KPMG

Программы-вымогатели в новых реалиях

Как защититься и реагировать на них

КПМГ в Центральной Азии

Программы-вымогатели тогда и сейчас

Программы-вымогатели впервые получили всемирную известность в результате атаки WannaCry в 2017 году. Эта кампания была беспрецедентной по масштабу, согласно данным Европола[8], который оценивает, что около 200 000 компьютеров были заражены в 150 странах.

Одной из основных целей была Национальная служба здравоохранения Англии, затронувшая 80 из 236 медицинских фондов. Тридцать четыре из этих трастов и более 600 других организаций первичной медико-санитарной помощи имели активные вирусы, вызывающие блокировку компьютеров, включая сканеры МРТ, холодильники для хранения крови и театральное оборудование[9].

Успешные атаки программ-вымогателей могут служить причиной значительных затрат:

— **Материальные затраты** включают потерю дохода при неработающем оборудовании, затраты на восстановление и компенсацию клиентам или судебные разбирательства. Некоторые компании могут решить заплатить выкуп, но это не всегда приводит к восстановлению данных или систем.

— **Нематериальные затраты** труднее измерить, но они включают потерю репутации. В худшем случае, если доверие будет подорвано, в долгосрочной перспективе это может иметь еще больший эффект.

COVID-19, изоляция и массовый переход к удаленной работе вызвали стремительный рост инцидентов с участием программ-вымогателей[10]. Уязвимости в управлении людьми, процессами и технологиями из-за перехода на удаленную работу в этот период открыли огромные возможности для киберпреступников.

Злоумышленники могут использовать множество различных методов для проникновения программ-вымогателей в систему, что затрудняет защиту от этих угроз.

Чтобы программа-вымогатель работала должным образом, она должна проникнуть на хост, как вирус. В этом случае хост - это ваша сеть и системы. Чтобы внедрить программу-вымогатель в вашу систему, злоумышленники ищут сетевые уязвимости, которые они могут использовать. Поскольку COVID-19 увеличил количество сотрудников, работающих на дому, риск увеличился.

US$1M

Средние глобальные затраты на устранение атаки с использованием программ-вымогателей[11]

21%

атак совершается через электронную почту или фишинг.[12]

29%

атак совершаются через удаленный доступ[13]

---

8 “Cyber-attack: Europol says it was unprecedented in scale”. BBC News. 13 Мая 2017.

9 National Audit Offce, Investigation: WannaCry cyber attack and the NHS, Апрель, 2018.

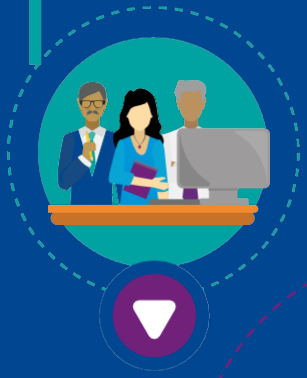
10 Harvey Nash/KPMG CIO Survey, 2020.

11 H1 2020 Cyber Insurance Claims Report, Coalition Inc., 2020.

12–13 Sophos Whitepaper, Май, 2020.

Как изменились атаки в результате COVID-19

До COVID:
Широкий профиль компаний и людей



Два года назад киберпреступники часто зашифровывали файлы, блокируя предприятия до тех пор, пока они не заплатят выкуп. Это были широкие кампании без какой-либо конкретной цели, играющие числами для получения дохода.

В мае 2017 года WannaCry затронул 80 трастов NHS. Некоторые комментаторы предполагают, что WannaCry заработал преступникам всего 50 тысяч долларов, но исправление обошлось NHS в 128 миллионов долларов.

Злоумышленники проводят атаку с использованием программ-вымогателей.

