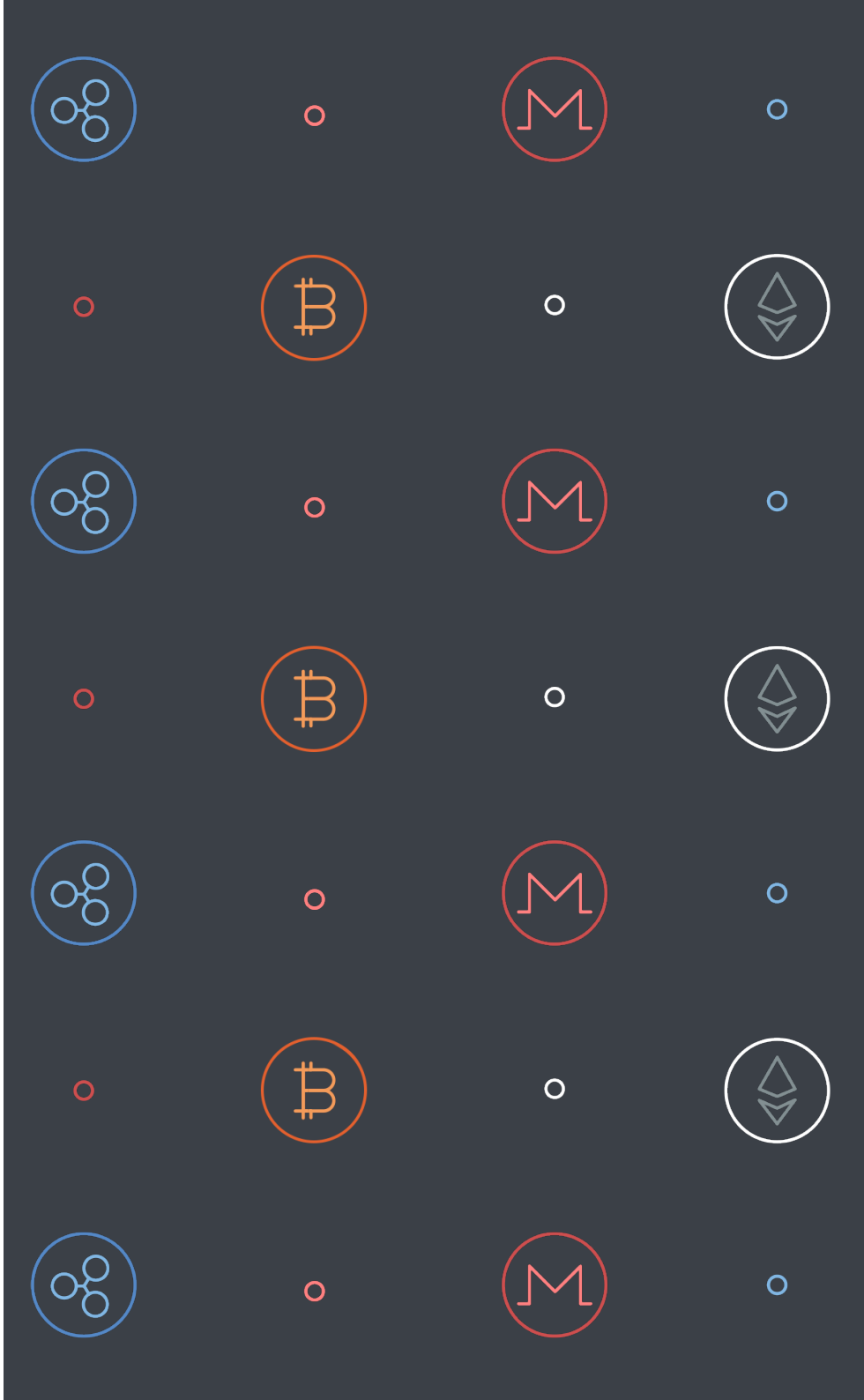
Содержание



panda

1. Скрытые расходы

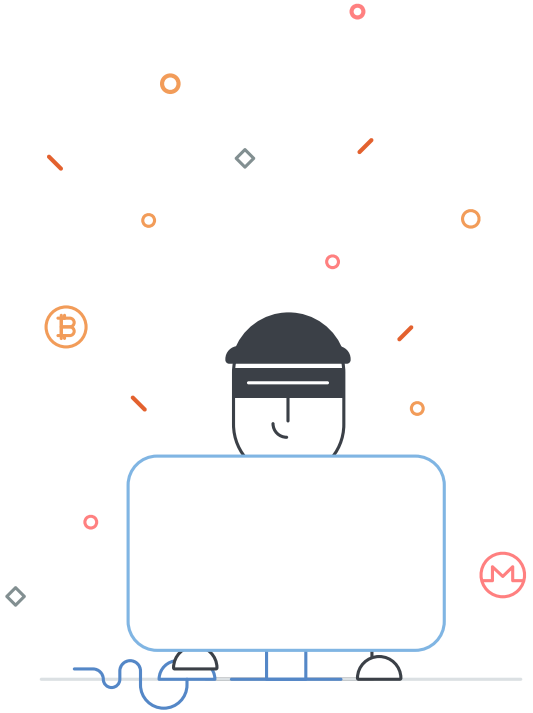
Криптоджекинг - это явление, которое характеризует 2018 год сточки зрения информационной безопасности. Он стал основной угрозой безопасности и работоспособности электронных устройств в первом полугодии 2018 года. С начала года мы видели **2,4 млн. случаев таких атак**, которые очень популярны среди хакеров.

