Секция «Информационное общество, цифровая экономика и информационная безопасность»

Роль эффективной парольной защиты в условиях цифровой трансформации

Научный руководитель – Бритвина Валентина Валентиновна

Шабайкина А.А.[1], *Усоева А.С.*[2]

1 - Московский политехнический университет, Москва, Россия, *E-mail: shabbaykina@mail.ru*; 2 - Московский политехнический университет, Москва, Россия, *E-mail: alyonausus@gmail.com*

- Безопасность личных данных в сети является актуальной проблемой, а кибератаки и киберпреступления приобретают все более и более серьезный характер и несут за собой глобальные последствия.

  По статистике, около 90% цифровых ограблений и кибератак приходится на рядовых пользователей, 9,9% - целевые атаки, т.е. атаки, нацеленные на конкретных людей и организаций и 0,1% - остальные типы (рис.1). Безопасность личных данных должна являться приоритетной задачей для всех владельцев ПО.

  Рис 1. Распределение цифровых ограблений

  Цель исследования: разработать практические рекомендации по обеспечению надежности парольной защиты и веб-сайт по подбору эффективных комбинаций

  Задачи исследования:

  1) Рассмотреть крупнейшие цифровые атаки в мировой истории интернета

  2) Разработать программный продукт, содержащий практические рекомендации по генерации эффективных парольных комбинаций

  Результаты исследования:

  1. КРУПНЕЙШИЕ ЦИФРОВЫЕ АТАКИ В МИРОВОЙ ИСТОРИИ ИНТЕРНЕТА

  Сегодня в сети ведется настоящая цифровая война. Мы увеличиваем защиту, а мошенники придумывают все более изощренные способы ее обойти. Каждый десятый аккаунт можно взломать простым перебором паролей, а каждый пятый пользователь использует один пароль ко всем ресурсам, что значительно упрощает работу злоумышленникам. Далее (на рис. 2) будут рассмотрены крупнейшие кирепреступления в истории Интернета:

  Рис. 2 Хронология киберпреступлений

  Zeus - это троянская программа, которая распространялась в 2007 г. в социальных сетях. Zeus моментально получала доступ к системе компьютера и незамедлительно снимала деньги со счетов европейских банков. Данная кибератака коснулась Италии,

Испании и Германии преимущественно, а суммарный ущерб составил приблизительно 42 мдрд долларов [2].

Следующей мы рассмотрим, вероятно, самую легендарную кибератаку в истории человечества, а именно Stuxnet. Это комплексный вирус, лишивший работоспособности центрифуги, обогащающие уран в Иране, тем самым значительно замедлив иранскую ядерную программу. Stuxnet проявлял себя, когда попадал на вычислительные машины, которые управляли программируемыми контроллерами и софтом Siemens. Именно тогда он назначал недопустимо большие значения скорости вращения центрифуг, благодаря чему они начинали разрушаться.

Dark hotel или «Темный отель» - это кибершпионская сеть преимущественно в азиатских гостиницах. Алгоритм работы Darkhotel представлен на рис.3:

Рис. 3 Алгоритм работы Darkhotel

Далее мы проанализируем компьютерного червя Carbanak, который способен вывести из строя компьютеры банков на ОС Microsoft Windows . Атакующие стремились вывести деньги через банкоматы или онлайн. Алгоритм работы Carbanak представлен ниже на рис.4:

Рис.4 Алгоритм работы Carbanak

По итогу примерно 100 банков из 40 стран попали под удар, а приблизительный урон составляет 1 млрд. долларов. Именно данный вирус относится к немногочисленным целевым атакам повышенной сложности [3].

12 мая 2017 г началась настоящая эпидемия Wannacry - трояна-шифровальщика, ведь более 45 000 случаев атаки было зафиксировано всего лишь за один день. Атакующие разработали вирус, который был способен мгновенно распространяться по сети. За 4 дня WannaCry поразил около 200 000 компьютеров в 150 странах.

Вирус кодирует разные файлы и помещает

- уведомления о заражении и действиях, которые необходимо выполнить, чтобы получить доступ к файлам обратно. Злоумышленники запрашивают некую сумму, после которой якобы расшифруют файлы вашего компьютера. Оказывается, некоторые образцы вируса запрашивали определенный несуществующий домен и, если не получали положительного ответа, устанавливали трояна-шифровальщика. Заражение удалось приостановить, когда данный домен был зарегистрирован.

2. ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ПАРОЛЯ И ПРИНЦИП РАБОТЫ РЕСУРСА ПО ЕГО ГЕНЕРАЦИИ.

