# Программы-вымогатели: многоуровневая защита для блокирования хакерских атак

## Об этом документе

*По мнению издательства Los Angeles Times*, 2016 год обещает стать годом программ-вымогателей. И этот вид вредоносного ПО приносит огромную прибыль. Ежегодно преступники получают от своих хакерских кампаний до 60 млн долл. США.

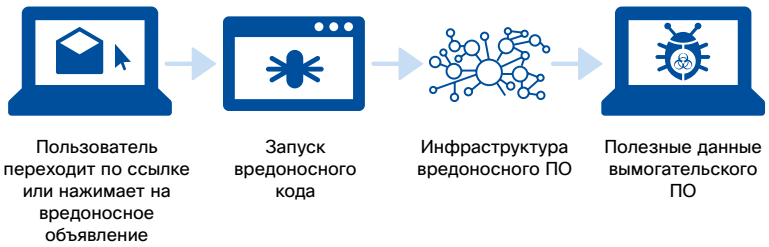
Как сообщают новостные издания, Cisco активно борется с программами-вымогателями. Мы видим, какими тревожными темпами эта угроза настигает компании во всех отраслях. Заказчики обязательно спросят у нас, насколько они защищены от этих угроз.

В этом документе рассказывается о том, что собой представляют программы-вымогатели, какие действия они совершают и как заказчики могут защитить свои организации от этой угрозы. Хотя основное внимание здесь уделяется программам-вымогателям, описанные процессы применимы и к другим угрозам.

## Что такое программы-вымогатели и как они действуют

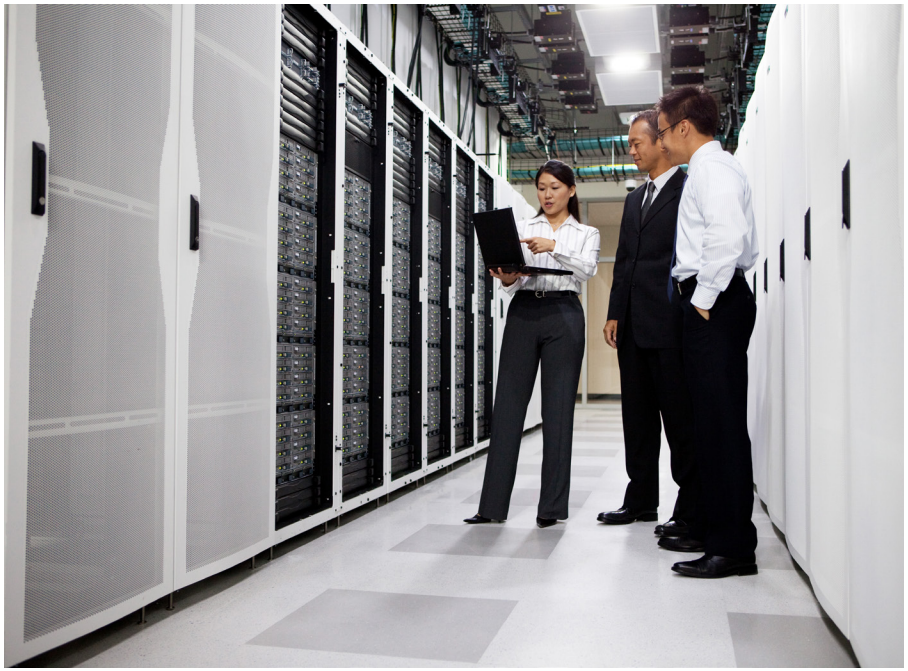
Программы-вымогатели — это вредоносное программное обеспечение, разработанное для захвата пользовательских файлов (например, фотографий, документов и музыки) с целью получения выкупа. Хакеры зашифровывают файлы и за их расшифровку требуют, чтобы пользователь заплатил определенную сумму, обычно в биткоинах. Недавний пример: в результате атаки программы-вымогателя клиника Лос-Анджелеса потеряла доступ к важным данным. Лишившись возможности вести документацию в электронном виде, клиника заплатила выкуп в размере 40 биткоинов (около 17 000 долл. США), чтобы вернуть доступ к своим файлам.

