Get a PDF

В связи с нарастающей международной напряжённостью...

...дам-ка я несколько простеньких советов по гражданской обороне в условиях электронной войны. Вдруг кому полезно будет.

Начать следует с того, что современные системы дырявы насквозь. Все. Вне зависимости от операционной системы, браузера и архитектуры. Ну то есть разница в количестве багов между конкретными продуктами имеется и может составлять и два и пять раз. Но важно ли, идёт ли речь о 100 или 300 дырах? С практической точки зрения это уже не имеет особого значения.

Как так получилось? Исторически пользовательский софт в первую очередь ориентировался на скорость и удобство. Не на безопасность. А это такая же разница, как между BMW и БТР. BMW недурно защитит Вас от дождя, града, попытки угона и даже хулиганского камня. Но обыкновенным пулемётом он прошивается насквозь в любом месте, хоть из угла в угол и по диагонали.

То же и с пользовательскими системами. Что клиентскими, что облачными. Они могут неплохо защищать от атак оборзевшего соседа и даже корпоративного шпионажа. Но любой military grade fuzzer разорвёт их в клочья. И я уверен, что у большинства государств должны быть в запасе готовые и взведённые для запуска эксплойты против любой сколько-нибудь распространённой ОСи или браузера. С разными боеголовками, от “жучков” для кражи информации до самораспространяющихся червей, форматирующих диски. Stuxnet (http://en.wikipedia.org/wiki/Stuxnet) всем в помощь как один из (очень немногих) доступных для изучения примеров.

В таких условиях достаточно одному дураку нажать на кнопку, чтобы в инфраструктуре современного мира разом легло очень многое. Интернет. Телефоны (кроме старых некомпьютеризированных АТС). Банки. Госпитали. Управление транспортом, логистика. Корпоративные компьютеры и базы данных. Да, всё это можно восстановить за неделю, но хаоса и бардака за это время случиться может о-очень много. Поэтому лучше к нему быть минимально подготовленным.

Китай, например, это явно осознаёт. Подробности нам никто не расскажет, но со стороны выглядит так, что там готовы в любой момент отрубить себя от мировой сети, если в ней начнётся война, и полностью переключиться на внутренние заменители всех систем коммуникации и контроля. Россия, похоже, тоже пытается построить нечто подобное.

Ну а что делать нам, индивидуальным пользователям, не обладающими знаниями хакеров и ресурсами государственных спецслужб? Не претендуя на полноту охвата вопроса, я составил самый минимальный список рекомендаций, следование которым, надеюсь, поможет легче пережить электронную войну, если она вдруг случится.

Итак:

1. Запасные копии.

Люди делятся на две категории: тех, кто никогда не терял своих данных, и тех, кто их бэкапит. Если у Вас нет запасной копии своих данных – сделайте её прямо сейчас. В Вашем распоряжении множество вариантов, примерно в порядке возрастания сложности:

А. Послать важные файлы самому себе электронной почтой. Можно ежедневно. Дёшево и сердито, много так не убережёшь. Зато просто и быстро. Особенно если Вы вот прямо сейчас работаете над чем-то

важным (диплом, научная работа, книга, презентация), то вообще идеальный вариант.

Б. Скопировать на флэшку. Все Ваши фотки, конечно, туда не влезут. Но уж пара гигабайт самого важного точно поместится. Ну и вообще флэшку носить с собой полезно, мало ли где что нужно бывает перехватить.

В. Купить внешний USB-диск и регулярно на него всё заливать. Более продвинутая версия: делать это с помощью xcopy, чтобы обновлялись только новые или изменённые файлы. Ещё более продвинутая: воспользоваться готовым софтом для бэкапа, от встроенных возможностей Windows до множества предлагаемых платных и бесплатных решений (https://www.google.com/?gws_rd=ssl#q=backup+software).

Г. То же самое – но в облако. Google Drive, Microsoft One Drive, DropBox, Amazon Glacier, и прочие (http://www.thetop10bestonlinebackup.com/cloud-storage). Список плюсов и минусов этого решения я на три страницы развернуть могу, но не стану. А упоминаю лишь потому, чтобы закрыть вопрос.