Перечисленные ранее методы защиты персональных данных являются надежной гарантией безопасности в сети, но стоит отметь, что важнейшую роль в этом все-таки играют пароли. Пароль является надежным, если соответствует двум основным принципам, а именно:

1. В комбинации использованы как можно более разнообразные символы (что обеспечивает паролю наименьшую предсказуемость)

2. Значительная длина пароля

Стоит также отметить, что эти качества способны компенсировать друг друга: вы можете не использовать символы вида «%», «#», «&» или разные регистры, но сделать ваш пароль длиннее.

Для каждого сервиса или сайта используйте свой уникальный пароль, чтобы не дать злоумышленнику получить вашу конфиденциальную информацию из всех источников сразу.

Надежный пароль совсем не обязательно должен представлять собой случайную комбинацию символов. Несмотря на то, что такие пароли, безусловно, оправданы с точки зрения безопасности, не всегда удается быстро и легко запоминать их. Именно поэтому стоит составить комбинацию, которую просто выучить, но длиннее (12 символов и более). Более того, стоит руководствоваться тем, что пароль может быть сложным на вид, но совершенно простым для взлома и хищения ваших персональных данных.

Кроме того, обезопасить свои данные поможет двухфакторная аутентификация, а точно не забыть придуманные комбинации различные менеджеры паролей [4].

Данные практические рекомендации подробно описаны на разработанном нами сайте.

Сервис содержит в себе информацию проведенного исследования и форму генерации надежной комбинации, алгоритм которой был описан ранее. Принцип работы ресурса предельно прост. Пользователю необходимо вписать в форму фразу, состоящую из 5 слов, выбрать символ, которым он планирует усложнить пароль и указать цвет, ассоциирующийся с тем сервисом, для которого данная комбинация создается. Далее ресурс обрабатывает полученные данные и выводит на экран получившийся пароль. Данные комбинации легко запомнить, а главное, сложно взломать, ведь даже зная алгоритм, хакер не сможет понять, какие именно слова и символы были выбраны пользователем.

Рис. 5 (Разработанный продукт)

ВЫВОД

Таким образом, на основание полученных знаний, можно сделать вывод о том, что сохранить свои данные может каждый, а цифровая грамотность - важный элемент современного общества. Разработанный ресурс поможет наглядно описать принцип работы приведенного алгоритма. Придерживаясь этих несложных правил, мы способны не только сохранить конфиденциальную информацию, но и не стать жертвой злоумышленников, использующих вычислительные машины рядовых пользователей

как оружие при атаке на крупные организации.

-

Источники и литература

1) Статья «Кибератаки» [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru
2) Селютина Е.П. Безопасность онлайн-платежей и личных данных в интернете. В сборнике: Информационное пространство в аспекте гуманитарных и технических наук - 2015Материалы IV междисциплинарной межвузовской конференции студентов, магистрантов и аспирантов. 2015. С. 56-61.
3) Зайцев В.А., Пономарёва Н.А. Кибербезопасность как неотъемлемая часть защиты информации в кредитных организациях. Вестник Хабаровского государственного университета экономики и права. 2015. № 3. С. 74-78.
4) Ошибочное понимание ИТ-безопасности: пароли [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/

