КИБЕРПРЕСТУПНОСТЬ И ЧТО ОНА ЗА СОБОЙ ВЛЕЧЁТ

Толоконцева А.С.[1], Овчинникова А.А.[2], Валагов Д.А.[3] Email: Tolokontseva633@scientifictext.ru

[1]Толоконцева Анастасия Сергеевна – студент;
[2]Овчинникова Ангелина Александровна – студент;
[3]Валагов Дмитрий Александрович – студент,
направление подготовки: информатика и вычислительная техника,
Федеральное государственное бюджетное образовательное учреждение высшего образования Поволжский государственный университет телекоммуникаций и информатики,
г. Самара

Аннотация: *в данной статье пересмотрены аргументы выполнения хакерских атак и их результаты, а кроме того презентованы сведения о хакерских атаках в 2015 - 2017 годах; установлены наиболее популярные хакеры общества. Перечислены основные правила безопасного использования персонального компьютера. Исследованы статистические данные по количеству хакерских атак, как в России, так и за рубежом. Рассмотрены одни из самых популярных паролей пользователей за 2017 год. Приведены виды самых новейших вирусов и принцип работы одного из них.*
Ключевые слова: *хакеры, хакерские атаки, угроза, пользователи, персональные компьютеры, мошенники, информация, киберпреступник.*

CYBER CRIME AND THAT IT INVOLVES

Tolokontseva A.S.[1], Ovchinnikova A.A.[2], Valagov D.A.[3]

[1]Tolokonseva Anastasia Sergeevna – Student;
[2]Ovchinnikova Angelina Aleksandrovna – Student;
[3]Valagov Dmitry Aleksandrovich – Student,
DIRECTION OF PREPARATION: INFORMATICS AND ADP EQUIPMENT,
FEDERAL STATE BUDGET EDUCATIONAL INSTITUTION OF HIGHER PROFESSIONAL EDUCATION POVOLZHSKIY STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS,
SAMARA

Abstract: *in this article arguments of execution of the hacker attacks and their results are reconsidered, but also data on the hacker attacks in 2015-2017 are presented; the most popular hackers of society are set. The basic rules safe use of the personal computer are listed. Statistical data by the number of the hacker attacks, as in Russia, and abroad are probed. One of the most popular passwords of users for 2017 are considered. Types the newest viruses and the principle of operation of one of them are given.*
Keywords: *hackers, hacker attacks, threat, users, personal computers, swindlers, information, cybercriminal.*

УДК 004

Компьютерная индустрия очень уязвима с точки зрения безопасности. Когда-то под компьютерной безопасностью подразумевалась физическая безопасность. Компьютерные экраны имели тёмные фильтры чтобы никто не мог легко увидеть данные на экране. Под более замысловатой безопасностью понималось предохранение компьютерных систем от таких угроз как кража со взломом, вандализм, пожар, природные катастрофы, кража данных ради выкупа, промышленный шпионаж и множество различных преступлений которые могут осуществить «белые воротнички». Колоссальное влияние на социум проявило возникновение в завершении 70-х – истоке 80-х годов персонального компьютера. С каждым днем появляется всё больше пользователей глобальной сети Интернет и локальной сети. В связи с появлением в обществе ПК, возникла особая категория людей, которых в данный период времени называют хакерами (высококвалифицированные эксперты в IT-сфере, которые разбираются в деталях деятельности Электронно-Вычислительной машины (ЭВМ) [2]). Согласно аргументам их умышленных операций, и в связи с данными сведениями этих экспертов разделяют на «белых» и «черных». Так именуемые «белые» хакеры обнаруживают небольшие слабые участки в компьютерных системах и ликвидируют их. В то время как «черные» хакеры, распознавая эти слабые места в компьютерных концепциях, используют их в своих собственных интересах.

Хакер, в своём начальном значении, представлял человека, который имел великолепные знания в современных информационных технологиях. На сегодняшний день хакером чаще всего называют того, кто распознает слабые места в компьютерных системах ради забавы или личной выгоды, что порой для окружающих представляет собой откровенное мошенничество, преследуемое наказанием по закону той или иной страны. В соответствии с законодательством предусмотрено достаточно жёсткое наказание в

виде крупных денежных штрафов и выплат, вплоть до тюремного заключения, например, по статье 272 УК, 274 УК РФ [1, 4].

Множество злоумышленников создают IP-адрес так, чтобы их самих и их вмешательства не могли распознать, найти и прекратить. Для того чтобы хакерских атак с каждым днём становилось всё меньше, каждый человек должен сам обеспечивать себе безопасное пользование персональным компьютером, соблюдая элементарные правила защищённого использования. К таковым правилам можно отнести:

1. Старайтесь быть в курсе последних новостей информационной безопасности и чаще обновляйте ПО.
2. При регистрировании своего аккаунта на любом сайте желательно использовать пароль максимальной сложности.
3. При проверке писем в почтовом ящике электронной почты настоятельно не рекомендуется переходить по предлагаемым ссылкам на неизвестные пользователю сайты.
4. Пользователь должен быть крайне внимательным при переходе на подозрительные рекламные web-страницы.