Уязвимые системы зашифрованы, запрещая доступ к потенциальным жертвам атаки

Злоумышленники требуют выкуп

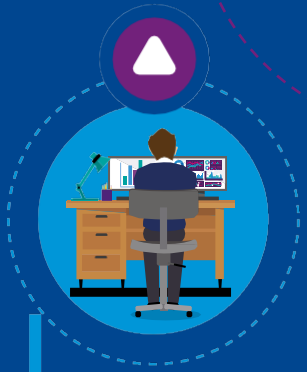
Бизнесу приходится платить огромные суммы за выкуп за восстановление систем.

Злоумышленники устанавливают свое присутствие в системах

Они повышают свои привилегии внутри компании и устанавливают контроль

Злоумышленники нацелены на ключевые системы, чтобы оказать наибольшее влияние, и выполняют атаку программ-вымогателей и требуют выкупа.

Бизнесу приходится платить сотни тысяч за восстановление своих систем.



▶ Работа на дому создает в 3,5 раза больший риск[14]

Пост-COVID:
Организации с более конкретными целями

Теперь хакеры часто незаконно вывозят данные, а также шифруют их. Они хранят данные для выкупа, и, если платеж не производится, происходит утечка данных, что вынуждает жертв сообщать регулирующим органам об утечке данных. Это признание может привести к штрафу (до 4% от мирового оборота).

В июле 2020 года компания Garmin подверглась атаке программы-вымогателя, которая, как сообщается, была сделана Evil Corp., которая потребовала 10 миллионов долларов США для восстановления систем.

[14] Identifying Unique Risks of Work from Home Remote Offce Networks, Bitsight Blog, 14 Апреля, 2020.

Адаптация к программ-вымогателей

85–90% кампаний вымогателей работают путем нацеливания на известные уязвимости для получения начального доступа.[15] Это существующие проблемы или пробелы в ИТ-системах, для которых известны ошибки, что указывает на то, что для упреждающей борьбы с угрозой можно сделать гораздо больше.

Однако, если атака программы-вымогателя окажется успешной, можно предпринять ответные меры для уменьшения воздействия и минимизации сбоев в работе.

[15] Отчет об утечке данных Verizon 2020

Подготовка к атакам - проактивный подход

90% успешных кибератак связаны с отсутствием базовых средств контроля и защиты от известных уязвимостей;

Жизненный опыт - это то, как мы учимся. **Смоделируйте опыт, чтобы команда могла извлечь из него уроки** и уменьшить влияние атаки.

Обучите своих сотрудников тому, как защитить себя и организацию. Они являются важной линией защиты и отличными возможностями для сбора информации, если знают, на что обращать внимание.

Вам придется восстанавливать систему с нуля, если ваши системы и данные исчезли после атаки. Убедитесь, что у вас есть резервные копии, которые, как вы знаете, обеспечивают хороший уровень безопасности..

Быстрое масштабирование удаленной работы означает, что ИТ-отдел быстро включил множество подключений с использованием новых технологий. Риск ошибок новых настроек высок. **Найдите время, чтобы проверить эти «двери»;** это займет всего несколько дней.

«Тяжело в учении – легко в бою», попробуйте взломать вашу организацию, как это сделал бы киберпреступник; **выявите проблемы и исправьте основы за неделю**.

[16] Verizon 2020 Data Breach Investigations Report

Быстрая реакция на атаку - реактивный подход

Это случилось - вы были атакованы программой-вымогателем - вы не можете получить доступ к своим системам, клиенты звонят и спрашивают, что происходит, и **вам необходимо принять меры.**

Любая атака программы-вымогателя, скорее всего, повлияет на контракты, которые вы заключаете с другими - данные, услуги, обязательства, - **поэтому юридическая консультация необходима.**

Когда атака угрожает остановкой всех ваших операций, **учебник дает вашим командам готовый ориентир.**

У вас есть политика на случай событий с низкой вероятностью и высоким финансовым воздействием. Поскольку количество атак продолжает расти, разумно покрыть расходы на киберинциденты.

Нет ничего лучше спокойствия, чтобы заинтересовать клиентов и партнеров. Определите позицию вашей организации в случае атаки и подготовьте контент для быстрого реагирования.