Д. То же самое – но на другой компьютер дома. Как ни странно, этот вариант менее надёжен. Почему? Выключенный диск, пассивно лежащий на полочке вне дома, вряд ли сможет атаковать какая-нибудь зараза. А вот домашний комп, известно где физически расположенный, постоянно работающий и подключённый к сети, вполне может пасть жертвой внезапной атаки.

2. Развод сервисов.

Вот есть у Вас аккаунты в полусотне мест, от Фейсбука до Вашего банка. И все-все они завязаны на один-единственный электронный адрес. На котором же сидит и Ваша персональная переписка. Что случится, если этот адрес взломают? Правильно. Следующим ходом, скорее всего, грохнут и все Ваши сервисы. Одним движением.

[Кстати, увод данных в облака вообще мало что меняет. Да, облачные системы защищены лучше. Но их взлом бьёт не по одному пользователю, а сразу по миллионам. Математическое ожидание убытков примерно то же.]

Конечно, сейчас много где поддерживают двухфакторную аутентикацию, и если есть возможность, её стоит включить. Хотя лично я к этой мере отношусь с подозрением. Закручена она зачастую так, что ломает рабочий порядок, и при этом всё равно обходится голимым Social Engineering-ом. Но если есть, пусть будет.

Главное – другое. Главное, не складывайте все яйца в одну корзину. Заведите как минимум три электронных адреса. Один для банка и финансовых дел. И по возможности только для них, чтобы никто больше даже не в курсе был, что этот адрес существует. Второй – для личной переписки с друзьями. И только для этого. И, наконец, парочку бросовых для ЖЖ и прочих вконтактиков, которые, во-первых, в других контекстах стараться не светить, а, во-вторых, если что и выкинуть не жалко. А для борьбы с автоматическими спамерами (но, увы, не с хакерами) пригодятся email aliases (https://support.google.com/mail/answer/12096?hl=en). В gmail, например, можно использовать vasya_pupkin+bank@gmail.com для банка и vasya_pupkin+junk@gmail.com для рассылок, все письма будут приходить на vasya_pupkin@gmail.com, но залогиниться как 'vasya_pupkin+bank' нельзя.

Чем больше разных адресов – тем лучше. В идеале, вообще было бы здорово создавать по уникальному адресу на каждый сервис. Но, учитывая, что большинству людей и полудюжину-то паролей трудно упомнить, фиг с ним, пусть будет хотя бы три.

3. Пароли!

Ох, сколько же на эту тему “сказано, нарисовано, сплясано и спето”! Всю эту (без сомнения, полезную) бесконечность я попытаюсь, безмерно упрощая, сжать до четырёх материальных точек:

1. Все пароли из букв и цифр длиной менее 9 символов сегодня взламываются простым перебором. Да, с поправкой на необходимость непрерывного взлома (а не пять попыток через браузер), но в каких случаях можно дать надёжную гарантию отсутствия такой возможности? Вот именно.

2. Пароли из слова, комбинаций двух слов, слова и цифры, слов с 1-2 буквами, замененными на хитрые значки и закорючки, вполне неплохо взламываются современными методами, основанными на словарях (http://reusablesec.blogspot.com/2010/01/analysis-of-10k-hotmail-passwords-part.html). С той же поправкой, что и выше, которая, в общем, несущественна.

3. Миллион (или там что-то около того) самых распространённых паролей, используемых людьми, давно известен. Если Ваш пароль – abcd1234, то время его жизни может не составить и нескольких секунд. (https://xato.net/passwords/more-top-worst-passwords/)

4. Автоматические менеджеры паролей, конечно, жизнь облегчают, но обладают двумя неустранимыми и, на мой взгляд, фатальными недостатками.

Во-первых, без них Вы никто. Если Вам вот прямо сейчас надо куда-то залогиниться, а менежера нет, и установить его нельзя, то Вы просто конкретно попали. Это раз.

