Программы-вымогатели: все, что нужно знать об этом виде угроз

Вы заняты. Вы устали. Вы хотите сыграть в Pokémon Go или открыть страницу в интранет-сети вашей компании. Причина не имеет значения. Щелкая Remind me later (Напомнить позже) в окне с запросом об установке обновлений, вы упрощаете задачу для авторов программ-вымогателей.

Но это лишь один из путей проникновения таких программ в вашу систему. Злоумышленники широко применяют вредоносную рекламу, фишинговые письма и даже сложные схемы на основе USB-накопителей. Рассмотрим подробнее один из самых распространенных сценариев.

Вы щелкаете Remind Me Later

Программное обеспечение несовершенно. Разработчики регулярно обнаруживают ошибки в собственных программах и выпускают соответствующие исправления. Откладывая обновление плагинов и приложений, вы даете злоумышленникам возможность воспользоваться известными уязвимостями. Пример: в 80 % случаев атака с применением одного из известных комплектов эксплойтов оказывалась успешной, поскольку своевременно не были устранены уязвимости Flash. Будь то Flash, Silverlight или Google Chrome, необходимо регулярно устанавливать исправления и обновления.

Ваша система заражается

Оказавшись на вашем устройстве, программа-вымогатель берет под контроль соответствующие системы. Затем программа шифрует ваши файлы с помощью асимметричного алгоритма шифрования. Ваши данные зашифрованы без вашего участия, при этом ключ к шифру есть только у злоумышленника. Некоторые виды программ-вымогателей распространяются по сети самостоятельно. По данным экспертов, способность ПО-агрессора к самораспространению встречается все чаще и чаще.

Отображается сообщение с требованием выкупа

По окончании заражения программа выдаст сообщение с требованием выплатить выкуп в биткоинах. Взамен будет обещано восстановление доступа к данным. Как правило, сумма выкупа составляет от 200 до 10 000 долл. США, однако в некоторых случаях компаниям приходилось терять гораздо большие суммы. Одна из калифорнийских клиник выплатила 17 000 долл. США, чтобы восстановить доступ к данным. При этом каждые сутки клиника теряла около 100 000 долл. США, поскольку работа учреждения была частично парализована.

Эксперты по информационной безопасности не рекомендуют платить выкуп. Некоторые программы-вымогатели не способны корректно разблокировать файлы. Иногда файлы автоматически уничтожаются. По данным исследовательской группы Talos, количество случаев с полным уничтожением файлов постепенно увеличивается. В отчете Cisco по кибербезопасности за первое полугодие 2016 г. затрагивается новая важная проблема, возникшая в связи с масштабной активизацией программ-вымогателей. Речь идет о целостности данных. Злоумышленники не гарантируют целостности и корректного восстановления зашифрованных данных. В частности, искажение медицинских записей или проектной документации может иметь самые серьезные последствия.

Кроме того, выплачивая выкуп, жертва финансирует деятельность преступной организации. Прибыльность этих схем является стимулом к разработке новых, еще более мощных видов программ-вымогателей.

Как защититься от программ-вымогателей

В отношении программ-вымогателей наиболее эффективен многоуровневый подход.

До атаки

Оборону можно укрепить несколькими простыми способами. Мы настоятельно рекомендуем обратиться к поставщику услуг аварийного восстановления, который поможет сохранить работоспособность организации в случае неблагоприятного развития событий. Однако можно действовать и проще. Организуйте регулярное резервное копирование важных данных. Установите средства блокировки рекламы и обязательно обновляйте программное обеспечение при появлении соответствующего запроса.

К сожалению, обычные блокировщики не способны полностью исключить вредоносную рекламу и выявить опасные ссылки. Обратите внимание на продукт Cisco® Umbrella*, установка которого потребует не более пяти минут. Продукт эффективно распознает вредоносные веб-сайты и блокирует запросы на уровне хоста.

Во время атаки

Благодаря Umbrella абсолютное большинство программ-вымогателей будут заблокированы на уровне DNS задолго до попадания на пользовательское устройство. Однако ни один отдельно взятый метод не гарантирует стопроцентно полной защиты от программ-вымогателей.

Необходимы мощные средства мониторинга сетевой активности, которые позволят распознать начавшуюся атаку. Система обнаружения угроз Cisco Stealthwatch™ отслеживает сетевой трафик, выявляя различные аномалии, в том числе и вызванные программами-вымогателями. Обнаружив угрозу, система сообщает о компрометации сети.

* Cisco® Umbrella являтся частью решения Cisco Open DNS, которое будет доступно в России с 2017 года.

© Компания Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

Программы-вымогатели: все, что нужно знать об этом виде угроз

Cisco предлагает мощные средства, блокирующие запуск и функционирование вредоносных файлов.

- Umbrella блокирует запросы, посылаемые вредоносным файлом при попытке сформировать ключ шифрования. Таким образом, программа-вымогатель не сможет получить необходимую информацию для шифрования ваших данных.
- Блокировка запроса силами Umbrella сопровождается дополнительной мерой защиты в виде блокировки соединения как такового, за что отвечает межсетевой экран нового поколения Cisco.
- Если вредоносный файл преодолел защиту на уровне DNS и межсетевой экран, в действие вступает продукт Cisco AMP для оконечных устройств. Заблокировав запуск файла, эта система принимает дополнительные меры безопасности. Производится непрерывный хронологический анализ активности файла в масштабах всей сети, что позволяет найти и удалить все вредоносные файлы.

После атаки

Если в сеть попала программа-вымогатель, необходимо предпринять шаги по минимизации ущерба и предотвратить дальнейшее распространение. Система защиты от сложного вредоносного ПО блокирует запуск известного вредоносного ПО и удаляет соответствующие файлы с оконечных устройств.

Динамическая сегментация на основе технологии Cisco TrustSec® позволяет выделить скомпрометированные участки сети и предотвратить дальнейшее распространение программ-вымогателей.

Хотите узнать больше? Перейдите на страницу cisco.com/go/ransomware.

Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками компании Cisco и/или ее дочерних компаний в США и других странах. Чтобы просмотреть список товарных знаков компании Cisco, перейдите по ссылке www.cisco.com/go/trademarks. Товарные знаки других организаций, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает партнерских взаимоотношений между компанией Cisco и любой другой компанией. (1110R)

C11-737870-00 09/16