Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Меня взломали, что делать?

Обзор

Известно, что большинство людей заботятся о безопасности своего компьютера и сохранности информации. Однако ситуация аналогична вождению автомобиля: как бы аккуратно вы не ездили, рано или поздно вы все равно попадёте в аварию. В этом выпуске мы расскажем, как определить взломан ли компьютер, и что делать, если это произошло. В конечном счёте, чем быстрее вы обнаружите, что это произошло, и чем раньше предпримите меры по защите, тем меньший вред будет причинён вам или вашей компании.

Автор выпуска

Джейк Уильямс (@MalwareJake; malwarejake.blogspot.com) – Старший научный консультант в CSRgroup Computer Security Consultants. Джейк также является соавтором курсов SANS Memory Forensics (FOR526) и Malware Reverse Engineering (FOR610).

Признаки того, что компьютер взломали

Прежде всего, нужно понимать, что нет какого-то конкретного признака того, что компьютер взломан. Как правило, их несколько. Если вы обнаружили комбинацию признаков, то это означает, что ваш компьютер взломали. Вот некоторые из них.

- Ваш антивирус сообщает, что обнаружен вирус, в частности, если сообщается, что заражённый файл невозможно удалить или поместить в карантин
- Домашние страницы браузера изменились, и вы попадаете совсем на другие сайты, не на те, которые хотели
- Появились новые аккаунты, которые вы не создавали
- Запускаются новые программы, которые вы не устанавливали
- Ваш компьютер постоянно сообщает о сбое или запускается очень медленно
- Программы на вашем компьютере запрашивают разрешение на изменения, несмотря на то, что вы ничего не устанавливали и не обновляли
- Ваш браузер сообщает о неизвестной программе, которая запрашивает доступ в Интернет

Меня взломали, что делать?

Какие меры предпринять

Как только вы поняли, что ваш компьютер взломали, действовать нужно незамедлительно. Если компьютер служебный, не пытайтесь ничего делать самостоятельно и не выключайте его. Иначе вы причините больше вреда, чем пользы и помешаете расследованию инцидента. Вместо этого сразу же сообщите вашему работодателю, например, обратитесь в Службу Поддержки, Службу Безопасности или непосредственно к руководителю.

Рано или поздно ваш компьютер может быть взломан. Чем быстрей вы это обнаружите и примите меры, тем лучше.

Если по какой-то причине это сделать невозможно или нескоро, то просто отключите компьютер от Интернет сети, а затем включите «спящий» режим. Даже если вы до конца не уверены, был ли ваш компьютер взломан, всё равно стоит сообщить о своих подозрениях в офис. Скорее всего, команда, отвечающая за безопасность, сталкивалась с подобными ситуациями и сможет во всем разобраться.

Если вы пользуетесь компьютером в личных целях, то следуйте следующим инструкциям:

- **Резервная копия**. Самое важное, что вы можете сделать – это создать резервные копии. Резервные копии необходимо делать регулярно, тогда вы всегда сможете восстановить все файлы. Очень часто при взломе компьютера уничтожается жёсткий диск, в этом случае приходится устанавливать новую операционную систему или покупать новый компьютер. Вот для чего нужны резервные копии.
- **Смена паролей**. Убедитесь, что поменяли все пароли. Подразумевается смена не только паролей компьютера или мобильных устройств, но и всех онлайн паролей. Менять пароли следует с другого, надёжного и безопасного компьютера.
- **Антивирусные программы**. Если ваш антивирус сообщает о зараженном файле, следуйте инструкциям программы. Обычно этот файл нужно поместить в карантин, затем обезвредить или удалить. Большинство антивирусных программ предоставят ссылки, по которым вы сможете узнать больше о конкретном вирусе. При любых сомнениях отправляйте файл в карантин; если это невозможно, просто удалите его.

Меня взломали, что делать?

- **Переустановка**. Если вы не можете очистить компьютер с помощью антивируса, то самым безопасным способом будет переустановка системы. Прежде всего, отключите компьютер от сети Интернет. Далее следуйте инструкциям производителя вашей системы: как правило, есть встроенная функция переустановки. Если эта функция отсутствует, повреждена или заражена, то следует запросить у производителя DVD с программой переустановки. Не переустанавливайте систему из резервных копий. Ваши копии могут содержать подобные уязвимости, которые изначально позволили хакерам получить доступ к системе. Резервные копии следует использовать только для восстановления личных данных. Если компьютер устаревший, то может быть проще (в некоторых случаях и дешевле) купить новый, чем долго переустанавливать систему.
- **Профессиональная помощь**. Если вы думаете, что ваш компьютер взломали, но сами не знаете что и как делать, то можно обратиться к профессионалам. Например, после взлома вы обнаружили, что ваши резервные копии неполные или устаревшие. Вам нужно перенести файлы, например, документы, фото, видео, с заражённого компьютера на новый. Вместе с этим вы можете перенести на новый компьютер и вредоносные программы. Более безопасной альтернативой являются услуги профессионалов, которые помогут безопасно восстановить нужные файлы без риска инфицирования.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Ресурсы

OUCH! Резервное копирование и восстановление:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Пароли:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Что такое вредоносные программы:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 3.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова