Cisco Ransomware Defense: оградите сеть от программ-вымогателей

Существует ли система защиты, способная перекрыть все пути вторжения для программ-вымогателей? Только Cisco предлагает архитектуру и продукты, готовые предоставить такую защиту.

Обзор

Основой рабочих процессов любой организации сегодня является информация, в том числе и в формате файлов. Целостность этой информации — это одно из необходимых условий работоспособности компании.

В систему проникает программа-вымогатель. Она блокирует информацию (документы, фотографии, музыку) на личном или корпоративном устройстве. За разблокировку файлов запрашивается выкуп. При отсутствии адекватных механизмов защиты программа-вымогатель способна полностью парализовать цифровую архитектуру — придется довольствоваться бумагой и ручкой.

Как правило, программы-вымогатели внедряются в систему при помощи эксплойт-китов, вредоносной рекламы (зараженные рекламные блоки на веб-сайте), фишинга (мошеннические электронные письма, выдаваемые за сообщения от доверенных отправителей) и спам-кампаний. Источником заражения может стать вложение или ссылка в фишинговом письме. Опасность также исходит от веб-сайтов с вредоносной рекламой, которая автоматически заражает компьютеры.

Представляем Cisco® Ransomware Defense. Многоуровневый подход позволяет этому решению обеспечивать эффективную защиту от программ-вымогателей. Решение охватывает DNS, оконечные устройства, сеть, электронную почту и веб. Мы предлагаем комплексную защиту на базе подхода, основанного на архитектуре сети, — самый эффективный мониторинг в сочетании с наилучшими средствами реагирования для борьбы с программами-вымогателями.

Преимущества

- **Минимизация угрозы, исходящей от программы-вымогателя,** позволяет сосредоточиться непосредственно на бизнесе.
- **Мощная защита в кратчайший срок** с возможностью блокировки угроз задолго до первой попытки проникновения.
- **Беспрецедентное качество мониторинга и скорость реагирования** благодаря подходу, основанному на архитектуре сети, — от DNS до сети и оконечных устройств.
- **Предотвращение горизонтального распространения вредоносного ПО** благодаря жесткой сегментации сети.
- **Результаты исследований ведущей группы специалистов Talos,** изучающей современные угрозы и программы-вымогатели.

Серьезная угроза, набирающая популярность

Этот год идет под знаком программ-вымогателей. Атаки на его основе приносят немалый доход. Программы-вымогатели в короткий срок превратились в один из самых прибыльных видов вредоносного ПО.

По данным ФБР, годовой оборот этой «отрасли» постоянно растет и вскоре достигнет 1 млрд долл. США. Исследования группы Cisco Talos показали, что отдельно взятая кампания на основе программ-вымогателей может приносить до 60 млн долл. США в год. Проблема программ-вымогателей привлекает огромное внимание и уже обсуждается на телевидении.

Киберпреступники располагают необходимыми денежными ресурсами и работают над «инновационными продуктами», которые будут распространяться еще более эффективно. По нашему мнению, в ближайшем будущем механизмы самораспространения программ-вымогателей будут усовершенствованы. Это означает, что злоумышленники смогут блокировать работу крупных участков корпоративных сетей. В таких случаях доступная ИТ-функциональность корпоративной инфраструктуры будет приблизительно соответствовать уровню 1970-х годов.

В настоящее время для защиты от программ-вымогателей чаще всего применяются разрозненные продукты. Необходим более целостный, архитектурный подход, поскольку мы имеем дело с большим количеством разнообразных векторов заражения.

В этом обзоре решения мы рассматриваем различные векторы и методы, применяемые киберпреступниками. Требуется защита электронной почты и веб-трафика, блокировка доступа к инфраструктуре вредоносного ПО в Интернете, удаление вымогательских программ, которые все-таки проникли на оконечное устройство, блокировка управляющего трафика вредоносного ПО, предотвращение горизонтального распространения программ-вымогателей в случае успешного инфицирования.

Что вы покупаете

Решение объединяет в себе все компоненты архитектуры безопасности Cisco, необходимые для устранения проблемы программ-вымогателей. Вы можете взять полный комплекс или же выбрать отдельные компоненты для решения той или иной конкретной задачи.