Вот какую картину рисует антивирусная лаборатория **PandaLabs** компании Panda Security: хотя "традиционные типы" вредоносных программ (трояны или черви) по-прежнему активно используются злоумышленниками, новые тенденции, такие как безфайловые атаки или атаки, не использующие вредоносное ПО, показывают стремительный рост.

Данная тенденция такова, что **Биткоин**, наиболее широко используемая цифровая валюта, была включена в шорт-лист Fundéu BBVA как "слово года" в 2017 году, что подчеркивает влияние, которое оказывают криптовалюты на нашу жизнь в настоящее время.

Кибер-преступники **постоянно развивают свои техники**, придумывая все новые способы, как можно набить свои карманы деньгами. Такая непрерывная эволюция помогла им нащупать новую золотую жилу: **криптомайнинг.**

Но чтобы понимать, как и почему "плохие парни" хотят добывать криптовалюту за наш счет, мы рассмотрим весь тот процесс...



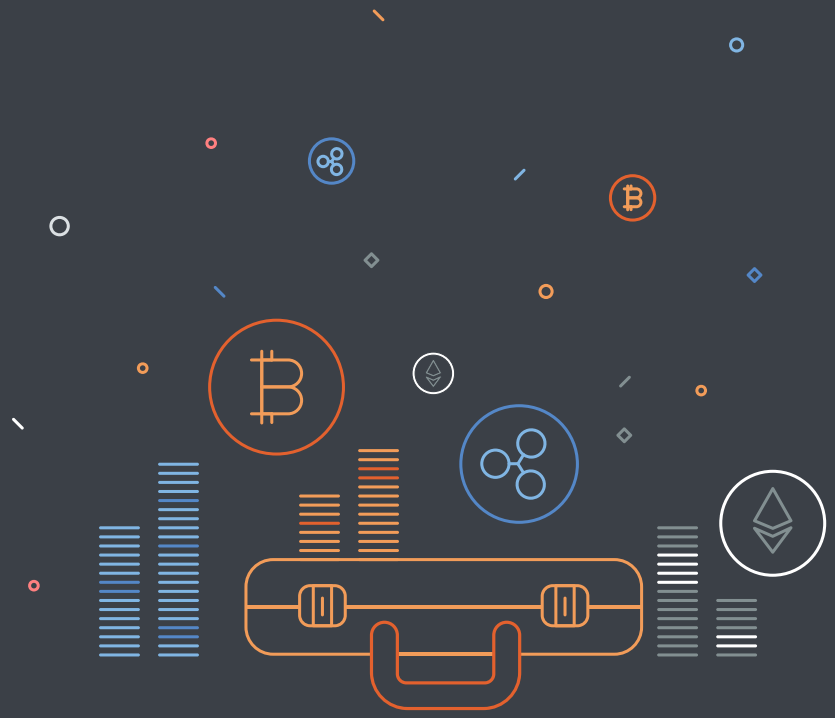
2. Что такое криптовалюты?

Появление новых криптовалют связано с необходимостью проведения анонимных транзакций. В 2009 году была создана первая криптовалюта: Биткоин. **В наши дни существует свыше 1300 различных криптовалют** с различным происхождением и характеристиками, но все они имеют цифровую природу и намерение обеспечивать анонимность своих транзакций.

Законность использования криптовалют в настоящее время является очень актуальной темой: некоторые страны обсуждают их запрет, а в других странах ценность таких валют имеет подвешенное юридическое состояние.

В конечном счете, это палка о двух концах: цифровая валюта, обеспечивающая прозрачность и простоту транзакций, может показаться идеальным инструментом для оплаты нелегальных действий хакера. Она также идеально подходит для кибер-преступников: сейчас почти каждая атака шифровальщиков требует оплату в биткоинах или другой криптовалюте благодаря тому, что эти транзакции почти невозможно отследить.

Рост стоимости таких криптовалют как **Биткоин**, **Ethereum** или **Ripple** означал, что эти валюты стали одними из основных источников дохода для кибер-преступных организаций.



3. Блокчейн, смысл существования криптовалют

Один из вопросов, который порождает множество сомнений относительно криптовалют, - это возможность их "добычи", т.е. криптомайнинга. **Многие из этих криптовалют могут быть получены путем выполнения математических операций**, подобно любым вычислениям.

Впрочем, майнинг криптовалют - это все более сложная задача, которая потребляет все больше и больше электроэнергии и вычислительных мощностей. Отчасти это связано с технологией Блокчейн.

Технология Блокчейн - это краеугольный камень непробиваемой обороны криптовалют, также как и их анонимность. Блокчейн был создан для поддержки биткоинов. Криптомайнинг жизненно необходим для работы системы: эта компьютерная активность необходима для обработки транзакций, которые выполняются на уже существующих блокчейнах. Он служит для производства новой криптовалюты и подтверждения транзакции в сети блокчейн. Т.е. чтобы создавать больше криптовалюты, необходимо ее добывать (майнить). **Без майнинга система рухнет.**

Блокчейн состоит из распределенной базы данных, и в силу особенностей разработки, **блокчейны полностью защищены от несанкционированного доступа.** С этой целью криптовалюты используют надежные метки времени, которые подтверждают точное время существования данных в цепочке.

Поэтому неудивительно, что для работы этому процессу необходимы определенные компьютерные мощности, запредельные даже для крупнейших технологических компаний. Именно поэтому хакеры нашли способ облегчить данную задачу: они вторгаются на компьютеры других людей и используют их вычислительные ресурсы для майнинга криптовалют.

