Приложение 2. Антология кибератак

написано Александр Астахов | 11 июня, 2023

В следующей таблице представлена антология наиболее значимых кибератак на информационную инфраструктуру США в их исторической последовательности. Не все эти атаки носили предумышленный характер, и ни одна из них не привела и не могла привести к массовым разрушениям, катастрофам или гибели людей. Однако все эти события принесли массу неприятностей и финансовых проблем очень большому количеству людей и компаний.

1988	Роберт Моррис запустил в Интернет первого сетевого червя, поразившего примерно 3–4 тысячи из 60000 тысяч Интернет-серверов.
1989	Хакерская группа «The Legion of Doom» получила контроль над телефонной сетью BellSouth, включая возможность прослушивания телефонных каналов связи, маршрутизацию вызовов и маскировку под технический персонал станции.
1990	Отказ маршрутизатора AT&T вызвал глобальный сбой сети на большой территории, длившийся 9 часов. Многие думали, что это дело рук хакера.
1994	Хакер, известный под кличкой Merc, по модему получил доступ к серверу проекта «Солт Рива» и взломал компьютеры, при помощи которых осуществлялся мониторинг водных каналов в области Фоникса.

1994	Российский хакер Владимир Левин взломал систему управления денежными операциями Ситибанка и перекачал 10 млн. долл. на свои собственные счета. Украденные счета были без криптографической защиты. Все похищенное, за исключением 400 тысяч долларов, было восстановлено, а в 1995 году Левин был арестован и в 1997 году выдан США. В 1998 году он был признан виновным в компьютерном мошенничестве. Судья федерального суда приговорил Левина к трем годам заключения и штрафу в 240 тысяч долларов, выплачиваемым Ситибанку.
1995	Это было годом, с которого Митник начал отбывать пятилетний срок тюремного заключения после двух с половиной лет хакерства, в течение которого он взламывал компьютерные системы и крал файлы у ряда корпораций, включая Motorola и Sun Microsystems. Он был арестован после взлома очередной системы одного компьютерного исследователя, который помог ФБР арестовать Митника.
1997	Технический работник небольшого Интернет-провайдера Virginia внес в конфигурацию одного из маршрутизаторов неправильные данные. Это привело к отказу большого количества критичных маршрутизаторов сети Интернет.Подросток выводит из строя основной компьютер телефонной компании, обслуживающей маленький аэропорт в городе Ворсестер, из-за чего диспетчерская вышка не смогла выполнять свои функции в течение 6 часов. Однако самолеты получали информацию по радио и из других аэропортов, находившихся поблизости.
2000	Крупнейшая атака на отказ в обслуживании поразила серверы Yahoo, eBay, CNN, ZDNet, которые оставались недоступными от 2 до 3 часов.Вирус LoveLetter поразил сети множества компаний по всему миру, нанеся огромный совокупный финансовый ущерб.
2001	Вирус Nimda поразил Интернет, нанеся особо ощутимый ущерб финансовым компаниям.

2002	Тринадцать корневых DNS-серверов Интернет подверглись распределенной атаке на отказ в обслуживании (DDoS). Только четверым из них удалось устоять. Большой уровень избыточности, присущий структуре сети Интернет, позволил избежать задержек при прохождении трафика, несмотря на выход из строя 2/3 корневых элементов инфраструктуры сети.
2004	Компьютерный червь Witty Worm (Остроумный 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 тыс. компьютеров за 45 минут. По сравнению с предыдущими червями этот червь также инфицировал меньшие и более устойчивые к заражению хосты.
2005	Титановый дождь (Titan Rain) – кодовое название, данное правительством США ряду хакерских инцидентов посредством китайских веб-сайтов, начавшихся в 2003. Целями служили вычислительные сети в Министерстве обороны и других правительственных агентств США.
2005	ChoicePoint, один из крупнейших накопителей данных и реселлеров в США, объявил, что мошенники смогли получить доступ к базе данных, содержащей информацию о 145 тыс. потребителей. Компания была не в состоянии полностью идентифицировать частные лица и организации, купившие эту информацию, включая личные дела и номера социального страхования.
2006	Данные о 26,5 млн. ветеранов и членов действующего резерва национальной гвардии и резервных войск США были украдены у служащего агентства, который отнес свой ноутбук домой. Незашифрованные данные, которые включали номера социального страхования и даты рождения ветеранов и их супруг, были скомпрометированы.

2007	Интернет поразил троян Storm Worm (Штормовой червь), который содержит во вложении исполняемый файл. Когда получатель электронной почты открывает вложение, его компьютер становится частью бот-сети (сети зараженных компьютеров), которая используется для распространения вирусов и спама.
2007	Розничный гигант (чья торговая сеть включает TJ Maxx, Home Goods и Marshalls) изначально объявил, что данные о 46 млн. его клиентов были рассекречены посредством атаки через беспроводные сети компании. Хакеры были способны проникнуть в сеть и получить доступ к данным, передаваемым между переносными проверяющими цену наладонными устройствами, компьютерами магазина и кассовыми аппаратами. (Первичные атаки, возможно, имели место уже 2005 году, а также в период с мая 2006 года по январь 2007 года.) В октябре 2007 года количество скомпрометированных данных удвоилось. TJX критиковали за сбор избыточной информации, ее слишком долгое хранение и за то, что он был не в состоянии улучшить безопасность своей беспроводной сети, перейдя от WEP-протокола шифрования (старый стандарт) к WPA (который намного более надежен). TJX также подвергся нападкам за то, что долго выжидал перед уведомлением клиентов о нарушениях, а также за несоответствие стандартам безопасности данных индустрии платежных карт (PCI DSS).