**Рис. 1.** Как программы-вымогатели проникают в сеть




Программы-вымогатели обычно распространяются в наборах эксплойтов, вместе с вредоносной рекламой (зараженные объявления на веб-сайте), в ходе фишинговых атак (мошеннические электронные сообщения, маскирующиеся под безопасные) или спам-кампаний. Фактически заражение начинается, когда пользователь открывает ссылку или вложение в фишинговом сообщении, зараженное рекламное объявление или веб-сайт, распространяющий вредоносный код.

**Рис. 2.** Типичное уведомление программы-вымогателя

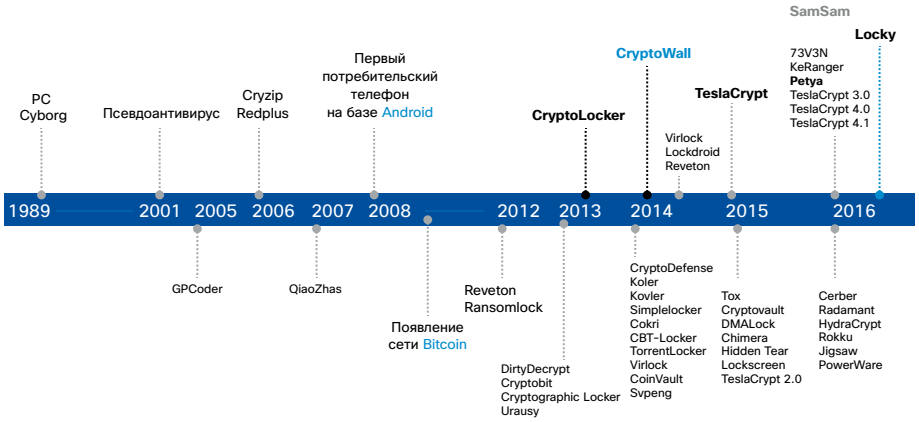



© Cisco и/или ее дочерние компании, 2016. Все права защищены. В данном документе содержится общедоступная информация компании Cisco.

## Эволюция программ-вымогателей

Простые и эффективные методы шифрования, популярность наборов эксплойтов, фишинга и готовность жертв заплатить выкуп — все это привело к появлению многочисленных разновидностей программ-вымогателей (рис. 3).

**Рис. 3.** Эволюция разновидностей программ-вымогателей




## Защита от программ-вымогателей

Для решения проблемы программ-вымогателей требуется сочетание людей, процессов и средств. Владельцу компании нужен достаточный уровень контроля, возможность отслеживать бизнес-процессы, сетевые операции и управлять ими. Сопоставив политику и поведение, можно дать определение нормальной работы сети и компании.

Нормативные требования и бизнес-правила, также называемые политикой, устанавливают, насколько операция может отклониться от нормы, прежде чем она будет расценена как аномальная. Возможность увидеть отклонения и нейтрализовать реальные и субъективные угрозы называется применением средств контроля на протяжении всего жизненного цикла атаки. Жизненный цикл кибератаки состоит из нескольких этапов (от выявления уязвимостей в целевой системе до внедрения вредоносного ПО) и в случае программ-вымогателей шифрования файлов жертвы.

Защита от программ-вымогателей — интересная задача. Данные технической экспертизы содержат список заведомо неблагонадежных источников сообщений и их адресатов, поэтому атаки часто можно остановить еще до того, как они произойдут. Программы-вымогатели используют систему доменных имен (DNS) для преобразования IP-адреса для целей контроля и управления (C2). На этом этапе Cisco может блокировать угрозу, прежде чем она превратится в серьезную проблему, и вам не придется платить выкуп.

Однако защита от программ-вымогателей не ограничивается мониторингом и устранением угрозы (применением технологий для решения проблемы). Важен также эффективный бизнес-процесс. В частности, необходимо ответить на два вопроса.