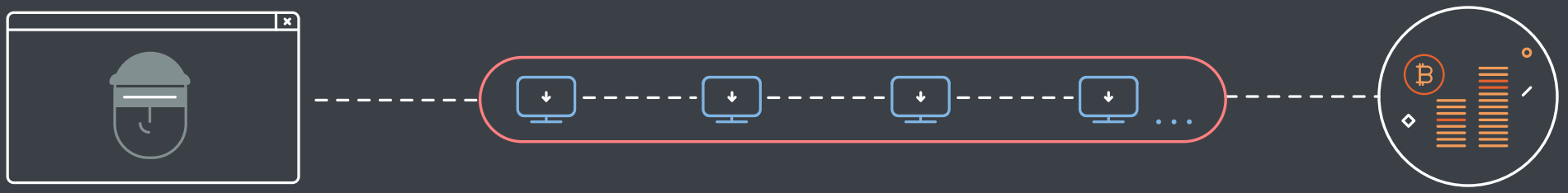
4. Работать на врага

Криптоджекинг (cryptojacking) - это несанкционированное использование устройства пользователя для майнинга криптовалют. Проще говоря, злоумышленники используют вредоносную программу, чтобы заполучить контроль над этими компьютерами, планшетами или смартфонами, и использовать часть их вычислительных мощностей для скрытой добычи криптовалют. **Вот как в конечном итоге Вы могли бы работать на "плохих парней", без ведома предоставляя им свои ресурсы (электроэнергию, компьютерные мощности).**

Как... Возможно, пользователь заметит, что его устройство стало работать медленнее, но при этом может не догадываться, что это связано с атакой для майнинга криптовалют. Одна из самых распространенных техник: **"получить" устройство пользователя при посещении им сайта, зараженным вредоносной программой для криптомайнинга**, что недавно произошло на YouTube.

Другой метод атаки состоит в **использовании функции онлайн-видео в Microsoft Word**, которая позволяет вставлять видео в документы без необходимости встраивать его или делать связку с ним. В этом случае злоумышленники используют эту функцию Word для вставки вредоносных скриптов, чтобы тайно использовать ресурсы процессора жертвы.

Зачем... Криптовалюты стали золотом XXI века. По этой причине в этом году мы наблюдаем существенный рост числа атак для майнинга криптовалют. Теперь, когда ИТ-службы и государственные органы внимательно следят за атаками шифровальщиков, кибер-преступники выбирают более безопасные способы заработка денег, и они, похоже, попали в новую многообещающую "золотую жилу" с незаконным использованием ИТ-ресурсов для криптомайнинга. **Чем больше вычислительных мощностей они смогут украсть, тем быстрее будет идти майнинг.** Это уже приводит к боям между различными хакерами, пытающимися получить контроль над максимально возможными ресурсами процессора пользователя.



Хосу Франко, Консультант по стратегии и технологиям в Panda Security, считает, что бум майнинга связан с тем, что "это простой способ делать деньги, и делать это весьма дешево.

Наборы для криптоджекинга можно купить в "теневом" Интернете всего за 30 баксов. Хакер может установить его, например, на 100 машинах, и все они будут постоянно приносить деньги, генерируя криптовалюту с очень низким риском. Более того, мы видим значительный рост легальных сайтов, зараженных скриптом CoinHive: т.е. теперь пользователю не требуется даже устанавливать программу для майнинга, т.к. скрипт будет работать до тех пор, пока пользователь активен на этом сайте. А в случае с шифровальщиками, хакер, возможно, сможет получить несколько жертв, которые заплатят лишь однажды".

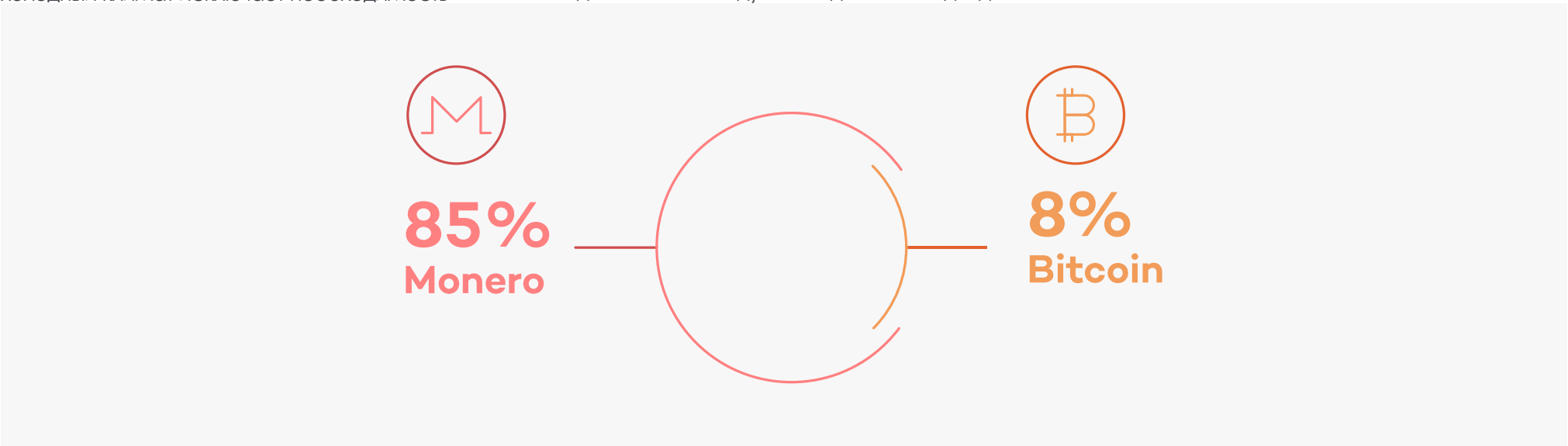
Как и в случае с шифровальщиками, **предприятия являются основной целью для злоумышленников в 2018 году**, т.к. если они смогут проникнуть в корпоративную сеть, они получат огромные вычислительные ресурсы.