Подробное описание того, что именно произошло, как это произошло и что именно было затронуто, может потребовать особых навыков судебной экспертизы. Собранная информация может служить обоснованием любого судебного иска.

Быть в курсе событий, связанных с программами-вымогателями

Организации ускоряют цифровую трансформацию, стремясь повысить функциональность и устойчивость в мире после COVID-19. Это, вероятно, приведет к еще большему распространению облачных сервисов и принесет много преимуществ - и потенциальных рисков. Вот некоторые действия, которые вы можете предпринять сейчас и в среднесрочной перспективе, чтобы улучшить свою кибербезопасность, и некоторые проблемы, с которыми ваш бизнес может столкнуться в будущем.

Действия, которые нужно предпринять сейчас

Assess the impact of system loss on your business and prepare a response action plan.

- Оцените влияние потери системы на ваш бизнес и подготовьте план действий по реагированию.
- Обновите свои тренинги по безопасности и ресурсы для работы после COVID.
- Проверьте возможности обнаружения и реагирования конечных точек (EDR), а также то, что вы можете регистрировать и отслеживать.
- Проводите попытки взломов собственных систем этичными хакерами
- Проверьте свои возможности реагирования на инциденты и резервные копии.

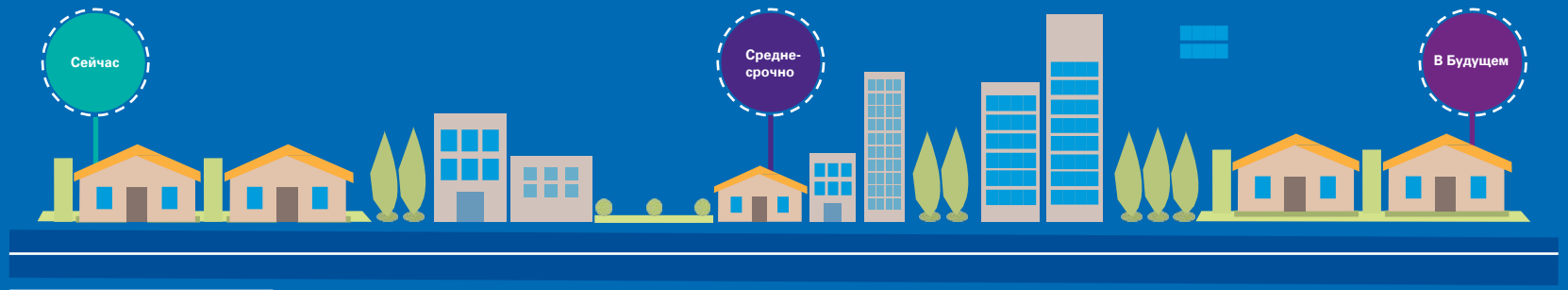
Действия на среднесрочную перспективу

Обдумайте и проверьте внесенные вами технологические изменения на предмет ошибок.

- Подумайте, как определенная реструктуризация бизнеса может повысить риск «внутренней угрозы».
- Выполните упражнения на основе сценариев, которые окажут наибольшее влияние на вашу организацию, и извлеките уроки из него.
- Проведите попытки взломов собственных систем этичными хакерами снова и обязательно возвращайтесь к этому процессу, чтобы проверить уровень своих защитных систем.
- Подумайте, что может означать для общей ответственности за безопасность принятие и расширение облачных сервисов.

Будущие тенденции и вызовы

Согласно опросу генерального директора KPMG Outlook Pulse Survey на период до 2021 года, большинство опрошенных руководителей указали на поразительный прогресс, достигнутый в оцифровке своей деятельности, бизнес-моделей и потоков доходов во время пандемии. Три четверти (74 процента) говорят, что скорость оцифровки увеличилась на несколько месяцев. Кроме того, руководители планируют больше тратить на цифровые технологии по сравнению с прошлым годом, при этом 49 процентов вкладывают значительные средства в новые технологии[8].



8 KPMG CEO Outlook Pulse Survey, 2021

Спасибо за внимание!