### Применяется ли в вашей организации проверенная процедура аварийного восстановления?

В некоторых случаях для аварийного восстановления используется конфигурация «активный/активный». Такую услугу предлагают несколько партнеров Cisco. Важную роль играет метод аварийного восстановления. Не рекомендуется в качестве узла аварийного восстановления использовать подключенный накопитель рабочей станции.

На многих предприятиях накопитель (например, диск F) подключается к определенному, совместно используемому сетевому ресурсу. Такая конфигурация нецелесообразна для узла аварийного восстановления. Почему? Природа программ-вымогателей такова, что любой подключенный накопитель и файлы на нем будут зашифрованы вредоносным кодом. Поэтому обязательное требование — продуманная сегментация и изоляция узла аварийного восстановления. Неотъемлемой частью этой стратегии является применение методов управления политиками Cisco TrustSec®. Также очень важна сегментация в сети и управлении политиками, которое обеспечивает поставщик решения для аварийного восстановления.

### Как вы справляетесь с серьезными нарушениями?

В ответе на этот вопрос одинаково важны бизнес-процесс и технология (стратегия и частота резервного копирования, проверка резервных копий и т. д.). Бизнес-процесс обычно проработан не полностью. Но во время атаки дорабатывать процесс будет слишком поздно. Если для отражения атаки придется прекратить работу некоторых подразделений, предусмотрено ли в вашей организации ранжирование бизнес-функций по важности? И согласны ли ваши руководители внедрить такое ранжирование в качестве корпоративной политики?

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

## Эффективная защита от программ-вымогателей

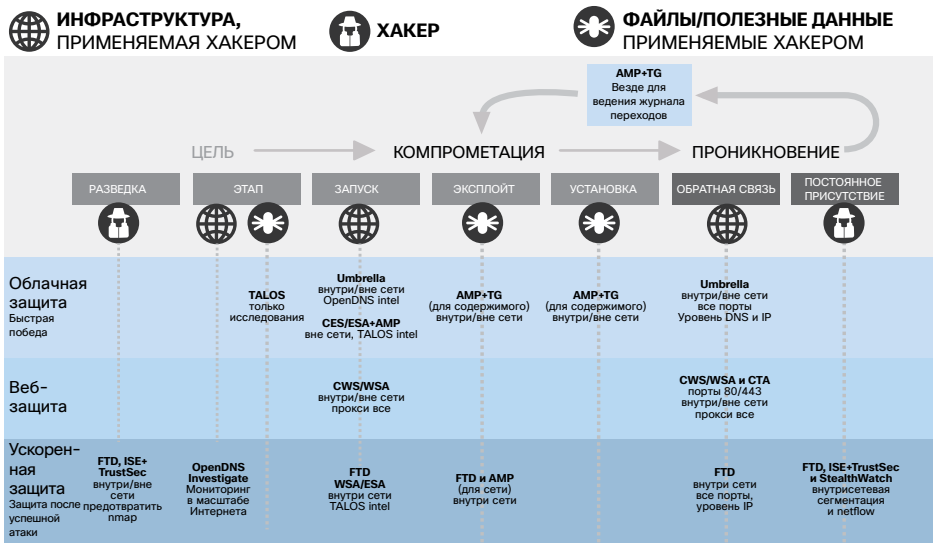
Cisco обеспечивает защиту от программ-вымогателей, предлагая многоуровневый подход при поддержке ведущей в отрасли группы по информационной безопасности и исследованиям Talos. Мы провели больше исследований программ-вымогателей, чем какой-либо другой поставщик. Мы обеспечиваем многоуровневую защиту для отражения и блокировки этой угрозы, если она незаметно проникла в организацию (а рано или поздно это обязательно произойдет).

Обычно злоумышленники находят способы обойти точечные решения. Чтобы противостоять им, требуется глубинная защита.

Наш многоуровневый подход обеспечивает безопасность от уровня DNS вплоть до оконечного устройства, сети, электронной почты и Интернета. Мы предоставляем интегрированные средства защиты, в которых сочетаются максимальная прозрачность и быстрота реагирования на атаки программ-вымогателей. Этот многоуровневый подход предлагается партнерам и заказчикам в виде предложений. Предложения позволяют вам мобилизовать группы людей, процессов и средств для защиты от программ-вымогателей.

