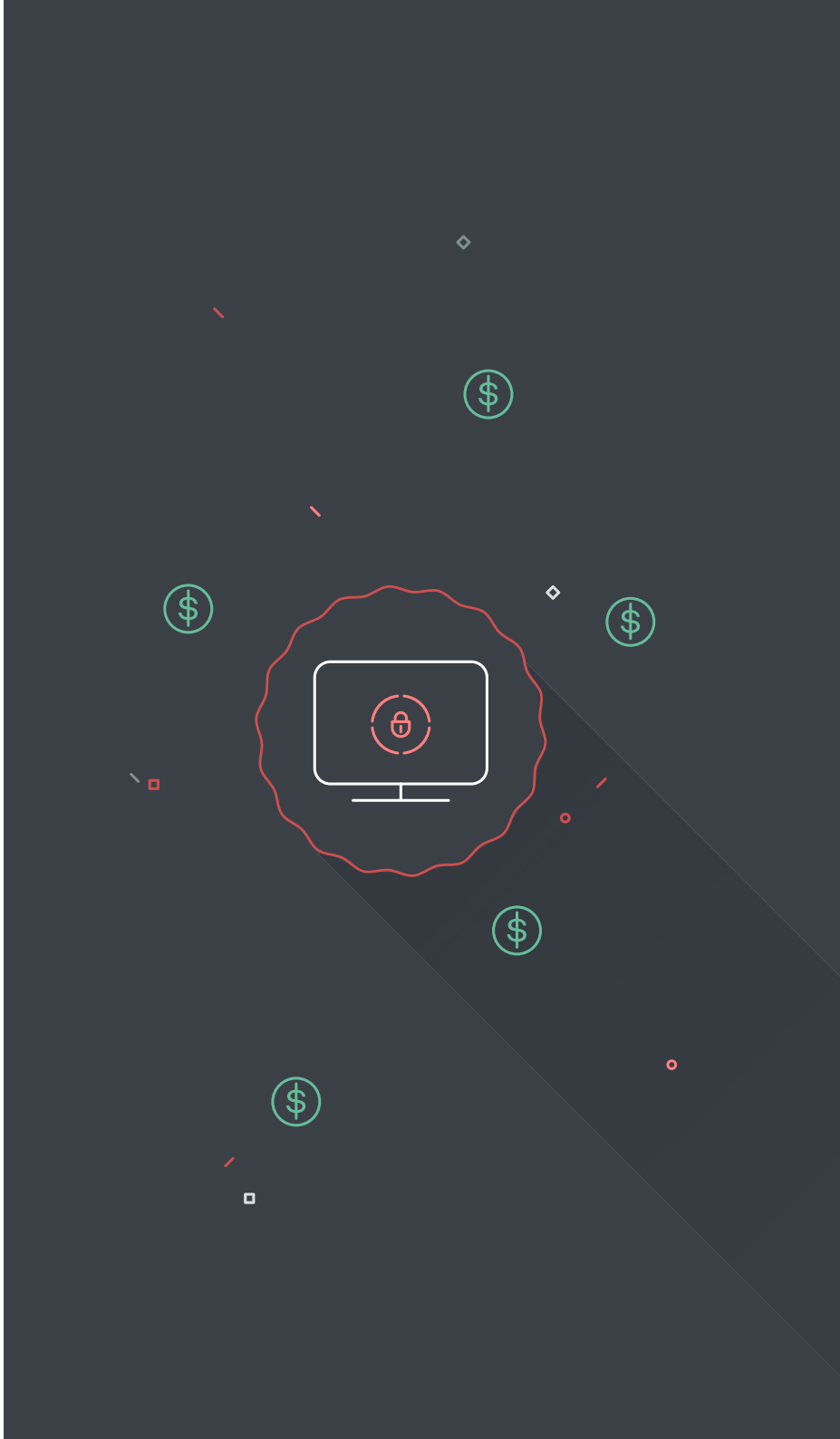
Panda Adaptive Defense 360

Неограниченная видимость, абсолютный контроль

panda

cloudav.ru/intelligence-platform/

Содержание

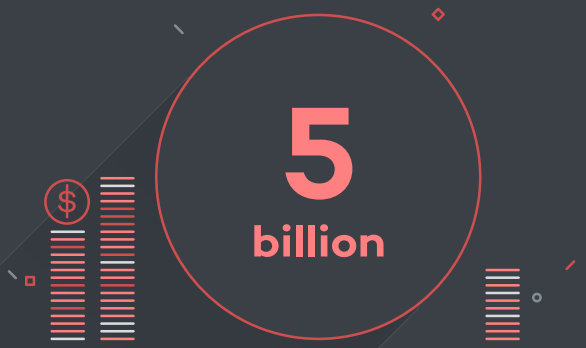


panda

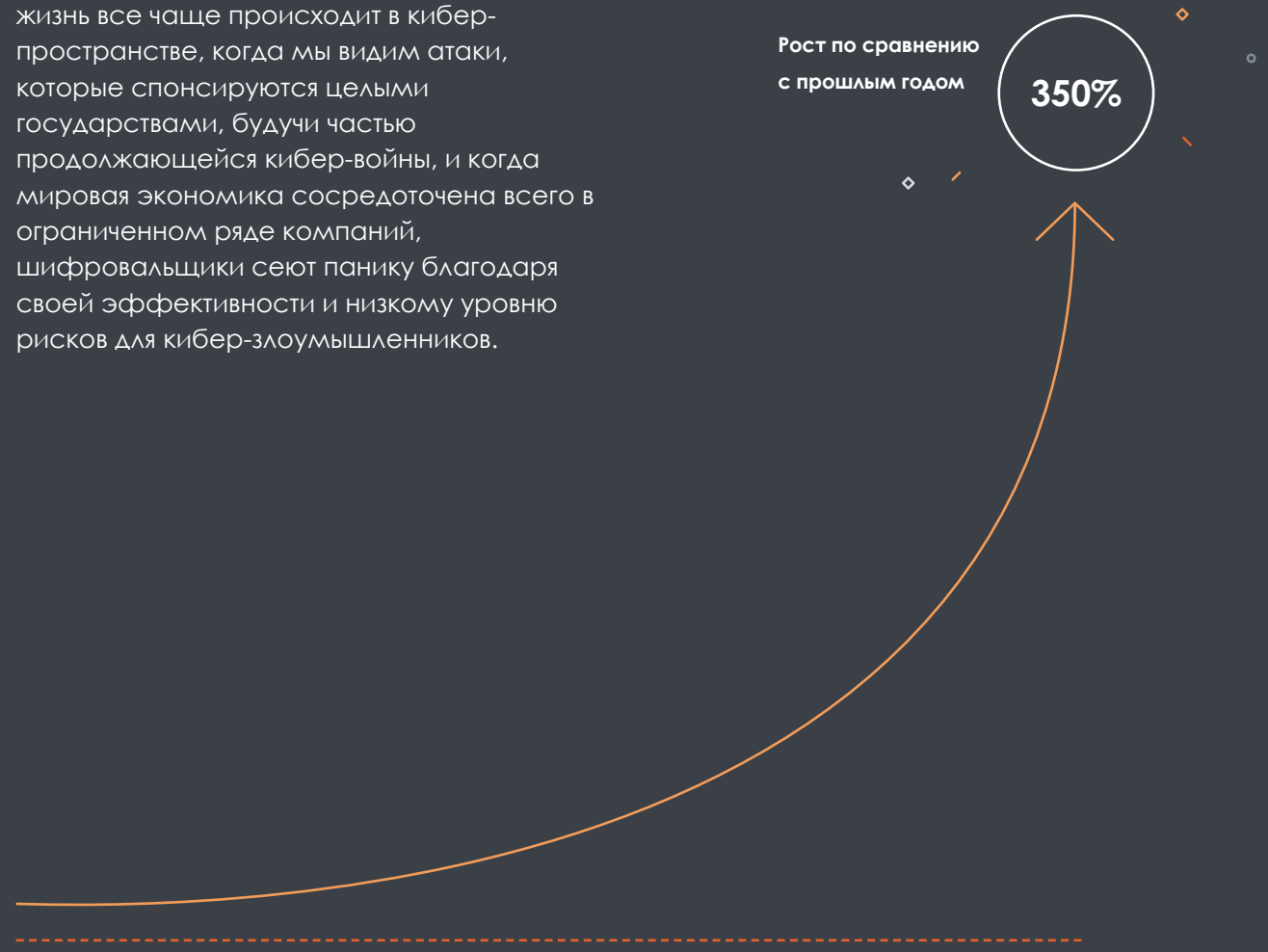
1. Введение

Вымогатели/шифровальщики (ransomware) все еще являются наиболее прибыльным оружием в арсенале кибер-преступников. Этот тип кибер-преступлений шифрует файлы на компьютере и блокирует доступ к ним до тех пор, пока не будет получен запрашиваемый выкуп, как правило, в биткоинах, которые являются неотслеживаемой **виртуальной криптовалютой.**