Эксперты по информационной безопасности утверждают, что **преступники переходят от шифровальщиков к криптомайнингу, потому что он менее заметный и требует меньше ресурсов, чтобы избежать обнаружения.** С шифровальщиками нет никакой гарантии, что жертва заплатит, т.к. у нее может быть резервная копия файлов. А в случае с криптомайнингом больше шансов вернуть инвестированные деньги, и **он намного менее агрессивен**. Майнинг может осуществляться на любом устройстве, не ограничиваясь Windows, Mac или Linux, как в случае с шифровальщиками, при этом система жертвы будет продолжать работать, несмотря на атаку.

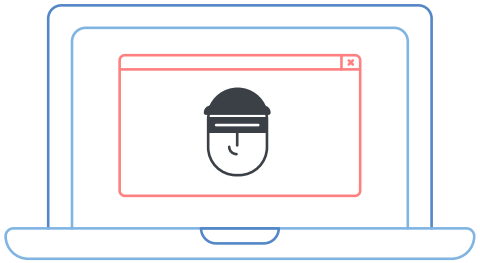
5. Какие криптовалюты нужны кибер-преступникам?

Самая известная и "старая" криптовалюта - это Биткоин. Впрочем, в наши дни майнинг данной криптовалюты для любителей практически невозможен, т.к. это требует так много ресурсов и специальных процессоров, что подобная деятельность возможна только для специализирующихся на этом компаний. Так много, что в последние годы Исландия отметилась всплеском числа компаний-майнеров Биткоина, т.к. в этой стране (особенно на фоне Евросоюза, США и Канады) дешевая электроэнергия, а ее холодный климат исключает необходимость тратить больше средств на охлаждение процессоров. По словам Иоганна Снорри Сигурбергссона, который работает в энергетической сфере Исландии, потребление энергии для майнинга биткоинов скоро превысит потребление энергии в домах.

Если кибер-преступники не могут легко генерировать биткоины с помощью криптоджекинга, так что именно им нужно? Ответ прост: это Monero - криптовалюта, созданная в 2014 году. Она идеально подходит для майнинговых операций, т.к. она не требует специального оборудования, она не использует так много вычислительных мощностей и она также обладает повышенной конфиденциальностью по сравнению с другими криптовалютами. Фактически, **85% атак криптоджекинга направлены на генерацию Monero, и лишь только 8% - для генерации биткоинов.**



6. Путь к Вашему компьютеру



Как и в случае со многими кибер-угрозами, которые мы наблюдаем в наши дни, криптоджекинг имеет **различные векторы атаки,** которые он использует для проникновения в компьютеры и ИТ-системы, чтобы начать использовать вычислительные мощности зараженных устройств.

Зараженные сайты

Одним из наиболее распространенных методов "захвата" процессора (CPU) является использование сайтов, которые тайно используют Интернет-соединения посетителей для майнинга, **обманывая посетителей этих сайтов в предоставлении их ресурсов третьим лицам.**

Рождение этой техники связано с **CoinHive** - компанией, которая в сентябре 2017 года предложила законную альтернативу рекламным объявлениям на сайтах. Впрочем, прошло совсем немного времени, как кибер-преступники стали использовать преимущества кода этой службы в своих злых умыслах. Эта техника подразумевает получение доступа к сайтам, встраивание кода CoinHive и извлечение криптовалюты, сгенерированной с помощью **процессоров** посетителей этих веб-сайтов.

Действительно, CoinHive - это наиболее широко распространенный скрипт для такого рода атак. **Исследование, проведенное экспертом по безопасности Троем Маршем,** обнаружило **50 000 сайтов со скриптом для криптоджекинга,** 80% из которых использовали CoinHive. Коды, подобные CoinHive, приносят примерно **250 000 долларов** каждый месяц...

Хакерам сильно облегчило жизнь то, что CoinHive не требовал разрешения пользователя на тех сайтах, где он был запущен. Это означало, что можно было осуществить атаку без ведома посетителя. Хотя сейчас компания запрашивает разрешение у пользователей, но кибер-преступники могли скопировать и изменить код под свои собственные нужды.

Это не есть нечто маргинальное: среди пострадавших сайтов оказались такие известные организации как ***The LA Times*** и целый ряд общественных организаций и правительственных органов, например, **Правительство Австралии.** На самом деле, для злоумышленников **чем популярнее сайт, тем лучше**, т.к. большее число посетителей означает больше вычислительных ресурсов, которые они могут заполучить, а значит, больше криптовалюты они смогут сгенерировать.

Именно это и произошло с YouTube, вторым в мире сайтом по посещаемости. В этом случае рекламная платформа **DoubleClick** стала жертвой атаки, которая спрятала код с криптоджекингом CoinHive в рекламу на YouTube.

Как такой код попадает на веб-сайты? Кибер-преступники уже давно используют уязвимости в системах управления сайтами для поражения сайтов. Одна из наиболее популярных уязвимостей для такого рода атак, которая использовалась уже сотни раз, находится в Drupal.

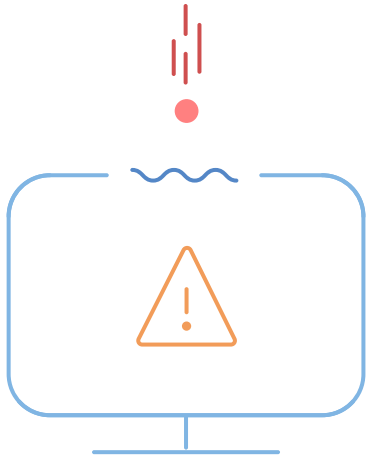
Особенно интересный случай - это использование уязвимости в **Apache Struts** – веб-приложении, которое уже вызвало очень много проблем. В этом случае используется вредоносная программа, которая при попадании на сайт ищет другие программы для майнинга, и если она находит их в системе, то деактивирует их для того, чтобы максимально использовать ресурсы процессора только для себя.

