KASPERSKY lab

DUQU 2.0:

ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

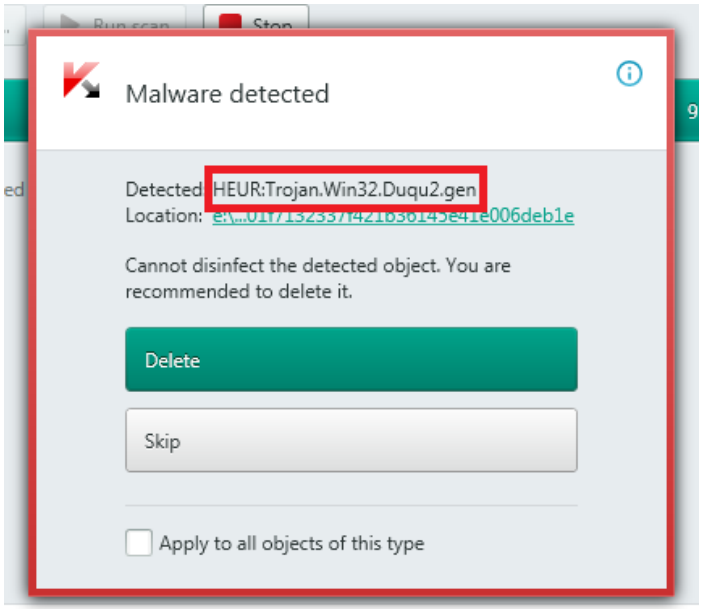
Общая информация

Ранней весной этого года «Лаборатория Касперского» зафиксировала кибервторжение в свою корпоративную сеть. В ходе последовавшего за этим расследования мы обнаружили новую вредоносную платформу, имеющую непосредственное отношение к одной из самых сложных и загадочных кампаний кибершпионажа – Duqu. Есть основания считать, что эта кампания спонсируется на государственном уровне.

Duqu – сложная платформа для кибершпионажа, впервые обнаруженная в 2011 году компанией CrisysLab и изученная «Лабораторией Касперского». Этот зловред ведет себя в системе как бэкдор, помогая атакующим красть конфиденциальную информацию. 4 года назад Duqu был найден в Венгрии, Австрии, Индонезии, Великобритании, Судане и Иране. Некоторые свидетельства указывают на то, что Duqu был создан для шпионажа за иранской ядерной программой, а также для заражения сетей органов сертификации с целью кражи цифровых сертификатов, которые впоследствии использовались для подписи вредоносных файлов.

«Лаборатория Касперского» полагает, что атакующие были уверены в незаметности своих действий. Они использовали уникальные и ранее не встречавшиеся инструменты и практически не оставляли следов в системе. Атака осуществлялась при помощи эксплойтов, использовавших уязвимости нулевого дня в ОС Windows, а дополнительное вредоносное ПО доставлялось в атакованные системы под видом Microsoft Software Installers (MSI) – установочных файлов, используемых системными администраторами для инсталляции ПО на компьютеры в удаленном режиме. Вредоносное ПО не создавало и не модифицировало какие-либо дисковые файлы или системные настройки, что затрудняло детектирование атаки. Способ мышления и тактика группы Duqu 2.0 на целое поколение опережают любые кибератаки и вредоносные кампании, встречавшиеся ранее. Но благодаря нашим технологиям и первоклассным специалистам, атака была обнаружена.

Для нейтрализации этой угрозы «Лаборатория Касперского» публикует индикаторы заражения, а также предлагает свою помощь всем заинтересованным организациям. Кроме того, необходимые функции для защиты от Duqu 2.0 были добавлены в продукты компании.



Более подробную информацию о Duqu 2.0 можно найти в аналитическом отчете «Лаборатории Касперского».

На кого нацелена кампания?

«Лаборатория Касперского» была не единственной целью атакующих – эксперты компании обнаружили других жертв в западных, ближневосточных и азиатских странах. Среди наиболее заметных мишеней новой кампании Duqu в 2014-2015 годах стали площадки для переговоров по иранской ядерной программе «Группы 5+1» и мероприятий, посвященных 70-й годовщине освобождения узников Освенцима.