Суммарный ущерб от них в 2017 году составил примерно **5 млрд. долларов США**, что на **350% выше по сравнению с предыдущим годом**. Эти угрозы стали не только самым сложным типом кибер-атак, но и причинившими наибольший вред.



В тот момент, когда наша повседневная жизнь все чаще происходит в кибер-пространстве, когда мы видим атаки, которые спонсируются целыми государствами, будучи частью продолжающейся кибер-войны, и когда мировая экономика сосредоточена всего в ограниченном ряде компаний, шифровальщики сеют панику благодаря своей эффективности и низкому уровню рисков для кибер-злоумышленников.

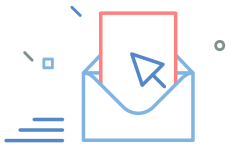


2. Парадигма цифровой трансформации

С более чем 258 000 новых угроз, ежедневно обнаруживаемых лабораторией PandaLabs, так называемая цифровая трансформация подразумевает множество новых серьезных проблем. Сейчас кибер-преступность является более активной угрозой, чем раньше. Кибер-атаки и финансовое мошенничество, использующие современные ИТ-технологии, достигли невообразимой прежде изощренности и сложности. В Интернете, где легко стать анонимным, доверие людей можно завоевать с помощью социальной инженерии, что заставляет их снижать свой уровень защиты и бдительности, обнажая их конфиденциальность.

Наряду с этими новыми онлайн-привычками мы также получаем новые платформы, например, **Android**, которая стала самой распространенной операционной системой в мире. Популярность Android также делает ее основным вектором атаки для заражения и распространения таких **шифровальщиков как** Charger, который способен блокировать доступ пользователя к своим данным на любом смартфоне до тех пор, пока не будет выплачен выкуп.

Ожидается, что к 2020 году во всем мире будет подключено к Интернету свыше 50 миллиардов устройств, генерирущих трафик в объеме 40 трлн. ГБ каждые 10 минут. **В Интернете вещей (IoT)** безопасность приобретает критический аспект. Наличие еще большего количества портативных устройств, которые могут подключаться к Интернету, означает, что хакеры могут использовать новые методы: могли бы вы рассматривать возможность заражения других людей, чтобы самому не платить выкуп? А это ужасный метод распространения, используемый угрозой Popcorn Time.

