Краткий обзор

Cisco Ransomware Defense

Преимущества

- **Минимизация опасности**, исходящей от вымогательского ПО, благодаря эффективной системе защиты, которая способна блокировать угрозы задолго до первой попытки проникновения.
- **Мощная защита в кратчайший срок** – вы сможете сосредоточиться на решении бизнес-задач, не отвлекаясь на проблемы безопасности.
- **Многоуровневая интегрированная структура защиты** обеспечивает беспрецедентную эффективность мониторинга и реагирования – от уровня DNS до сети и оконечных устройств.
- **Динамическая сегментация** позволяет предотвратить распространение вымогательского ПО в сети.
- **Высококачественная аналитика** от группы Cisco Talos, изучающей угрозы безопасности.

Расцвет программ-вымогателей

Программы-вымогатели – вредоносное ПО, которое шифрует информацию (документы, фотографии, музыку) на личном или корпоративном компьютере. И требует выкуп за расшифровку файлов и получение доступа к ним.

Программы-вымогатели быстро превратились в самый прибыльный вид вредоносного ПО в истории. По данным ФБР, ежегодный оборот этой «отрасли» постоянно растет и вскоре достигнет 1 млрд долл. США.

Чаще всего вымогательское ПО проникает на компьютер или в сеть через веб-сайты или электронную почту. На веб-сайтах опасность исходит от зараженных рекламных блоков, именуемых вредоносной рекламой. При посещении веб-сайта, содержащего вредоносную рекламу, возможны автоматическая загрузка вредоносного ПО или перенаправление на страницы с эксплойт-китами. В случае с электронной почтой применяются фишинговые письма и спам. Перейдя по ссылке или открыв вложение из такого письма, пользователь загружает на свое устройство вымогательское ПО, которое сразу же связывается с сервером инфраструктуры контроля и управления.

Также для распространения программ-вымогателей часто применяются эксплойт-киты. Набор эксплойтов представляет собой программный пакет, предназначенный для поиска уязвимостей в программном обеспечении конечных систем. Обнаруженные уязвимости используются для загрузки вредоносного кода, включая программы-вымогатели.

В ближайшем будущем круг потенциальных жертв вымогательского ПО будет расширен – атакам подвергнутся не только отдельные пользователи, но и целые сети. Совершенствуя методы полуавтоматического самораспространения, авторы программ-вымогателей будут использовать все доступные пути для проникновения в сеть и дальнейшего горизонтального перемещения, чтобы взять под контроль крупные сетевые сегменты, увеличив таким образом охват атаки и вероятность выплаты.

Минимизация угрозы, исходящей от вымогательского ПО, за счет более эффективной системы безопасности

Программы-вымогатели способны проникать в сеть самыми различными способами, поэтому проблема требует комплексного подхода – отдельные продукты не обеспечивают нужного уровня защиты. Атаку вымогательского ПО необходимо по возможности предотвратить. Если злоумышленникам все же удалось получить доступ в сеть, необходимо вовремя распознать вторжение, изолировать угрозу и минимизировать ущерб.

В основе решения Cisco® Ransomware Defense лежит архитектура безопасности Cisco, которая обеспечивает надежную защиту корпоративной инфраструктуры, охватывая сети, уровень DNS, электронную почту и оконечные устройства. Благодаря усилиям Cisco Talos, одной из лучших аналитических групп, изучающих угрозы, достигается максимальная эффективность реагирования в случае атаки вымогательского ПО.

«Мы смогли устранить риски, связанные с проникновением программ-вымогателей через Интернет, и заметно повысили удобство работы пользователей, что касается интернет-подключений».

Octapharma

Решение состоит из следующих компонентов.

- **Cisco Umbrella** – защита устройств внутри и вне корпоративной сети. Эта система блокирует DNS-запросы и не дает устройству установить соединение с вредоносными веб-сайтами, где находится вымогательское ПО.
- **Cisco AMP для оконечных устройств** – блокировка запуска программ-вымогателей на оконечных устройствах.
- **Cisco Email Security с AMP** – блокировка спама, фишинговых писем, вредоносных вложений и ссылок. Для решения этих задач применяется та же технология, что и на оконечных устройствах, – Cisco AMP. Однако в этом случае соответствующие средства развертываются на шлюзах электронной почты.
- **Межсетевой экран нового поколения Cisco Firepower** с защитой от сложного вредоносного ПО (AMP) и технологией изоляции Threat Grid – блокировка известных угроз, блокировка обратной связи с инфраструктурой управления и контроля, динамический анализ с целью обнаружения неизвестных угроз и новых видов вредоносного ПО.
- **Cisco ISE на основе сети Cisco** – динамическая сегментация, позволяющая надежно защитить доступ к службам и приложениям, а также предотвратить горизонтальное распространение вымогательского ПО.
- **Услуги Cisco по обеспечению безопасности сети** позволяют незамедлительно определить и устранить причины инцидента. Кроме того, эти услуги помогают оптимизировать развертывание AMP, межсетевого экрана нового поколения и других продуктов в составе данного решения.

Дальнейшие шаги

Решив проблему вымогательского ПО, вы сможете сосредоточить усилия на ключевых бизнес-задачах. Обратитесь к представителю Cisco за подробной информацией о Cisco Ransomware Defense.