На рис. 4 показаны продукты Cisco®, совместно действующие против программ-вымогателей. Среди них решение для защиты от сложного вредоносного ПО (AMP), Threat Grid (TG), Cloud Email Security (CES), Email Security Appliance (ESA), Cloud Web Security (CWS), Web Security Appliance (WSA), система когнитивного анализа угроз (CTA), решение для защиты от угроз Cisco Firepower (FTD) и платформа Identity Services Engine (ISE).

**Рис. 4.** Как Cisco обеспечивает защиту на протяжении всего цикла атаки




**Быстрый результат**: на этом уровне облачные решения обеспечивают исключительно надежную защиту при незначительном влиянии на работу сети.

**Защита веб-трафика:** защита контента, веб-прокси и другие антивредоносные функции дополняют защитой веб-трафика средства, применяемые на уровне «Быстрый результат».

**Оперативная защита и защита после вторжения:** в сочетании с уровнями «Быстрый результат» и «Защита веб-трафика» этот набор решений составляет межсетевой экран нового поколения. Вы получаете функции мониторинга и контроля приложений, защиты от вторжений, от вредоносного ПО и защиты содержимого. Управление сегментацией и возможность отслеживать и анализировать поведение сети позволяют автоматически обновлять и распространять политику. Анализируются аспекты поведения объектов, похожих на программы-вымогатели, так что политику можно быстро применить.

Иногда, если появляется новая разновидность программы-вымогателя, подозрительное поведение можно выявить еще до того, как мы узнаем его истинное значение. Благодаря аналитическим данным от группы Talos, Cisco может оперативно реагировать на новые разновидности вредоносного ПО на протяжении всего цикла атаки. Это позволяет создать самые современные и гибкие решения для защиты от программ-вымогателей.

При самом плохом сценарии, если вредоносный код проникнет в сеть, динамическая сегментация, предусмотренная технологией Cisco TrustSec, может предотвратить масштабное заражение. В результате программа-вымогатель не сможет широко распространиться и поразить большинство систем. Сервисы Cisco для защиты от вредоносного ПО (AMP и Threat Grid) дают возможность ретроспективно удалить вредоносное ПО с тех оконечных устройств, где код был обнаружен. В худшем случае могут пострадать одно или два оконечных устройства, пока идет накопление данных. Затем средства глубинной защиты удаляют вредоносное ПО с оконечных устройств, где оно может пребывать в скрытом состоянии.

Но как обеспечить немедленную защиту? Начнем с самого простого и эффективного способа.

## Немедленная защита

Для заказчиков, которые хотят немедленно усилить свои средства защиты, есть две отличные отправные точки: Cisco AMP и OpenDNS Umbrella.

В случае атак программ-вымогателей Umbrella отклоняет DNS-запрос, блокируя соединение на уровне DNS до того, как программа-вымогатель проникнет в систему. Кроме того, сервис Umbrella можно ввести в действие менее чем за час.

Cisco Advanced Malware Protection (AMP) для оконечных устройств блокирует запуск файлов программ-вымогателей. Это решение также непрерывно анализирует активность всех файлов в системе, помогая надежно обнаруживать и удалять вредоносное ПО.

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

Защита от сложного вредоносного ПО в сочетании с Umbrella может блокировать подавляющее большинство угроз на уровне DNS, не позволяя им проникнуть в сеть организации. Оконечные устройства защищены во время и даже после атак. Вы можете устранить все программы-вымогатели в два счета.

## Дополнительные уровни защиты

Помимо сервисов AMP и Umbrella, многие заказчики уже внедрили другие решения Cisco для обеспечения безопасности, которыми они могут воспользоваться в борьбе против программ-вымогателей.

Как уже говорилось, эти программы-вымогатели часто проникают в сеть при помощи спама, фишинговых сообщений, зараженных веб-страниц или рекламных объявлений. Исключительно важно обеспечить защиту электронной почты и веб-трафика.

