OUCH! Июль 2020

Ежемесячный информационный бюллетень по безопасности

Программы-вымогатели

Что такое программы-вымогатели?

Программы-вымогатели, это разновидность вредоносного программного обеспечения (вредоносная программа), которая предназначена для удержания ваших файлов или заложников компьютера и требует оплаты за восстановление доступа. Программы-вымогатели стали очень распространенными, потому что они выгодны для преступников.

Как и большинство вредоносных программ, вымогатели начинают с заражения вашего компьютера, чаще всего, когда вы открываете зараженное вложение или нажимаете на вредоносную ссылку в фишинг-письме. После того, как вымогатель заразил ваш компьютер, он шифрует файлы на вашем жестком диске - возможно, даже на всем жестком диске - или что-либо еще, подключенное к вашему компьютеру, чтобы вы больше не могли получить доступ к вашим файлам. Затем он информирует вас о том, что единственный способ восстановить ваши файлы - это заплатить выкуп злоумышленнику. Иногда преступники если вы не заплатите выкуп, угрожают публично опубликовать ваши файлы. Преступники могут потребовать оплату в виде не отслеживаемой цифровой валюты, такой как биткойн. Если вы заплатите выкуп, преступники могут предоставить вам доступ к вашим файлам, но нет никаких гарантий. Иногда они даже забирают ваши деньги и все равно оставляют ваш компьютер зараженным, не зная об этом, или продолжают просить больше денег.

Защита от заражения

Вы можете защитить свой компьютер от заражения вымогателями так же, как защищаете его от других видов вредоносных программ. Вот три ключевых шага:

- **Обновите свои системы и программное обеспечение**: Киберпреступники часто заражают компьютеры или устройства, используя нефиксированные ошибки (известные как уязвимости) в вашем программном обеспечении. Чем актуальнее ваше программное обеспечение, тем меньше в нем известных уязвимостей и тем труднее киберпреступникам заразить их. Поэтому убедитесь, что в ваших операционных системах, приложениях и устройствах включено автоматическое обновление.

- **Включить антивирус**: Используйте современное антивирусное программное обеспечение от надежного поставщика. Такие инструменты предназначены для обнаружения и остановки вредоносных программ. Однако антивирус не может блокировать или удалять все вредоносные программы, и обычно он не может восстановить ваши файлы после

заражения вымогателями. Киберпреступники постоянно вводят новшества, разрабатывая новые и более сложные тактики заражения, которые могут избежать обнаружения. В свою очередь, антивирусные производители постоянно обновляют свои продукты новыми возможностями для обнаружения вредоносных программ. Во многом это стало гонкой вооружений, когда обе стороны пытаются перехитрить друг друга.

- **Будьте бдительны**: Киберпреступники часто вынуждают людей устанавливать вымогателей и другие вредоносные программы с помощью фишинговых атак по электронной почте. Например, киберпреступник может отправить вам электронное письмо, которое выглядит законным и содержит вложение или ссылку. Возможно, письмо приходит от вашего банка или друга. Однако, если вы откроете вложенный файл или нажмете на ссылку, вы можете активировать вредоносный код, который заражает ваш компьютер. Если сообщение создает сильное чувство срочности или кажется слишком хорошим, чтобы быть правдой, это может быть атака. Будьте бдительны - кибер-атакующие играют на ваших эмоциях. Здравый смысл часто является вашей лучшей защитой.

Сделайте резервную копию ваших файлов до заражения

Поскольку нецелесообразно предполагать, что вы всегда сможете предотвратить заражение, ваша лучшая защита от вымогателей - резервное копирование. Если у вас есть резервная копия важных документов и других файлов, у вас есть возможность восстановления из резервной копии вместо выплаты выкупа. Важно, чтобы вы использовали какой-либо тип автоматического резервного копирования, который регулярно создает резервные копии всех ваших файлов, и что вы тестируете свои процедуры восстановления, чтобы убедиться, что вы можете восстановить их в случае необходимости. Существует множество простых облачных и локальных решений для резервного копирования, которые вы можете установить на свой компьютер, которые будут безопасно и регулярно выполнять резервное копирование всех ваших файлов для вас.

Приглашенный редактор

Ленни Зельцер - директор по связям с общественностью в Axonius, компании по управлению активами в сфере кибербезопасности. Он также преподает борьбу с вредоносными программами и пишет в Институте SANS. Ленни активен в Твиттере как @lennyzeltserи пишет блог безопасности назeltser.com.

Ресурсы

Резервные копии: https://www.sans.org/security-awareness-training/resources/got-backups
Остановить вредоносное ПО: https://www.sans.org/security-awareness-training/resources/stop-phish
Обновление: https://www.sans.org/security-awareness-training/resources/power-updating
Курс SANS FOR610 - вредоносное ПО для обратного проектирования: https://sans.org/for610

Роман Полаков
OUCH! публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. Вы можете поделиться или распространить этот бюллетень, если вы не продаете или не изменяете его. Редакция журнала: Уолт Скривенс, Фил Хоффман, Алан Ваггонер, Шерил Конли