Два – без Вас менеджеры всё. Они знают *все* Ваши пароли. Если компьютер, где стоит такой менеджер, успешно атакуют, то *все* Ваши пароли утекут нафиг через несколько минут. Чего Вы, возможно, даже и не заметите.

Да, мне тут сейчас напомнят про Master Password, про хранение в облаке, про throttling, про сверение с UI, про TFA, но все эти механизмы вторичны, потому что любой Password Manager *принципиально* сделан так, чтобы успешно заменять Вас в 98% случаев необходимости ввода пароля. А значит, его и можно использовать *вместо* Вас в 98% случаев. Ибо если не заменяет, то кому он вообще такой нужен?

Хорошо, ясно, что всё плохо, но делать-то что? Как быть с паролями?

Вариантов много. Я поделюсь лишь одним, не самым продвинутым и сильным, зато простым, как три копейки.

Для начала заметим, что фраза “В девяносто седьмом году я напился пива с незнакомым гитаристом в поезде” – уже куда лучший пароль, чем всякие Hts8753fnn#$. Почему?

а. Её легко запомнить. Особенно если это Ваш реальный жизненный факт.

б. Для неё легко сформулировать подсказку.

в. При этом знаете её только Вы. И это не цитата, которую можно найти в поисковике.

г. Хрен её подберёшь грубой силой.

е. И по словарю хрен. Даже если Ваш словарный запас – несчастных 2000 единиц, из него можно слепить 10^33 паролей по 10 слов каждый. Ну, на самом деле, конечно, меньше, ибо корелляция в предложениях высока. После “напился” с куда большей вероятностью следует “пива”, нежели “телефона”. Но вариантов для перебора остаётся всё равно очень много, и, если надо, легко сделать ещё больше.

Это, в принципе, всё. Но для полноты картины добавим несколько штрихов:

1. Менять такие большие пароли каждый месяц не нужно. Можно раз в пару лет. Или если есть подозрения в утечке.

2. Но важно уделять отчётливое, пристальное внимание порядку слов. Потерялся порядок – потерялся пароль.

3. Их легко прятать. Кто догадается, что невнятная фраза на 27-й странице дневника – именно пароль? Особенно если для надёжности пара слов из него всё-таки оставлены в уме? :))

4. Если система требует цифр и процентов – пишите “2 пива” и не забывайте про знаки препинания, которые! для ? крас:оты можно, ставить; вооб!!ще -- от .ба,лды "где, ,захочешь

5. А если система дебильна и, например, умирает на строке длиннее 16 символов, то просто сократите. “Вдсгянпснгвп”. Даже такой кургузый паролишко уже не очень-то легко взломать.

6. В более общем виде полезно иметь свой собственный, личный способ отображать пароли-предложения в пароли-монстры вроде qZ!813-i_#dvY`. Особенно если Вы уверенно производите символьно-цифровые преобразования в уме и без труда запоминаете, например, номера букв английского алфавита.

7. И главное. По возможности, вообще избегайте заведения аккаунтов везде, где этого можно избежать. Вот, скажем, при покупке билета на паром от меня требуют зарегистрироваться. На хрена? Ответ: ни для каких полезных **мне** целей это не нужно. Ценной информации на сайте не хранится. И поэтому, что бы там хозяин бизнеса про себя не думал, все его пожелания идут в топку. **Мне** это не нужно? Нет. Конец разговора. В подобной ситуации либо не регистрируетесь вообще (если доступно). Либо даёте одноразовый электронный адрес (https://www.google.com/?gws_rd=ssl#q=disposable%20email), “регистрируясь” заново хоть при каждом посещении сайта. Либо при каждом возврате забываете пароль и требуете его восстановления. А что? Какой вопрос, такой и ответ.

4. Жизнь без внешних систем.

Предположим, завтра вдруг одновременно отключились на целую неделю:

1. Ваш домашний компьютер.
2. И рабочий тоже.
3. И сотовые телефоны.
4. GPS.
5. А Интернет, где-то, может, местами и сохранился, но по модему и где его искать, всё равно непонятно.

Вопрос: сможете ли Вы это пережить?