«Лаборатория Касперского» отмечает, что представленная информация – это предварительные результаты расследования. Без сомнения, географический охват и список жертв этой атаки гораздо шире. Однако исходя из тех данных, которыми компания располагает уже сейчас, ясно, что Duqu 2.0 использовался для атак на высокопоставленных жертв, а атакующие руководствовались, в том числе, геополитическими интересами.

Каково значение этого открытия?

Способ мышления и тактика группы Duqu 2.0 на целое поколение опережают любые кибератаки и вредоносные кампании, встречавшиеся ранее. Уровень сложности их операции превосходит даже деятельность группы Equation, на сегодняшний день считающейся самым сильным игроком в мире киберугроз.

Equation всегда использовала какую-либо форму закрепления в атакованной системе, принимая риск возможного обнаружения. Вредоносная платформа Duqu 2.0 сконструирована таким образом, что не нуждается в закреплении – она почти полностью базируется в памяти операционной системы. Это означает, что создатели Duqu 2.0 уверены в том, что всегда смогут найти способ поддержать работу платформы, даже если атакованный ПК будет перезагружен, и вредоносное ПО исчезнет из памяти.

Такой подход гораздо сложнее с технической точки зрения. Он также демонстрирует, что создатели Duqu 2.0 были достаточно уверены в своих силах, чтобы подготовить и поддерживать кибершпионскую операцию исключительно в памяти операционной системы без применения каких-либо механизмов закрепления.

Кроме того, группа Equation использовала один и тот же алгоритм шифрования с едиными специфическими функциями во всем своем вредоносном ПО, начиная с Equation Vector в 1999 году и заканчивая GrayFish в 2013-м. В случае с Duqu 2.0 шифрование всегда разное и с разными алгоритмами.

Именно эти особенности делают Duqu 2.0 самой сложной и серьезной угрозой из ныне выявленных.

Каковы последствия этого кибервторжения для «Лаборатории Касперского»?

«Лаборатория Касперского» провела расследование инцидента. Как показал первичный анализ, главной задачей атакующих было получение информации о технологиях, исследованиях и внутренних операциях «Лаборатории Касперского». Атакующие проявляли интерес к интеллектуальной собственности и разработкам компании для обнаружения и анализа таргетированных атак и кибершпионажа, а также к информации о текущих

расследованиях, проводимых «Лабораторией Касперского». Организаторы атаки были особенно заинтересованы в деталях разработки таких продуктов и сервисов, как безопасная операционная система «Лаборатории Касперского», Kaspersky Fraud Prevention, Kaspersky Security Network и решение для защиты от сложных целевых атак и кибершпионажа. Помимо попыток кражи интеллектуальной собственности, никакой другой вредоносной активности, в том числе вмешательства в процессы или системы, в корпоративной сети компании зафиксировано не было.

Атакующие, возможно, были наслышаны о репутации компании как эксперта в вопросах детектирования и нейтрализации сложных кибератак, поскольку они пытались найти способы сделать свои будущие атаки недетектируемыми.

Информация, доступ к которой могли получить организаторы атаки, не является критической для функционирования продуктов компании. Более того, глубокие знания об этой атаке и ее методах позволят «Лаборатории Касперского» повысить эффективность своих защитных решений.

Какое влияние эта атака оказала на клиентов «Лаборатории Касперского»?

«Лаборатория Касперского» уверена, что ее клиенты и партнеры в безопасности, поскольку атака не оказала влияния на продукты, технологии и сервисы компании. Целью атакующих были не данные пользователей, а доступ к интеллектуальной собственности «Лаборатории Касперского» и ее разработкам, предназначенным для детектирования и анализа сложных целевых атак и кибершпионажа, а также информация о текущих расследованиях, проводимых компанией.