Уязвимости

Одна из самых популярных точек входа для криптоджекинга - это уязвимости. Мы уже видели несколько случаев уязвимых веб-сайтов, но злоумышленники также используют преимущества **уязвимостей в операционных системах для проникновения вредоносной программы на конечное устройство.**

Одна из наиболее проблематичных уязвимостей за последний год - это та, что влияет на Microsoft Server Message Block (SMB), а ее название - **EternalBlue.** Самое печально известное ее использование было в рамках глобальной атаки шифровальщика WannaCry. Однако через несколько месяцев после этой атаки **PandaLabs обнаружила еще одну эксплуатацию этой уязвимости:** безфайловый зловред WannaMine, используемый для майнинга Monero.

Эта уязвимость также использовалась для проникновения Adylkuzz в системы. Данная вредоносная программа, подобно WannaMine, использовалась для генерации Monero, и она поразила тысячи компьютеров во всем мире. На самом деле, считается, что от нее пострадало даже больше людей, чем от WannaCry.

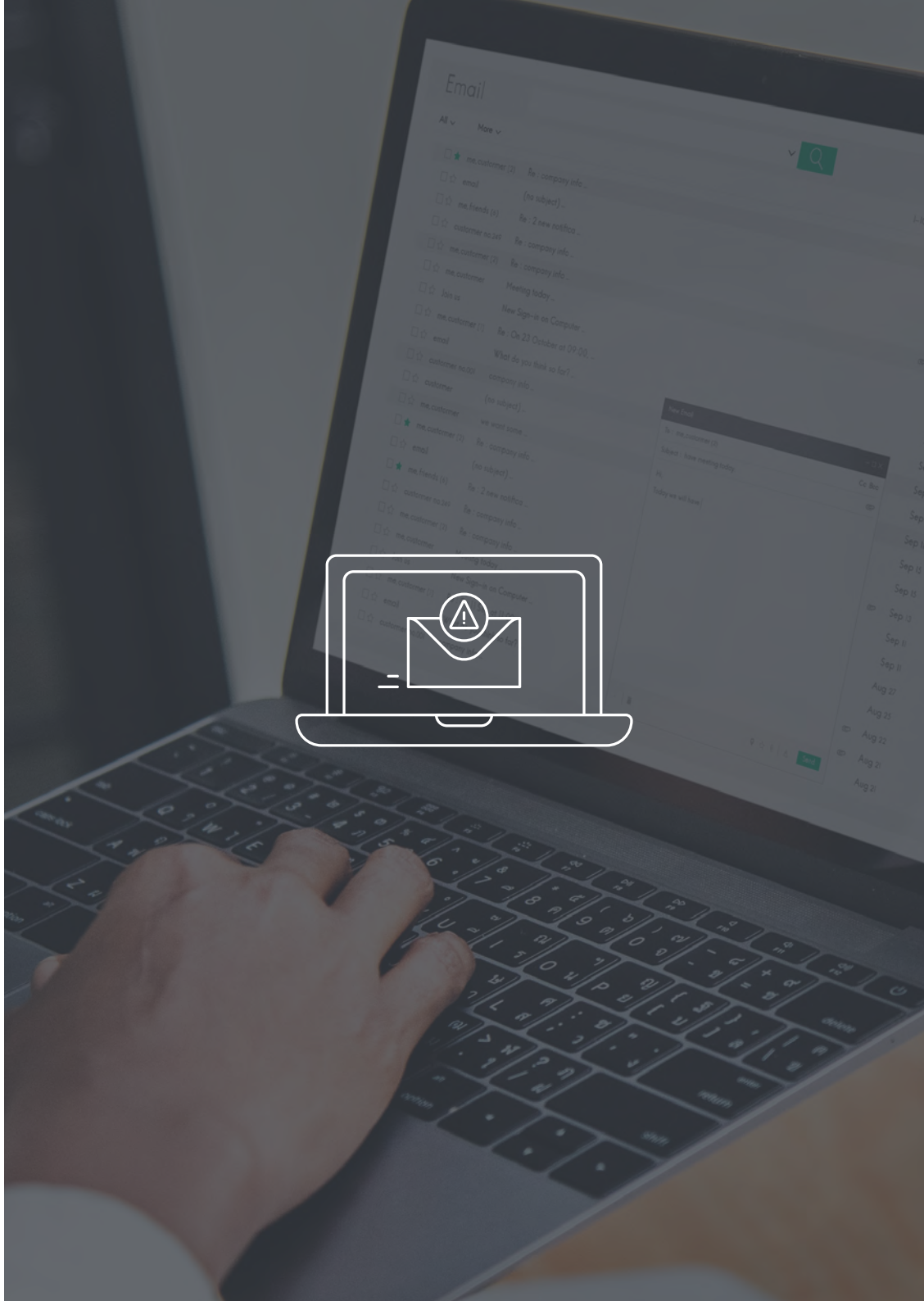


Фишинг

Свыше 90% вредоносных программ в мире передается через электронную почту. Возможно, поэтому неудивительно, что вредоносные программы для криптоджекинга не являются исключением.

Весьма популярный метод - это использование, казалось бы, легитимных документов. Один из таких примеров - это использование документов Word. Здесь злоумышленник размещает код для криптоджекинга в видео внутри документа Word, который затем вкладывается в электронное письмо. Как только документ открывается, запускается скрипт для криптоджекинга.