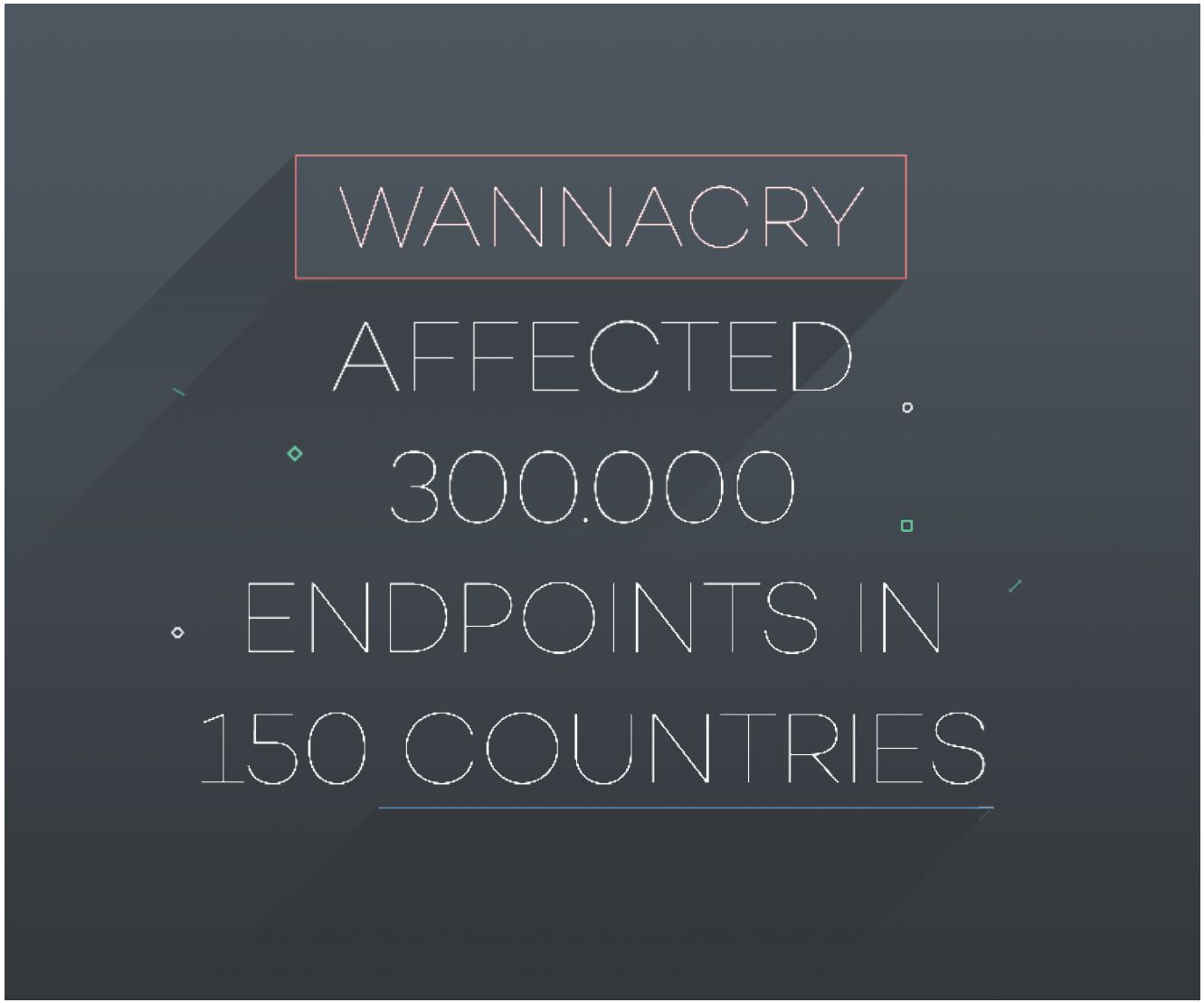


Стремительное распространение мобильных устройств породило целый ряд новых техник, которые позволяют хакерам выполнять атаки в современных технологических пространствах. Именно это произошло в австрийском отеле, где кибер-преступники атаковали отель, заблокировав двери номеров и отключив ПО для программирования пластиковых карт-ключей.

3. Атаки, спонсируемые государствами

В западных странах бытует мнение, что две самых крупных атаки в истории (WannaCry и Goldeneye/NotPetya) могли быть выполнены при поддержке правительств некоторых стран (КНДР в случае с WannaCry и Россия - с Goldeneye/NotPetya). Обе эти атаки использовали шифровальщиков с хорошо развитыми возможностями саморепликации, как это было и в случае с Bad Rabbit, который имел много общих черт с шифровальщиком NotPetya.

Т.к. шифровальщик был сетевым червем, то любой зараженный WannaCry компьютер, помимо того, что на нем были зашифрованы все документы и от его владельца теперь требовалось уплатить выкуп, также способствовал быстрому распространению этой угрозы более чем на 300 000 других компьютеров. При этом заражение осуществлялось через старую уязвимость в Microsoft Windows. В результате пострадало огромное количество организаций и предприятий.



4. Бизнес в центре внимания

Шифровальщики - это проблема, затрагивающая все большее число компаний. И она реально оказывается в центре внимания после того, как одна из таких атак становится вирусной, как это в случае с WannaCry в прошлом году.

Сегодня 18% рыночной капитализации представленных на биржах в США компаний принадлежит всего 5 компаниям: Apple, Google, Amazon, Microsoft и Facebook.