Помните ли вы адреса и дорогу до Ваших основных друзей, доктора, полиции, ключевых бизнесов? Или всё давно уже только по GPS? Умеете ли Вы пользоваться бумажной картой? Может ли Ваш бизнес пережить (пусть с убытками, но хотя бы пережить, не обанкротиться и не вылететь в трубу) неделю отсутствия связи с партнёрами, поставщиками, клиентами? Есть ли телефонные номера Ваших друзей и доктора где-либо, кроме памяти Вашего телефона? Как Вы им позвоните, когда связь восстановится? Есть ли дома запас наличности на неделю пусть по самому экономному варианту? Помимо Фейсбука, какие ещё каналы связи имеются с важными Вам людьми?

Проведите эксперимент. Попробуйте прожить несколько дней без компьютера и телефона вообще. Это может оказаться довольно поучительно. Где-то что-то рвётся? Какие-то вещи вдруг оказываются неожиданно невозможными? Вот их и надо укрепить. Заранее.

5. Шифрование

Это уже, скорее, продвинутая тема. По-хорошему здесь бы целую главу надо. Ограничусь кратким:

1. Bitlocker
2. TrueCrypt

Если у Вас есть действительно ценные данные – храните их под вышеназванными крышками.

6. Под колпаком

Важно понимать, что безопасности в идеальном смысле не существует. Компьютеры и браузеры взламываются. Сети (даже таких гигантов, как Гугл) инфильтруются. Криптографические алгоритмы устаревают или обходятся. Единственной гарантией сохранности и конфиденциальности информации в наши дни является её... малозаметность. Никто не станет тратить усиленное внимание и процессорные мощности на разбор писем Васи Пупкина, планирующего отпуск с супругой.

Но, чатясь в интернете или пересылая деловые письма, всегда лучше в уме предполагать, что Ваши сообщения читают. Пусть не сегодня, так через три года. И если цена Вашей информации – десяток миллионов, 10% рынка или 10 лет за решёткой, то лучше **вообще** не доверять её компьютерам и сетям. Не пишите. Встретьте нужного человека лично, и персонально сообщите ему всё, что хотите сообщить. Оно так, кстати, ещё и доходчивее получится.

Спасибо за внимание. А Ване Медведеву – отдельное спасибо за вычитывание и ценные комментарии.

21.10.2014

===

Text Author(s): Eugene Bobukh === Web is volatile. Files are permanent. **Get a copy:** [PDF] [Zipped HTML] === **Full list of texts:** http://tung-sten.no-ip.com/Shelf/All.htm] === **All texts as a Zip archive:** http://tung-sten.no-ip.com/Shelf/All.zip] [mirror: https://1drv.ms/u/s!AhyC4Qz62r5BhO9Xopn1yxWMsxtaOQ?e=b1KSiI] === **Contact the author:** h o t m a i l (switch name and domain) e u g e n e b o (dot) c o m === **Support the author:** 1. **PayPal** to the address above; 2. **BTC**: 1DAptzi8J5qCaM45DueYXmAuiyGPG3pLbT; 3. **ETH**: 0xbDf6F8969674D05cb46ec75397a4F3B8581d8491; 4. **LTC**: LKtdnrau7Eb8wbRERasvJst6qGvTDPbHcN; 5. **XRP**: ranvPv13zqmUsQPgazwKkWCEaYecjYxN7z === **Visit other outlets:** Telegram channel http://t.me/eugeneboList, my site www.bobukh.com, Habr https://habr.com/ru/users/eugeneb0/posts/, Medium https://eugenebo.medium.com/, Wordpress http://eugenebo.wordpress.com/, LinkedIn https://www.linkedin.com/in/eugenebo, ЖЖ https://eugenebo.livejournal.com, Facebook https://www.facebook.com/EugeneBo, SteemIt https://steemit.com/@eugenebo, MSDN Blog https://docs.microsoft.com/en-us/archive/blogs/eugene_bobukh/ === **License**: Creative Commons BY-NC (no commercial use, retain this footer and attribute the author; otherwise, use as you want); === **RSA Public Key Token:** 33eda1770f509534. === **Contact info** relevant as of 7/15/2022.

===