Еще одна особо опасная вредоносная программа - это WinstarNssmMiner. Она также используется при фишинге и на зараженных веб-сайтах. Попав в систему, она использует всю мощность компьютера для майнинга криптовалюты. Если ее обнаруживают или если кто-то пытается удалить ее из системы, то она нарушает работу зараженного компьютера.



Интернет вещей (IoT)

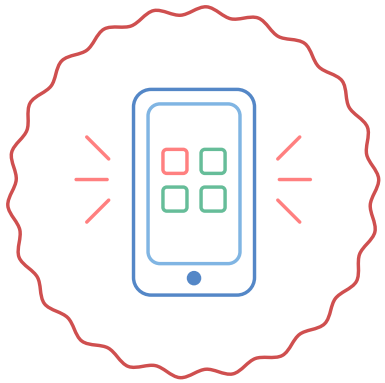
Широкое распространение получили мобильные устройства с подключением к Интернету, использование которых стало уже нормой. Поэтому стоит ожидать, что хакеры начали **использовать приложения, найденные на этих устройствах, для расширения своей криминальной деятельности.**

Одним из первых случаев, замеченных с IoT, был HiddenMiner, - вредоносная программа, которая проникала на мобильные устройства через приложения, загружаемые со сторонних (неофициальных) магазинов приложений. Одна из особенностей, которая делает ее столь опасной, связана с тем, что на старых версиях Android от нее практически невозможно избавиться. Более того, попав на устройство, она использует все его ресурсы, **полностью тормозя его работу или даже нарушая ее.**

На самом деле, были случаи, когда **вредоносной программой использовалось так много заряда устройства, что в результате этого зараженное устройство (в данном случае - смартфон) мог взорваться.**

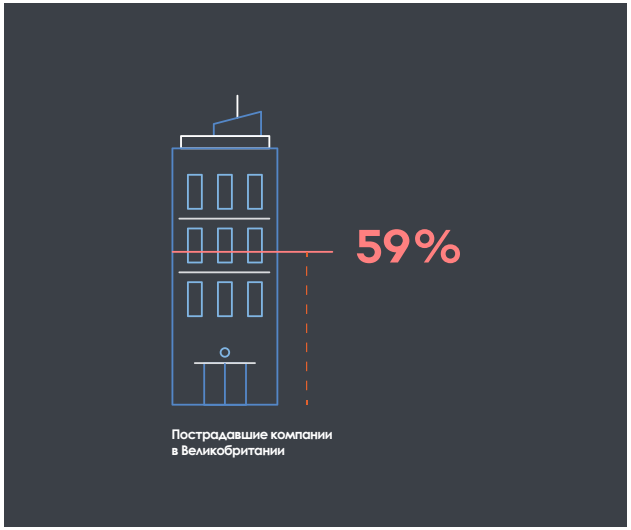
Но не только приложения, загруженные из ненадежных источников, мог вызывать проблемы. В начале этого года было установлено, что **несколько приложений, доступных в Google Play Store,** содержали вредоносные программы для криптоджекинга**.** Среди таких приложений были VPN, игры, и даже приложение, которое, по заверению ее авторов, осуществляло майнинг и жертвовало сгенерированную криптовалюту на благотворительность криптовалют.

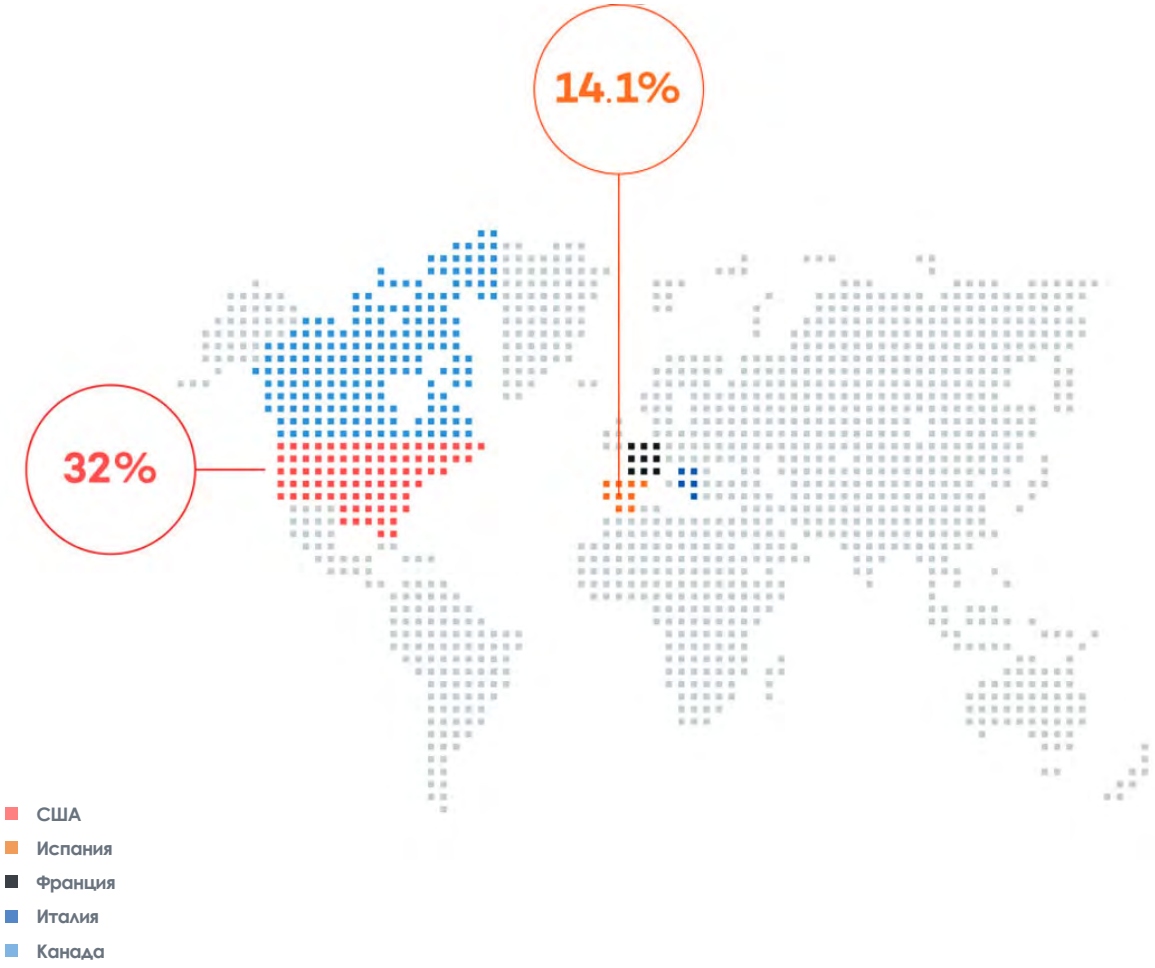
Другие IoT-устройства, такие как камеры безопасности, также не избежали атак криптоджекинга. Такие устройства особенно подвержены атакам, потому что, как правило, они имеют не такие строгие меры безопасности для своей защиты.