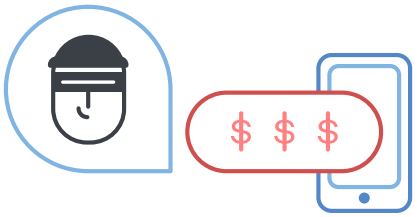
Целью шифровальщиков является финансовая выгода. И хотя невозможно получить выкуп физически, сейчас существует масса способов "виртуальной" передачи денег от одного человека к другому. Так что кибер-преступники спокойно используют техники обмана и шантажа, чтобы получить деньги своих жертв:

Кибер-кража

- Жертвой кибер-кражи стал, например, Equifax, что сделало его эпицентром самого крупного в истории нарушения конфиденциальной персональной информации. Нарушение стало возможным благодаря уязвимости, которая ранее была использована шифровальщиком, что "открыло" двери для кибер-злоумышленников

Вымогательство

- Тоже способ получения чего-либо, особенно денег, используя силу и угрозы. Есть три четких примера вымогательства: WannaCry, NotPetya и Bad Rabbit.



Саботаж

- Или диверсия в отношении гражданских или военных объектов. Например, в августе 2012 года Shamoon заразил свыше 30 000 систем, принадлежащих государственной нефтегазовой компании Aramco из Саудовской Аравии, парализовав их экспорт на 2 недели. Это же ПО было снова использовано через несколько лет для осуществления серии кибер-атак, но в этот раз там появился новый модуль, содержащий шифровальщика.

Как и вышеупомянутые преступления, за последние несколько месяцев мы видели несколько новых стратегий для проникновения шифровальщиков в корпоративные сети, такие как использование или злоупотребление легитимными инструментами Windows (например, PowerShell) для заражения компьютеров **Cerber**. Например, это было целью у **Crysis/Dharma**.

В этом случае сервер запускал протокол удаленного подключения к рабочему столу (RDP), а хакеры использовали атаку типа brute force для подроба регистрационных данных и получения удаленного доступа. Тенденця установки вредоносных программ с использованием RDP достиглшо такой степени изощренности, что даже сами шифровальщики уже имеют собственный интерфейс, который позволяет кибер-преступникам выбирать папки, чье содержимое необходимо шифровать, выбирать сетевые компьютеры, настраивать самоудаление, указывать почтовые адреса для контакта с жертвами и т.д. Все это мы видели с шифровальщиком **WYSIWYF**, обнаруженным лабораторией PandaLabs.

Существуют также семейства шифровальщиков, которые содержат дополнительные функции для причинения еще большего вреда, возможности работы в автономном режиме или более стремительного распространения с использованием страшного **Locky**.

Обладая такой информацией, теперь еще больше, чем когда-либо ранее, начинает казаться, что компаниям следует иметь **страховые полисы**, которые смогут хотя бы частично покрыть ущерб от кибер-атак.

5. Цена атак

Мы видели, как знкачительно упростились процессы осуществления кибер-атак за счет профессионализации хакеров, эволюции технологий и той легкости, с которой можно получить доступ к данным. Хотя, несомненно, основная причина популяризации такого типа угроз - это их высокая рентабельность. Кибер-вооружения, используемые хакерами для извлечения финансовой выгоды, продаются по вполне доступным для многих ценам.

Fuente: Recorded Future.

Атаки шифровальщиков по-прежнему развиваются, и их количество постоянно растет, потому что жертвы продолжают платить выкуп. Тем не менее, всегда есть несколько конкретных мер, которые мы можем предпринять во избежание таких атак:

Убедитесь, что учетные данные сотрудников защищены надежными паролями и они не имеют прав администратора.

Не открывайте непрошенные письма или письма от неизвестных отправителей: лучше всего их сразу удалить и ни в коем случае не отвечать на них.

Не доверяйте укороченным ссылкам или вложениям, даже если они пришли от тех контактов, кому вы привыкли доверять.

Регулярно делайте резервные копии для избежания потери данных.

Разработайте и внедрите план аудита (выполняется внутренней командой аудиторов или внешними аудиторами) корпоративных систем и политик, чтобы быть способным обнаруживать возможные уязвимости.

Выделите ресурсы для повышения уровня подготовки и осведомленности сотрудников по вопросам ИТ-безопасности, особенно о шифровальщиках.

Важно иметь многоуровневую безопасность, т.к. при наличии современных угроз (таких как шифровальщики) базовой защиты уже недостаточно. Для обеспечения максимальной защиты очень рекомендуется использовать комплексные и надежные мультиплатформенные системы, например, Panda Adaptive Defense 360.

Подробнее:
www.cloudav.ru/intelligence-platform/

Наши контакты:

+7 495 105-94-51
sales@rus.pandasecurity.com