«Лаборатория Касперского» заверяет своих клиентов и партнеров, что компания продолжит бороться со всеми кибератаками, независимо от того, кто за ними стоит и на кого они нацелены. «Лаборатория Касперского» считает своей важнейшей задачей сохранить доверие своих пользователей. Компания уверена, что меры, которые она приняла, не только помогут нейтрализовать эту угрозу, но также позволят избежать подобных инцидентов в будущем.

Как вы обнаружили вторжение в корпоративную сеть?

Атака была обнаружена ранней весной этого года. В ходе тестирования прототипа решения для защиты от подобных угроз – сложных целевых атак и кибершпионажа – были замечены признаки таргетированной атаки на корпоративную сеть. Затем последовало внутреннее расследование, в рамках которого эксперты, антивирусные аналитики и реверс-инженеры «Лаборатории Касперского» тщательно изучали эту необычную атаку.

Каковы причины полагать, что эта атака спонсируется на государственном уровне?

Разработка и организация такой хорошо подготовленной вредоносной кампании обходится крайне дорого, а также требует ресурсов, значительно превосходящих те, которыми располагают обычные киберпреступники. Стоимость разработки и поддержки подобной вредоносной платформы огромна: по оценкам экспертов «Лаборатории Касперского», она может достигать 50 миллионов долларов. Однако что впечатляет больше, так это то, что вся эта вредоносная платформа базируется только на уязвимостях нулевого дня. Следовательно, если

нет уязвимости, позволяющей вредоносному ПО работать в режиме ядра, оно не сработает. Исходя из этого можно предположить, что атакующие уверены в том, что в случае закрытия одной уязвимости они смогут воспользоваться другой. Иначе они не стали бы создавать платформу, целиком и полностью зависимую от уязвимостей нулевого дня.

В действиях группы Duqu 2.0 не было замечено стремления извлечь финансовую выгоду при помощи вредоносного ПО.

Использование многочисленных эксплойтов под уязвимости нулевого дня, а также сложные техники проникновения в корпоративную сеть также являются признаками того, что эта атака имеет поддержку на государственном уровне.

Почему «Лаборатория Касперского» стала целью атаки наравне с высокопоставленными государственными деятелями?

Атака на «Лабораторию Касперского» наглядно демонстрирует, как быстро набирает обороты гонка кибервооружений. Когда компании RSA и Bit9 стали жертвами таргетированных атак китайского происхождения в 2011 и 2013 годах соответственно, такие инциденты все еще были редкими случаями. В целом атакующие идут на большой риск, вторгаясь в сети секьюрити-компаний, поскольку они могут быть пойманы и опознаны.

Почему «Лаборатория Касперского» подверглась этой атаке, до сих пор точно не ясно. Однако мы предполагаем, что основной целью атакующих было получение доступа к информации о новейших защитных технологиях, разрабатываемых компанией.

Значит ли это, что от вредоносного ПО «государственного уровня» невозможно защититься?

Это не так. Разумеется, традиционный подход, применяемый для защиты рабочих станций, может не сработать в случае с вредоносным ПО, созданным при поддержке государства. Мы поняли это некоторое время назад и именно поэтому начали разрабатывать новые технологии, в частности специальное решение для противодействия сложным целевым атакам и кибершпионажу. Именно во время тестирования прототипа этого решения мы и обнаружили Duqu 2.0.

Целевые атаки бывают совершенно разными с точки зрения умений их организаторов и используемых ресурсов. К сожалению, некоторые такие кампании, например, Stuxnet, Flame и Equation, могут оставаться незамеченными в течение нескольких лет. Однако в долгосрочной перспективе секьюрити-компании все равно раскроют эти операции, поскольку идеального кода (в том числе и вредоносного) не существует.

Нанесен ли «Лаборатории Касперского» репутационный ущерб?