География криптоджекинга

Криптоджекинг - это глобальное явление, которое затронуло практически каждую страну в мире. Например, до 59% компаний в Великобритании когда-либо пострадали от такого рода атак. Но наиболее пострадавшие страны - это США (32% случаев), Испания (14,1% случаев), и затем Франция, Италия и Канада.



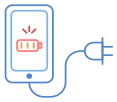


Медиа-центр Panda Security: "От года шифровальщиков к году криптоджекинга"

Отчет Malwarebytes: "Взгляд на глобальный феномен майнинга криптовалют", октябрь 2017

7.Какие могут быть последствия?

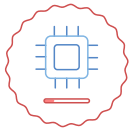
Хотя может показаться, что этот тип вредоносных программ является относительно безобидным, тем более, если учесть, что многие образцы разработаны таким образом, чтобы оставаться незамеченными и ограниченно использовать ресурсы процессора, тем не менее, как и все другие вредоносные программы, криптомайнеры представляют собой **серьезную угрозу для ИТ-безопасности.**



Рост потребления электричества. Одним из первых индикаторов заражения вредоносной программой для криптоджекинга является существенный рост потребления электроэнергии. По данным ряда источников, майнинг криптовалюты Monero использует примерно **332 миллиона КВт*час в год**, что сопоставимо с потреблением небольшой страны. Это одна из причин, по которой кибер-преступники ищут сторонние компьютеры для майнинга: необходимость сократить свои расходы.

Профессионализация данного типа атак такова, что некоторые типы вредоносных программ для криптоджекинга содержат код, который отключает режимы гибернации для того, чтобы продолжать майнинг, тем самым еще больше увеличивая потребление электроэнергии, т.к. **зараженные компьютеры круглосуточно осуществляют майнинг криптовалюты.**

Поэтому если вредоносная программа для криптоджекинга проникнет в Вашу корпоративную сеть, то достаточно быстро Вы заметите большое потребление электричества в Вашем счете за электроэнергию, потому как криптоджекинг будет задействовать для майнинга каждый Ваш компьютер так интенсивно, насколько это возможно.



Использование процессора. Цель криптоджекинга - использовать процессоры зараженных компьютеров для майнинга криптовалют, поэтому можно ожидать существенный рост уровня потребления Ваших вычислительных мощностей. Если несколько сотрудников сообщают о том, что их компьютеры стали медленно работать или вообще часто зависают, то, возможно, Вы столкнулись как раз со случаем криптоджекинга в Вашей компании.

Физический ущерб. Чрезмерное использование процессора приводит не только к замедлению в работе, но оно может привести даже к **поломке корпоративных компьютеров.** Если майнинг выполняется в течение продолжительного периода времени, то температура компьютеров или батарей мобильных устройств может достичь таких высоких значений, что они просто перестанут работать и могут даже сломаться.

Опасности для информационной безопасности компании. Если вредоносная программа для криптоджекинга проникла в ИТ-сеть Вашей компании, значит, **где-то существует "открытая дверь" в Вашу сеть.** А наличие такой "открытой двери" означает, что и другие типы угроз могут проникнуть в Вашу корпоративную сеть, поставив под угрозу работу и деятельность всей Вашей компании.

Изменение стратегии. Мы видели случаи с вредоносными программами для криптоджекинга, которые ранее использовались в качестве **шифровальщиков**. Возможен вариант, когда злоумышленник, видя, что криптоджекинг не столь выгоден, как ожидалось, вновь переключается на прямую атаку, чтобы подзаработать. Существуют даже такие вредоносные программы, которые **содержат обе атаки**, и в зависимости от характеристик компьютера они сами решают, запускать ли шифровальщика или осуществлять криптоджекинг.

Атака шифровальщика - это не единственное вторичное последствие, которое может произойти по воле хакера, который сумел проникнуть в Вашу корпоративную сеть с помощью вредоносной программы для криптоджекинга. Оказавшись в системе, **злоумышленник может получить доступ ко всему содержимому компьютера**, включая конфиденциальные корпоративные данные. Очень популярный среди кибер-преступников метод для заработка - это кража и продажа данных, будь то персональные данные клиентов, номера банковских карт или производственные ноу-хау.

