Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

Программы-вымогатели

Что такое программы-вымогатели

Программы-вымогатели – это особый тип вредоносных программ, который активно распространяется в Интернете в наши дни. Эти программы способны уничтожить документы и другие файлы пользователей. Популярность программ-вымогателей обусловлена большой выгодой для злоумышленников. В случае заражения компьютера программой-вымогателем, зашифровываются все файлы или даже весь жесткий диск. В этом случае у вас не будет доступа к системе или некоторым важным документам, фотографиям. Вирус вам сообщит, что для расшифровки данных нужно заплатить выкуп (вот почему они так называются). В большинстве случаев оплату требуют производить в особой электронной валюте, например, Биткойн. Программы-вымогатели распространяются как и большинство других вирусов. Чаще всего их рассылают по электронной почте, обманным путем вынуждая жертву открыть инфицированное вложение или перейти по ссылке на вредоносный сайт.

Об авторе

Ленни Зельцер обеспечивает информационную безопасность клиентов компании NCR Corp. Он также преподает в Институте SANS курс борьбы с вредоносными программами. Ленни ведет записи в Twitter **@lennyzeltser** и ведет блог по информационной безопасности **zeltser.com**.

Нужно ли платить выкуп программам-вымогателям?

Это очень сложный вопрос. Проблема в том, что чем больше людей платят выкуп, тем больше злоумышленники заинтересованы инфицировать других. Но с другой стороны, у людей нет другой возможности восстановить данные. В любом случае следует знать, что оплата выкупа совсем не гарантирует восстановление доступа к файлам. Ведь вы имеете дело с преступниками, они могут не расшифровать файлы, или попросить дополнительной оплаты за расшифровку данных, расшифровка может произойти неверно или вам установят новую вредоносную программу на компьютер.

Резервная копия

Пожалуй, единственным способом решения проблемы без уплаты выкупа является восстановление данных из резервной копии. В этом случае, даже при заражении компьютера программой-вымогателем, вы сможете

Программы-вымогатели

восстановить данные после переустановки системы или очистки от вирусов. Помните, что в случае заражения системы программой-вымогателем, ваши резервные копии тоже могут оказаться удалёнными или зашифрованными. Поэтому хранить резервные копии следует на «облаке» или съемных носителях, которые не подключены все время к компьютеру. Распространённой ошибкой является то, что многие люди не тестируют резервную копию, в некоторых случаях с неё нельзя восстановить данные. Регулярно проверяйте резервную копию на возможность восстановления данных. Резервные копии помогут не только при заражении вирусом-вымогателем, но и при случайном удалении файлов или поломке жёсткого диска.

при заражении компьютера программами-вымогателями все ваши файлы будут зашифрованы, и доступ к ним будет закрыт.

Способы защиты

Защититься от программ-вымогателей можно таким же способом, как и от остальных вирусов: предупредить заражение компьютера. Убедитесь, что у вас установлены и регулярно обновляются антивирусные программы от надёжных производителей. Эти программы помогают предотвратить установку или удаляют большинство вирусов. Однако, антивирусы не могут заблокировать или удалить все зловредные программы. Злоумышленники постоянно совершенствуют вредоносные программы, что вынуждает производителей антивирусов регулярно обновлять свои продукты и улучшать возможности обнаружения вирусов. Это напоминает гонку вооружений, в которой каждая из сторон пытается перехитрить другую. К сожалению, плохие парни часто оказываются на шаг впереди, вот почему вам следует делать резервные копии и соблюдать следующее:

- Чаще всего злоумышленники заражают компьютеры, используя уязвимости системы. Чем новее версия системы, тем меньше у нее уязвимостей. Следует использовать самые последние версии операционной системы, приложений, устройств и настроить автоматическое обновление.
- На компьютерах следует использовать аккаунт с ограниченными правами.
- Не следует использовать аккаунт с правами администратора или суперпользователя «root». Это поможет предотвратить установку многих вирусов.

Программы-вымогатели

- Мошенники часто устанавливают вредоносные программы обманным путем. Например, они рассылают электронные письма с инфицированной ссылкой или вложением, которые выглядят очень правдоподобно. Письма могут быть отправлены от имени вашего банка или друга. В случае перехода по ссылке или при открытии вложения активируется код, который заражает ваш компьютер вирусами. Будьте бдительны, если в письме создается ситуация срочности, вам что-то кажется подозрительным, слишком хорошим, чтобы быть правдой или встречаются грамматические ошибки - это может быть атакой. Проявляйте осторожность, здравый смысл является наилучшей защитой.

Проявляйте особую бдительность при переходе по ссылкам, открытии вложений электронной почты, убедитесь, что пользуетесь последней версией антивируса и регулярно его обновляете, регулярно создавайте резервные копии и проверяйте их.

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 securingthehuman.sans.org/ouch/archives.

Ресурсы

Фишинг:	https://securingthehuman.sans.org//ouch/2015#december2015
Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Шифрование:	https://securingthehuman.sans.org/ouch/2016#june2016
Резервное копирование и восстановление данных:	https://securingthehuman.sans.org/ouch/2015#august2015
Статья Microsoft:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
Учебный курс Института SANS FOR610 - Reverse Engineering Malware:	https://sans.org/for610

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