До сих пор распространено убеждение, что обнародование факта кибератаки нанесет, в первую очередь, ущерб репутации компании. Однако это опасное и обманчивое заблуждение, поскольку в современных условиях любая компания может стать жертвой сложной и хорошо спланированной целевой атаки. Чем опасна позиция сокрытия атаки? Прежде всего тем, что это играет на руку киберпреступникам и атакующим с господдержкой: они будут знать, что их вредоносная деятельность не предается огласке и не порицается, а информация о способах предотвращения подобных атак не получает широкого распространения.

Сообщая о кибервторжении в нашу сеть и публикуя подробный технический анализ Duqu 2.0, мы хотим подать пример другим компаниям, чтобы они тоже открыто рассказывали о кибератаках на их сети. Наш случай показывает, что даже ведущий разработчик защитных решений может стать мишенью хорошо подготовленной кибератаки. Не стоит забывать, что государственные спецслужбы имеют многомиллиардные бюджеты и сотни тысяч сотрудников. Мы можем бороться с подобными инцидентами, предавая их огласке, будучи открытыми и прозрачными.

«Лаборатория Касперского» является последовательным сторонником ответственного поведения в плане раскрытия кибератак. Мы уверены, что замалчивание киберинцидентов ведет к ограничению доступности информации, осведомленности и, как следствие, снижению общего уровня защищенности в мире. Мы уверены, что каждая атакованная компания должна делиться максимумом сведений о выявленном инциденте – это даст возможность другим компаниям усилить свою оборону.

Является ли этот инцидент первым случаем атаки, спонсируемой на государственном уровне, на секьюрити-компанию?

К сожалению, это не первый случай. Ранее атакам «государственного уровня» подвергались компании RSA Security и Bit9. Организаторы этих атак проникли в корпоративные сети секьюрити-компаний с «утилитарной целью» усовершенствовать свои кибервозможности.

Что было сделано для предотвращения подобных атак в будущем?

Мы предприняли достаточно радикальные меры для того, чтобы усовершенствовать свою IT-инфраструктуру и защитить наши разработки и наших клиентов. Мы делаем все возможное для того, чтобы организация любых атак на нас была настолько сложной и дорогой, насколько это возможно.

Какую стратегию противодействия этой угрозе вы рекомендуете?

Мы рекомендуем придерживаться четырех простых, но крайне эффективных мер:

1. Убедитесь, что вы поставили защитные продукты «Лаборатории Касперского» на все имеющиеся у вас машины, включая серверы, прокси-серверы и любые компьютеры.
2. Обновите Windows до последней версии – используйте для этого Microsoft Windows Update. Убедитесь, что у вас установлен пакет обновлений Microsoft от 9 июня 2015 года.
3. Перезапустите операционную систему на всех компьютерах одновременно, например, сымитировав перебой в электроснабжении. Крайне важно перезагрузить все системы в одно и то же время, иначе вредоносное ПО может выжить на одной из машин и впоследствии снова заразить все компьютеры.
4. Поменяйте все пароли.

Следующие методы позволят минимизировать риск, связанный с атаками Duqu 2.0:

- Регулярно устанавливайте обновления и перезапускайте системы на всех машинах в сети, включая контроллеры доменов. Эти действия позволяют удалять из памяти активное вредоносное ПО.
- Убедитесь, что все ваши северы работают на 64-битной версии Windows. Это вынуждает атакующих использовать подписанные драйверы для механизмов закрепления присутствия.
- Регулярно (раз в 1-2 месяца) меняйте пароли и используйте сильные комбинации, в которых более 20 символов. Удалите старые LM хеши.

Более продвинутым пользователям мы предлагаем применять правила Yara, а также использовать инструмент, помогающий обнаруживать заражение в дампе памяти и журнале событий.

Кроме того, вы можете воспользоваться стратегиями, предложенными в статье «Как избежать 85% всех целевых атак с помощью четырех простых стратегий».

К кому обращаться в случае, если я/моя компания стала жертвой кампании Duqu 2.0?

Если у вас есть вопросы, или вы хотите поделиться информацией об этой угрозе, пишите, пожалуйста, по адресу intelreports@kaspersky.com. Спасибо!