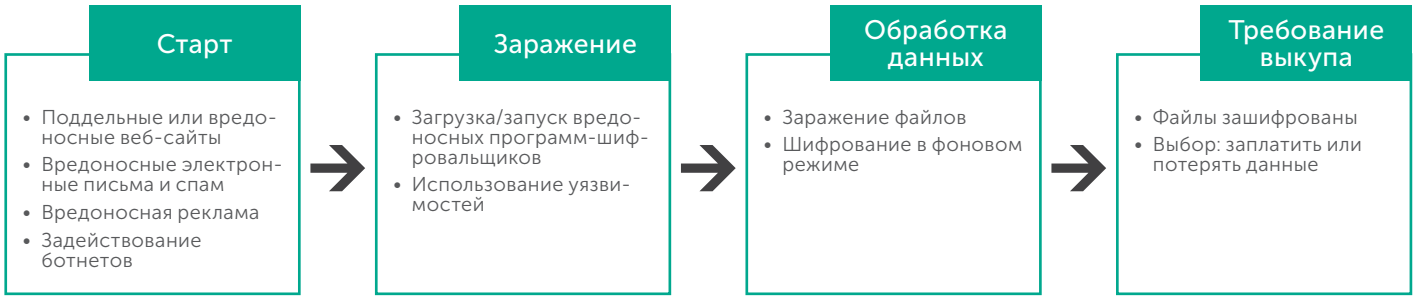
ЭПИДЕМИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ: ЦИФРЫ, ФАКТЫ, ЗАЩИТНЫЕ МЕРЫ

Только за первое полугодие 2015 года было зарегистрировано больше атак с использованием программ-вымогателей, чем за весь 2014 год.

- В 2014 году более 40% жертв вредоносных программ типа CryptoLocker согласились заплатить выкуп[1].
- Каждые 100 дней программы-вымогатели делают своих создателей богаче на 30 млн долл. США[2].
- Жертвами программ-вымогателей все чаще становятся крупные компании.
- Программы-вымогатели поражают файлы более 230 типов (в 2013 году — лишь 70 типов)[3].

СТАДИИ АТАКИ



КАК НЕ СТАТЬ ЖЕРТВОЙ:

ИНФОРМИРОВАНИЕ СОТРУДНИКОВ

Ваши сотрудники могут пройти тренинг в области IT-безопасности — например, приняв участие в игровом тренинге Kaspersky Cyber Safety, который является частью сервисов Kaspersky Security Intelligence.

КОМПЛЕКСНАЯ ЗАЩИТА IT-ИНФРАСТРУКТУРЫ

Чтобы защитить свой бизнес от программ-вымогателей, используйте комплексное решение Kaspersky Security для бизнеса, которое обеспечит:

- регулярное обновление баз;
- защиту от вредоносного ПО и сетевой экран;
- настройку параметров безопасности (например, включение эвристического анализа);
- интеграцию с облаком Kaspersky Security Network;
- мониторинг и устранение уязвимостей операционных систем и ПО.

Доступный функционал зависит от выбранного уровня Kaspersky Security для бизнеса.

РЕГУЛЯРНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ

В редких случаях, когда не удалось предотвратить заражение, спасти ваши данные, а вместе с ними и бизнес, поможет восстановление из резервной копии. Настоятельно рекомендуем регулярно проводить резервное копирование ваших систем и данных.

Специализированное решение Acronis Backup Advanced, предлагаемое надежным поставщиком решений в области защиты данных, позволит организациям:

- выполнять резервное копирование регулярно и по расписанию;
- сохранять резервные копии за несколько периодов в различных местах, в том числе в недоступной для программ-вымогателей среде — защищенном облаке;
- составить план восстановления, чтобы точно знать, как будет проходить восстановление и сколько времени оно займет;
- проводить регулярное тестирование — только в этом случае резервное копирование и восстановление окажутся эффективными;
- установить решение автоматизированного аварийного восстановления для повышения уровня защиты.

---

1 По данным проведенного в 2014 году исследования Центра междисциплинарных исследований в области кибербезопасности при Кентском университете.
2 Согласно отчету Dell SecureWorks.
3 Согласно отчету Bromium «Программы-вымогатели и их особенности».