**Требования к решениям для защиты электронной почты:** продукты для защиты электронной почты, такие как устройство Cisco Email Security Appliance, должны блокировать спам и фишинговые сообщения, которые используются для распространения программ-вымогателей. Они также должны блокировать вредоносные вложения, содержащие программы-вымогатели (рис. 5).

**Требования к решениям для защиты веб-трафика:** продукты для защиты веб-трафика должны препятствовать доступу к веб-сайтам, связанным с вредоносной рекламой, при помощи которой распространяются программы-вымогатели. Эти продукты должны также обнаруживать вредоносное ПО, используемое в атаках. Устройство обеспечения и облачные сервисы безопасности веб-трафика Cisco как раз отвечают этим требованиям (рис. 6).

## Роль безопасности сети

Организации рассчитывают, что их межсетевые экраны нового поколения будут блокировать известные сетевые угрозы, включая попытки программ-вымогателей передать информацию о жертвах на серверы контроля и управления. Межсетевые экраны нового поколения от Cisco идеально выполняют эту задачу.

**Рис. 5.** Защита электронной почты

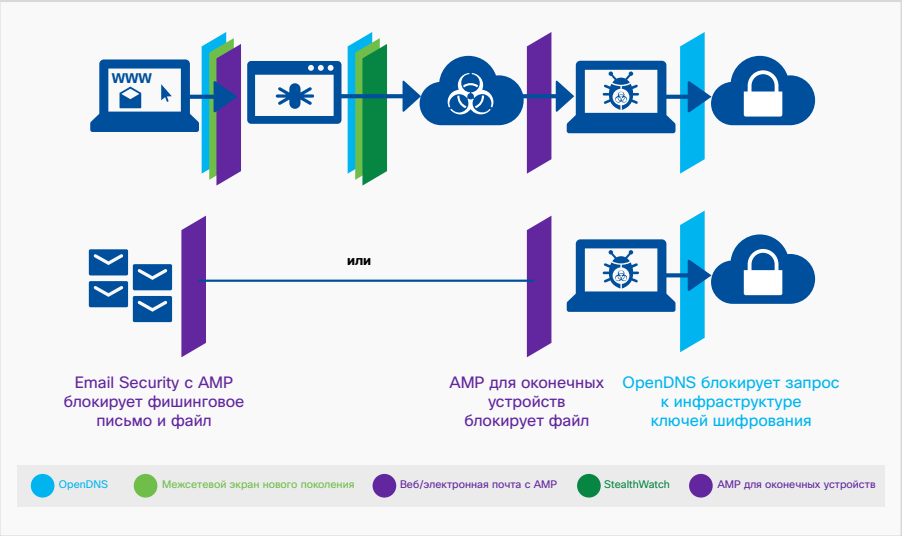
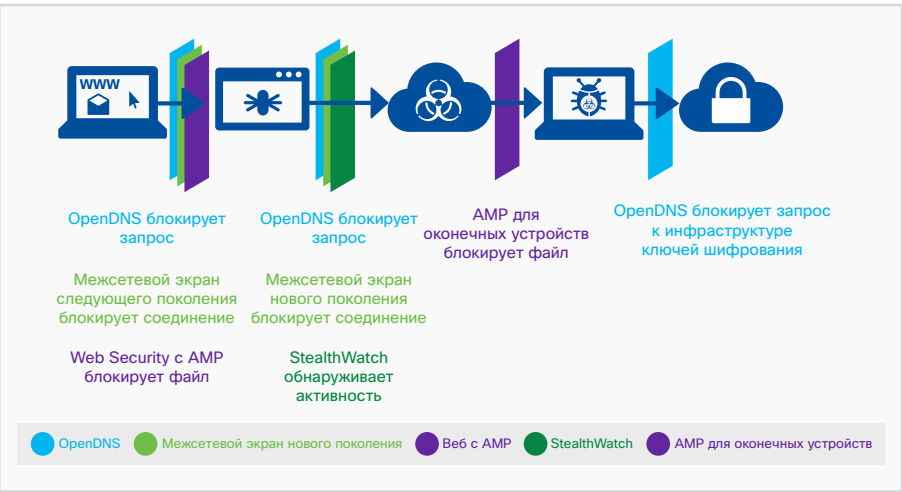



**Рис. 6.** Обеспечение безопасности веб-трафика




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

Межсетевые экраны нового поколения можно использовать с AMP для оконечных устройств. Если становится известно о вредоносных веб-серверах контроля и управления, межсетевой экран может блокировать несанкционированные попытки собрать и передать информацию о пользователях. Межсетевые экраны нового поколения препятствуют запуску программ-вымогателей, а защита от сложного вредоносного ПО обнаруживает и удаляет вредоносные файлы.

