлекательной манере повествует о том, каким образом осуществляются атаки и взламываются компьютерные системы.

2004: Остроумный Червь (Witty Worm)

Этот компьютерный червь атаковал брандмауэр и другие продукты безопасности компании ISS. Согласно Брюсу Шнеиру, старшему менеджеру по технологиям компании «Бритиш Телеком», после объявления об уязвимости распространение червя пошло очень быстро, заражая 12 000 компьютеров за 45 минут. По сравнению с предыдущими червями этот червь также инфицировал меньшие и более устойчивые к заражению хосты.

Остроумный Червь – первое значительное по воздействию вредоносное ПО, использовавшее в своих интересах уязвимость в определенном наборе продуктов безопасности – BlackICE ISS и RealSecure. Это был один из первых червей, которые используют предварительно загруженный список целевых систем. Этот вирус был нацелен на системы обеспечения сетевой безопасности, и ходили слухи, что он был создан сотрудником конкурирующей компании.

2005: Титановый дождь (Titan Rain)
Кодовое название, данное правительством США ряду хакерских атак, инициированных из Китая в 2003 году. Целями служили вычислительные сети в Министерстве обороны и других правительственных агентств США.

Титановый дождь – первый инцидент кибер-шпионажа национального масштаба. Однако подробности Титанового дождя спорны. Некоторые полагают, что в этом замешано китайское правительство, другие считают, что нападения были работой хакеров, использующих китайские веб-сайты просто для того, чтобы скрыть свои следы.

Наиболее уязвимой в отношении кибератак является инфраструктура самой сети Интернет. Достаточно привести пример сетевого червя Nimda, нанесшего подключенным к Интернет организациям совокупный ущерб, оцениваемый в 3 млрд. долларов.

Некоторые уязвимости Интернет могут приводить к серьезным последствиям и в отсутствии кибератак. Показательным является

пример, когда в 1997 году инженер одного из Интернет-провайдеров изменил две строчки кода в конфигурации маршрутизатора, что на три часа привело к останову почты всей глобальной сети. Тем не менее, несмотря на всю серьезность происшедшего, катастрофичным данный инцидент назвать нельзя, хотя совокупный ущерб оказался очень большим за счет того, что урон, хоть и незначительный, был нанесен слишком большому количеству компаний одновременно.

В октябре 2002 года была предпринята беспрецедентная в истории Интернет атака против всей инфраструктуры всемирной сети. Тринадцать корневых DNS-серверов Интернет подверглись распределенной атаке на отказ в обслуживании (DDoS). По словам председателя Консорциума Программного Обеспечения Интернет (Internet Software Consortium Inc.) Пола Викси только четверым из них удалось устоять. Большой уровень избыточности, присущий структуре Интернет, позволил избежать задержек при прохождении трафика, несмотря на выход из строя 2/3 корневых элементов инфраструктуры сети.

Угроза кибертерроризма уже не первый год широко обсуждается в современном обществе на самых разных уровнях, порождая множество споров, мифов и спекуляций. Неадекватная оценка рисков, связанных с осуществлением этой угрозы, приводит как к недооценке, так и к переоценке ее серьезности. В результате, наряду с «устрашающими» описаниями глобальных катастроф, нередко встречается и полное игнорирование этой проблемы. Понятие кибертерроризма часто используется для политических спекуляций и «запудривания мозгов» непосвященным.

Подключение к сети Интернет открывает дополнительные возможности проникновения злоумышленников в компьютерные системы, однако сам факт наличия такого подключения не следует во всех случаях рассматривать как уязвимость. Серьезные меры по резервированию данных и оборудования, предпринимаемые предприятиями различных отраслей, в большинстве случаев обеспечивают адекватный уровень защищенности, даже при успешном осуществлении кибератаки.

К таким выводам автор пришел в 2003 году, когда писал статью под названием «Реалии и мифы кибертерроризма». За прошедшие шесть лет риски киберпространства существенно возросли. Возможно, в ближайшем будущем нашу оценку этих рисков придется пересмотреть в большую сторону.