ЗАКРОЙТЕ ПРОГРАММАМ-ВЫМОГАТЕЛЯМ ДОСТУП К ВАШЕМУ БИЗНЕСУ

Решения «Лаборатории Касперского» обеспечат защиту ценных данных. При каждой попытке доступа к корпоративным файлам, обозначенным как важные, компонент Мониторинг системы мгновенно создает локальную защищенную резервную копию. Если в дальнейшем компонент обнаружит действие, которое может быть классифицировано как вредоносное (например, попытку зашифровать файл), он автоматически выполнит откат нежелательных действий. На экране при этом отобразится только процедура обновления.

Восстановить файлы после повреждения можно с помощью специальной функции — откат вредоносных действий. Благодаря этой возможности можно не беспокоиться, что вымогатели будут требовать выкуп — данные в любом случае останутся в целости и сохранности. Если большинство людей будет применять такие меры предосторожности, программы-вымогатели вскоре станут невыгодными и останутся в прошлом.

КАК РАБОТАЕТ ЗАЩИТА НА РАЗНЫХ СТАДИЯХ АТАКИ

Попытка атаки

- Фильтрация интернет-трафика с помощью решения для защиты интернет-шлюзов
- Блокирование вредоносных объектов на уровне почтовых серверов
- Мониторинг уязвимостей и управление установкой исправлений
- Тренинги по основам IT-безопасности для сотрудников

KASPERSKY lab

Попытка заражения

- Антивирус, эвристический и сигнатурный анализ трафика
- Репутационная фильтрация с использованием облачных технологий
- Контроль запуска приложений
- Запуск приложений в безопасной среде
- Автоматическая защита от эксплойтов (AEP)

KASPERSKY lab

Анализ поведения приложений

- Контроль активности программ
- Поведенческий анализ
- Откат вредоносных действий

KASPERSKY lab

Если заражение все же произошло

- Обращение в техническую поддержку производителя
- Восстановление из резервной копии

Acronis

ВОССТАНОВЛЕНИЕ В САМЫЕ СЖАТЫЕ СРОКИ

К сожалению, по всему миру отмечается рост числа успешных атак программ-вымогателей. Их жертвами становятся и небольшие, и крупные компании. И даже если в вашей компании позаботились о защите данных, не стоит забывать и о «плане Б» – аварийном восстановлении.

Компании любого размера и рода деятельности должны иметь возможность уменьшить вероятность несанкционированного шифрования своих данных, минимизировать размер возможного ущерба и обеспечить восстановление бизнес-процессов в кратчайшие сроки. Никто не может позволить себе прерывать бизнес-процессы из-за инцидентов IT-безопасности или вирусных атак. Именно поэтому так важен вопрос выбора правильного решения для аварийного восстановления.

KASPERSKY lab

«Лаборатория Касперского» предлагает инновационные решения для защиты от всех видов киберугроз, сочетая передовые технологии анализа угроз с уникальными возможностями комплексной платформы обеспечения безопасности. «Лаборатория Касперского» может предложить организациям необходимые им сервисы и решения, в том числе расширенную техническую поддержку. Гибкость решений позволяет подстраиваться под основные бизнес-цели, обеспечивая защиту организаций любого типа от угроз, нацеленных на физические и виртуальные узлы, мобильные устройства, почтовые системы, серверы и шлюзы.

Acronis

Компания Acronis является ведущим производителем современных решений для аварийного восстановления и защиты данных в физических, виртуальных и облачных средах. Продукты Acronis для резервного копирования, аварийного восстановления, развертывания и миграции систем обеспечивают оптимальную защиту и доступность серверов и данных. С их помощью легко улучшить показатели RPO (директивный срок восстановления) и RTO (директивное время восстановления) и значительно снизить издержки вашего бизнеса.

Чтобы выбрать решение для противодействия программам-шифровальщикам, проконсультируйтесь со специалистами компании-партнера «Лаборатории Касперского».

Контактная информация и адреса партнеров представлены на странице kaspersky.ru/find_partner_office

KASPERSKY lab