Система StealthWatch реализует концепции «сеть как сенсор» и «сеть как регулятор», действуя совместно с платформой ISE. Вместе эти решения способны выявить трафик программ-вымогателей в сети и автоматически изолировать подозрительные устройства.

## Безопасность для филиалов

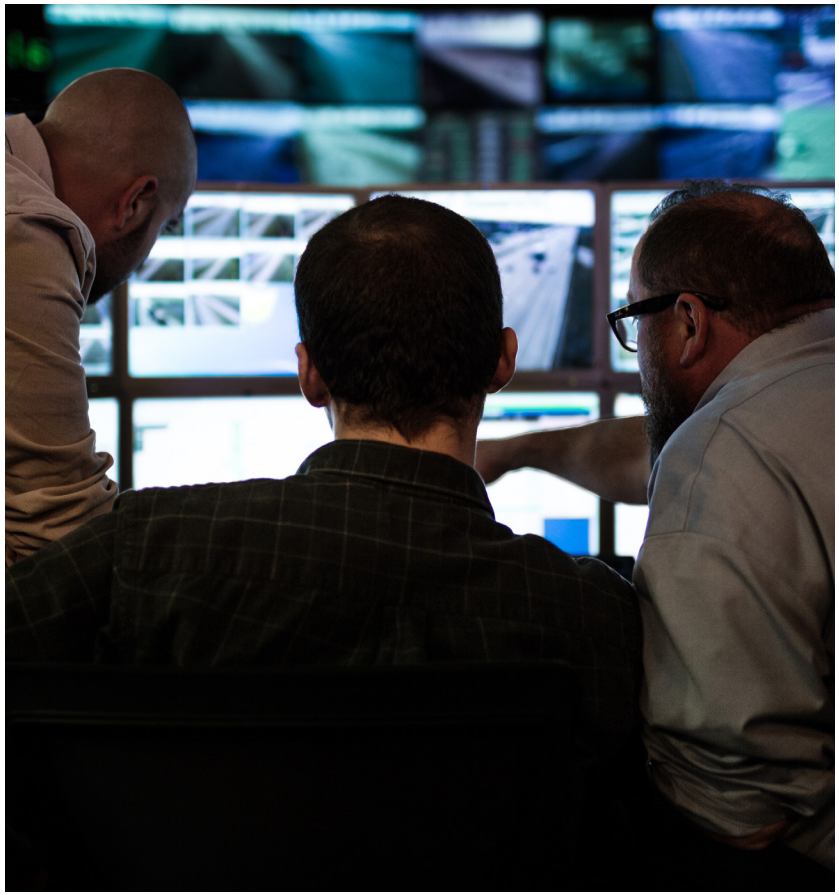
Филиалы, которым требуется прямой доступ к Интернету, а также защита от программ-вымогателей, могут внедрить сервис OpenDNS Umbrella в качестве начального уровня защиты. Чтобы укрепить безопасность филиала, можно также задействовать систему защиты от угроз Cisco Firepower™ для маршрутизаторов Cisco ISR. Оба варианта снижают расходы на глобальную сеть, поскольку не требуют передачи трафика по транспортной сети.

## Дополнительная информация

Чтобы узнать больше о защите от программ-вымогателей, примите участие в наших вебинарах: https://security-mktg.cisco.com/CiscoSecurityWebinarSeries.

Прочитайте сообщение блога Talos:
Программы-вымогатели: прошлое, настоящее и будущее.

Посетите веб-сайт: www.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 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)

C11-737871-00 09/16