Иллюстрации

Рис 1. Распределение цифровых ограблений

Рис. 1. Рис 1. Распределение цифровых ограблений

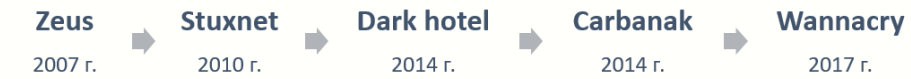


Рис. 2 Хронология киберпреступлений

Рис. 2. Рис. 2 Хронология киберпреступлений

Рис. 3 Алгоритм работы Darkhotel

Рис. 3. Рис. 3 Алгоритм работы Darkhotel

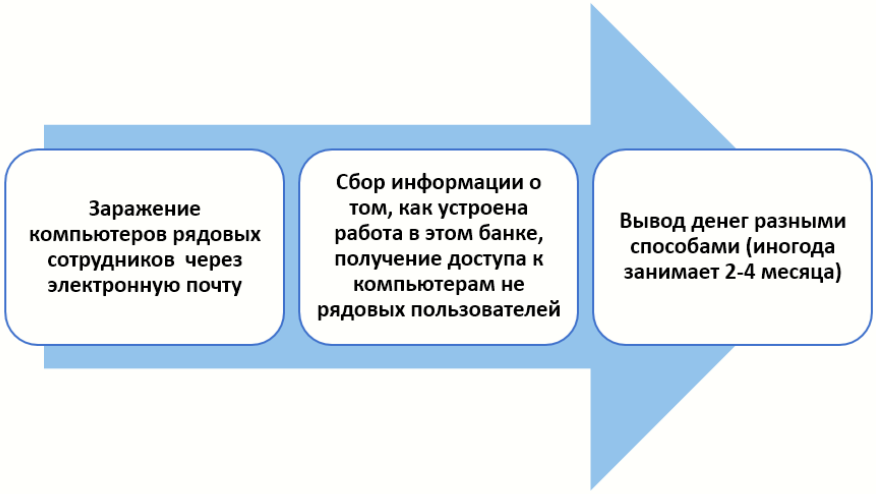
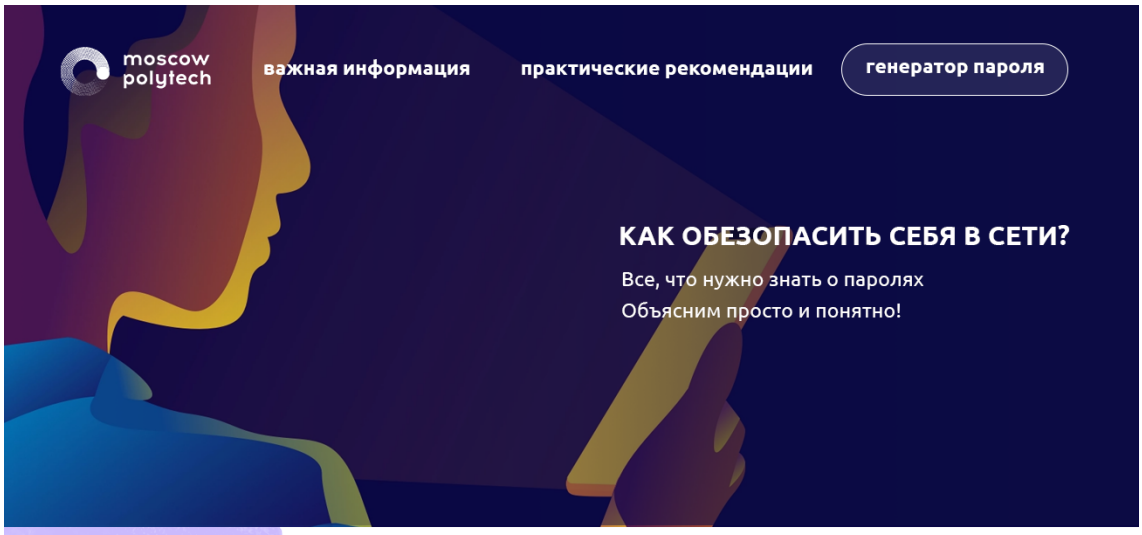


Рис.4 Алгоритм работы Carbanak

Рис. 4. Рис.4 Алгоритм работы Carbanak



ПОЧЕМУ ПАРОЛЬНАЯ ЗАЩИТА ТАК ВАЖНА?

Со времен изобретения Интернета мир сильно изменился. Сейчас, чтобы записаться в поликлинику, заполнить документы или просто договориться о встрече, достаточно нажать пару клавиш и отправить данные в глобальную сеть. Почти каждый из нас имеет **цифровые следы**, которые успешно используются злоумышленниками. За последние 50 лет мы придумали множество способов обеспечить **безопасность персональных данных**: от паролей до криптографических ключей.

К сожалению, способности хакеров так же не стоят на месте. Сегодня в сети ведется настоящая **цифровая война**. Мы увеличиваем защиту, а мошенники придумывают все более изощренные способы ее обойти.

Каждый **десятый аккаунт** можно взломать простым перебором паролей, а каждый пятый пользователь использует **один пароль ко всем ресурсам**, что значительно упрощает работу злоумышленникам. Подобная халатность со стороны пользователей и организаций способна привести к глобальным последствиям

КАКОЙ ПАРОЛЬ СЧИТАЕТСЯ НАДЕЖНЫМ?

Пароль является надежным, если соответствует двум основным принципам, а именно:

В комбинации использованы как можно более разнообразные символы (что обеспечивает паролю **наименьшую предсказуемость**)

Значительная длина пароля (**12 символов** и более)

Для каждого сервиса или сайта используйте свой **уникальный пароль**, чтобы не дать злоумышленнику получить вашу конфиденциальную информацию из всех источников сразу.

Надежный пароль совсем не обязательно должен представлять собой случайную комбинацию символов. Несмотря на то, что такие пароли, безусловно, оправданы с точки зрения безопасности, не всегда удается быстро и легко запоминать их. Именно поэтому стоит составить комбинацию, которую **просто выучить**, но длиннее.

Более того, стоит руководствоваться тем, что пароль