Компоненты решения Ransomware Defense

- Cisco Umbrella — блокировка угроз на уровне DNS, т. е. на дальних подступах к сети.
- Cisco AMP для оконечных устройств — блокировка запуска программ-вымогателей на оконечных устройствах.

- Cisco Email Security (облачная и локальная конфигурация) — блокировка фишинговых и спам-сообщений, предназначенных для доставки программ-вымогателей.
- Cisco AMP — этот продукт можно сочетать с продуктами, обеспечивающими безопасность электронной почты. Удобный механизм лицензирования позволяет легко добавить функции статического и динамического анализа (изоляция в «песочнице») неизвестных вложений, проходящих через шлюз защиты электронной почты Cisco.
- Межсетевой экран нового поколения Cisco Firepower™ — блокировка управляющего трафика вредоносного ПО, блокировка любых вредоносных файлов, передаваемых по сети.
- Платформа Cisco ISE — динамическая сегментация посредством сети Cisco во избежание горизонтального распространения программ-вымогателей.

Решение Ransomware Defense позволяет превратить корпоративную сеть в регулятор, препятствующий распространению программ-вымогателей. Даже если злоумышленникам удастся преодолеть защиту и проникнуть в сеть, дальнейшее распространение вредоносной программы будет невозможно.

Услуги Cisco по обеспечению безопасности сети позволяют незамедлительно определить и устранить причины инцидента. Кроме того, они помогают оптимизировать развертывание AMP, межсетевого экрана нового поколения и других продуктов в составе данного решения.

Основные возможности

- Блокировка программ-вымогателей, включая проникновение в сеть извне и загрузку на портативные компьютеры.
- Эффективная изоляция программ-вымогателей в случае успешного инфицирования.

Услуги обеспечения безопасности помогают бороться с программами-вымогателями

Группа специалистов по реагированию на инциденты (входит в состав подразделения, отвечающего за услуги Cisco по обеспечению безопасности сети) помогает обеспечить своевременное реагирование и оказывает услуги реактивного реагирования на инциденты в случае нарушения безопасности.

Подразделение услуг интеграции систем безопасности Cisco работает с архитектурными задачами на уровне конкретных решений. Специалисты этого подразделения помогают оптимизировать развертывание технологий, включая AMP для оконечных устройств и межсетевой экран нового поколения Cisco Firepower. Наши эксперты обладают богатым опытом создания комплексных систем защиты, которые позволяют ускорить внедрение технологий обеспечения безопасности без значительных перебоев в работе организации.

При этом необходимо также внедрить соответствующие политики и технологии резервного копирования, что обеспечит дополнительную защиту в случае успешной атаки программ-вымогателей.

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

— Octapharma

Cisco Capital

Возможности финансирования, которые помогут в достижении поставленных целей

Программы финансирования Cisco Capital® помогут вам в приобретении технологий, необходимых для достижения поставленных задач и обеспечения конкурентоспособности. Мы поможем вам снизить капитальные затраты. Ускорить развитие бизнеса. Оптимизировать капиталовложения и повысить окупаемость инвестиций. Программы финансирования Cisco Capital обеспечивают гибкие возможности для приобретения оборудования, программного обеспечения, сервисов и дополнительного оборудования сторонних производителей. И всего один прогнозируемый платеж. Программами Cisco Capital можно воспользоваться более чем в 100 странах. Подробнее.

Преимущества Cisco

Программы-вымогатели пытаются проникнуть в сеть вашей организации любыми возможными способами. Фишинговые письма, зараженные веб-баннеры, спам — необходима надежная защита, охватывающая множество векторов. Только Cisco предлагает мощную архитектуру безопасности для устранения проблемы программ-вымогателей. Средства точечной направленности не способны справиться с этой задачей. Наше решение имеет эффективную многоуровневую структуру и строится на результатах работы ведущей группы экспертов Talos, подробно изучающей программы-вымогатели. Мы обеспечим максимально надежную блокировку программ-вымогателей, а также эффективную нейтрализацию атак в случаях, когда злоумышленникам все же удается преодолеть первый рубеж обороны и проникнуть в сеть. К сожалению, такие случаи вполне возможны.

C22-737492-01 08/16