Возможен вариант, когда кибер-преступник, получив доступ к ИТ-системе для атаки криптоджекинга, **зарабатывает на "сдаче в аренду" этого доступа другим кибер-преступникам**. Так что они могут использовать Вашу систему по своему усмотрению.

8. Как я могу защитить свою компанию от криптоджекинга?

Эксперты PandaLabs по ИБ утверждают, что защититься от данной угрозы можно точно так же, как и от любых других типов вредоносных программы, т.к. криптомайнинг выполняется при использовании вредоносного кода, запущенного на Вашем компьютере.

Таким образом, основной совет: необходимо использовать решение безопасности с опциями расширенной защиты, такое как Panda Adaptive Defense 360, и не запускать и не скачивать неизвестные файлы.

Кроме того, для эффективной защиты от атаки криптомайнинга, очень важно соблюдать следующие меры безопасности:

Проводите периодические оценки рисков для выявления уязвимостей. Panda Patch Management выполняет автоматический поиск необходимых патчей для поддержания безопасности устройств в Вашей сети, назначая приоритет наиболее срочным обновлениям. По данным аналитиков Gartner, внедрение соответствующих политик применения патчей позволяет Вам сократить до 80% поверхность атак при использовании уязвимостей.

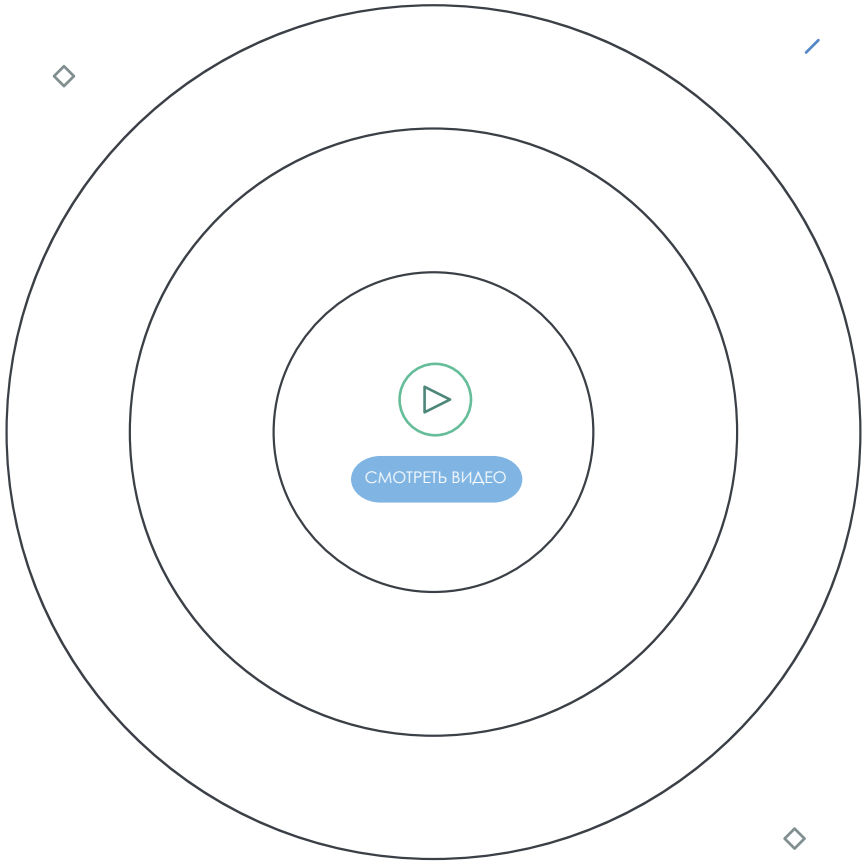
Осторожнее с Вашим браузером. Если Вы подозреваете, что криптоджекинг проникает через веб-сайты, установите плагины для блокировки этих сайтов в Вашем браузере или ограничьте доступ к ним с помощью опций URL-фильтрации.

Регулярно обновляйте все системы и устройства в Вашей компании, а также удалите все неиспользуемое ПО.

Анализируйте Ваши ресурсы. Все операционные системы имеют инструмент, похожий на Системный монитор для анализа ресурсов, потребляемых компьютерами Вашей компании. Следите за этим, чтобы убедиться в отсутствии необычной активности.

Тщательно исследуйте любые ИТ-проблемы, связанные с необычной работой процессоров. Если несколько сотрудников сообщают, что их компьютеры стали работать медленнее или постоянно зависают, то, возможно, Вы столкнулись со случаем криптоджекинга.

Создайте в компании среду для безопасного просмотра сайтов: активируйте контроль доступа к сайтам, доступный в решениях с опциями расширенной безопасности, и блокируйте сайты для криптомайнинга - это лучший способ защиты устройств и ресурсов Вашей компании.



Panda Adaptive Defense 360

Неограниченная видимость
Абсолютный контроль

Эти действия должны сопровождаться внедрением решения безопасности с опциями расширенной защиты, которое предоставляет такие ключевые функции, как детальная видимость всей активности на каждом конечном устройстве и полный контроль над всеми запущенными процессами. Все это предлагает решение безопасности **Panda Adaptive Defense 360** компании Panda Security, которое предназначено для защиты всех компьютеров в Вашей компании от всех типов кибер-угроз, будь то классические угрозы или новые и сложные атаки.

Следуйте нашим советам, чтобы криптоджекинг не подорвал репутацию Вашей компании и не поставил под угрозу всю ее деятельность и даже существование.

Panda Adaptive Defense 360

Неограниченная видимость. Абсолютный контроль

Подробнее:

cloudav.ru/enterprise/solutions/adaptive-defense-360/

Давайте обсудим:

+7 495 105 94 51

www.cloudav.ru

panda