Как защититься от кибероружия

Просянкина А.А., Трофименкова А.А.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Брянский государственный университет имени академика И. Г. Петровского»

г. Брянск, Россия

Аннотация: в статье рассматриваются виды кибероружия и способы защиты от него.

Ключевые слова: кибероружие, Интернет, защита.

How to protect yourself from cyber weapons

Prosyankin A. A., A. A. Trofimenkov

Federal state budgetary educational institution of higher education " Bryansk state University named after academician I. G. Petrovsky»

Bryansk, Russia

Abstract: the article discusses the types of cyber weapons and methods of protection against it.

Key words: cyberweapons, Internet, protection.

Определение кибератаки

Что такое кибератака? Это атака с одного или нескольких компьютеров на другой компьютер или сеть. Кибератаки можно разделить на два основных типа: атаки, в которых цель состоит в том, чтобы отключить целевой компьютер или отключить его в автономном режиме, или атаки, в которых цель состоит в том, чтобы получить доступ к данным целевого компьютера и, возможно, получить от них привилегии администратора.

Типы кибератак

Для достижения этих целей злоумышленники используют целый ряд различных технических методов. Всегда распространяются новые методы, и некоторые из этих категорий пересекаются. Далее представлены несколько типов кибератак:

1. Вредоносное ПО
2. Фишинг

3. DDoS-атаки
4. Атаки «человек посередине»
5. Cryptojacking
6. SQL-инъекция

Статистика кибератак

Чтобы понять, что происходит в темном мире киберпреступности, лучше погрузиться в цифры, которые, кажется, только растут. Число уникальных «кибер-инцидентов» во втором квартале 2018 года, по определению Positive Technologies, было на 47 процентов выше, чем за весь предыдущий год. И эти атаки становятся все более точными: 54 процента являются целевыми, а не частью массовых кампаний.

Вилли Саттон сказал, что он ограбил банки, потому что там деньги. Так что, возможно, неудивительно, что «Позитив» сообщил о большом всплеске атак на криптовалютные платформы, учитывая все более прибыльный характер этой технологии. В целом, киберпреступность принесла преступникам около $ 1,5 трлн в 2018 году. Отдельные киберпреступники могут рассчитывать на получение примерно на 10–15 процентов больше, чем их офлайновые эквиваленты. Около 10 процентов всех отмытых преступных доходов поступает от доходов от киберпреступности.

Но не стоит забывать о защите телефонов , ведь мобильные атаки растут. В третьем квартале 2018 года в «Лаборатории Касперского» количество вредоносных мобильных установочных пакетов выросло почти на треть по сравнению с предыдущими несколькими месяцами.

Компьютерный вирус – вид вредного ПО. Он способен создавать копии самого себя, внедряться в код остальных программ, в системные области памяти, в загрузочные секторы, а так же способен распространять свои копии по каналам связи.

Пока мы пользуемся своими ноутбуками и телефонами, за нашей сведениями разворачивается реальная охота. Кибервзломщики выдумывают все более трудные вирусы, а те кто с ними борются — придумывают все более трудную защиту.

Для начала необходимо отметить, что огромное количество атак ни на кого непосредственно не нацелена. Это как обычно Трояны либо фишинговые письма, которые просто так гуляют по сети. Их жертвами становятся обычно те, кто не побеспокоился о собственной безопасности.

Так же есть приложения при скачивании которых у вас могут списать средства. Однако приложения, которые готовы списывать у вас некоторые суммы это не так жутко. Самое ужасное, что может произойти — это если вы отдаете приложению свои root права. Приложение получает неограниченный доступ к глубинным функциям телефона и очистить уже будет нереально даже откаткой к заводской прошивке. Взломщик сумеет подсматривать за вами, он может перехватывать ваши смс, записывать речь с диктофона, следить за вами по геолокации.

Однако представим, что вы умнее всего этого: запретили покупки в сети интернет, не входите на какие-то непонятные веб-сайты, в принципе не пользуетесь интернетом и покупаете лишь на наличные, снимая средства в банкоматах. И здесь тоже может появиться опасность, по типу «скиммера», считывающих данные с вашей карты с помощью устройств, прикрепленных к банкомату, и посылает их жулику. Естественно, на данный момент банки направили на это внимание, но кибервзломщики тоже не посиживают без дела и выдумывают новые методы обхода, потому скиминг будет существовать, пока мы пользуемся платежными картами.

Цифровой мир в каком мы на данный момент живем кажется таким комфортным: все становится оцифрованным, все подключается к интернету, но вместе с этим приходят и новые угрозы от которых приходится защищаться. Уже на данный момент тостеры и регистраторы употребляют в кабератаках, а те же компании, которые 15 лет назад защищали ваши компы, на данный момент защищают фабрики и целые города. Однако какими бы надежными не были антивирусы, необходимо постоянно быть аккуратными в сети. Непременно удаляйте снимки экрана сообщений с паролями и не сохраняйте их в браузере, не переходите по ссылкам в комментариях. Непременно подключите двухфакторную аутентификацию на всех социальных сетях, пользуйтесь приложениями, а не веб-сайтами магазинов. Не пересылайте фото собственных платежных карт, не используйте всюду одни и те же пароли, скройте данные на сайтах социальных сетей и откройте ее лишь друзьям. Сделайте так, чтоб ваш профиль нельзя было найти по номеру телефона, и по данной же причине не доверяйте тем, кто просит вас выручить финансово, даже если это старый товарищ, которого вы знаете тысячу лет. Непременно инспектируйте, позвоните и удостоверьтесь, что это точно он. В общем, пользуйтесь правилами кибер гигиены.

Список литературы:

1. http://medicina-treat.ru/chto-takoe-kiberataka/ -кибератаки