Пользователь самостоятельно должен постоянно проводить мониторинг новостей и технологий в области информационной безопасности.

Когда рядовой пользователь регистрируется на сайте, не задумываясь о своей безопасности, и выдумывает такой пароль, который можно вспомнить, это может закончиться не очень хорошо. Другое дело, в случае если юзер не сохраняет на своем компьютере или на email никакой ценной для него информации (важные документы, личные контакты, номера банковских карт, счетов и т.п.), а другое дело, если бесценная информация может попасть в руки злоумышленников. В список наиболее часто используемых паролей на 2017 год входят: дата рождения, имя возлюбленного, qwerty, 123456789, 111111, zxcvbnm, имя питомца и многие другие.

При переходе по ссылкам на неизвестные сайты и сайты реклам, которые могут нанести угрозу ПК, пользователь может «заразиться» вредоносной программой или вирусом (например: троян, зомби, червь, программы - блокировщики), которые антивирус будет не в силах устранить. Самыми новейшими считаются вирусы электронной почты. Данный вирус распространялся среди вордовских документов отправленных по электронной почте. Принцип работы таков: кто-то создавал вирус как вордовский документ, загруженный в интернет. Любой пользователь, скачавший этот документ и открывший его, сразу же запускал тем самым это вирус. Затем вирус рассылал этот документ и самого себя в электронном сообщении первым 50 контактам адресной книги. Это письмо содержало информацию, которая казалась обычной, включала имя отправителя, и адресат не мог и предположить, что письмо окажется вредоносным. Затем данный вирус создавал ещё 50 сообщений, которые отправлялись теперь с компьютера этого пользователя. И в результате, данный вирус был признан самым быстро распространяющимся. И, как было упомянуто ранее, это заставило многие крупные компании отключить их серверы электронных сообщений.

С 2012 года масштабы хакерских атак резко возросли. К примеру, 12 мая 2017 года во второй половине дня произошла весьма масштабная хакерская атака, «зацепившая» более 65 стран. Под ударом оказались десятки британских клиник; ряд крупных компаний, банк Santander и отделение консалтинговой компании KPMG. В Российской Федерации факт атаки не опровергли и в «Мегафоне» и в Министерстве Внутренних дел. Кроме этого, в прессе осветили информацию о заражении компьютеров Следственного комитета. Вирус-вымогатель WannaCrypt представляет собой что-то вроде вредоносного программного обеспечения, которое блокирует зараженные устройства и требует выкуп в биткоинах [5].

Symantec зафиксировала рост на 55% целевых атак, за 2015 год было выявлено 1305 таких инцидентов, из них 11% — против госструктур, 13% — против любых сервисов. Для проведения данных вмешательств использовались тактика создания сайта «двойника», в точности копирующего настоящий сайт [6].

Обстановка в сфере информационной безопасности в России на сегодняшний день оставляет желать лучшего. В первой половине 2017 года Россия заняла 6-е место по числу кибер-атак, произошедших на территории РФ. Исходя из этих данных, знатоки делают вывод, что Россия занимает одно из ведущих мест в рейтинге стран, граждане которых подвержены наибольшему риску заражения и взлома компьютера через Интернет.

За историю существования ПК было выявлено множество хакеров, один из таких [3]: Загадочный британский 16-летний подросток под псевдонимом “Cracka”. Он взломал базу данных директора ЦРУ. У него получилось выкрасть персональную переписку директора ЦРУ, главы ФБР и директора Национальной разведки США.

В результате выходит, что, так как пользователи не заботятся о своей безопасности, киберпреступникам не составляет труда взломать персональный компьютер и вытянуть оттуда нужную ему информацию. А всё это потому, что в последнее время локальная сеть проникает во все сферы деятельности нашей планеты и всё большее количество людей пользуется платёжными системами.

В завершение, важно заметить: для того чтобы не стать жертвой киберпреступника, достаточно соблюдать наипростейшие правила безопасности при использовании компьютера.

Список литературы / References

1. [Электронный ресурс]. Режим доступа: http://about-windows.ru/virusy-i-xakery/xakery/kto-takoj-belyj-xaker-i-kto-takoj-chernyj-xaker/ (дата обращения: 13.09.2017).
2. [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Хакер/ (дата обращения: 13.09.2017).
3. [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/panda/blog/280091/ (дата обращения: 14.09.2017).
4. [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/ (дата обращения: 14.09.2017).
5. [Электронный ресурс]. Режим доступа: https://esquire.ru/hacker-attack (дата обращения: 14.09.2017).
6. [Электронный ресурс]. Режим доступа: https://www.symantec.com/ru/ru/security_response/publications/threatreport.jsp/ (дата обращения: 13.09.2017).