Символ года и безопасности

Без преувеличения можно сказать, что шифровальщики (они же энкодеры или вымогатели) стали одним из главных явлений уходящего года

текст Вячеслав Медведев, ведущий аналитик отдела развития ООО «Доктор Веб»

Эпидемия энкодеров показала неготовность компаний и частных пользователей к защите от современных угроз. Практически каждую неделю в новостях появляются описания очередного представителя этих популярнейших среди злоумышленников вредоносных программ. Список названий, которые стали известны как читателям новостей, так и пострадавшим, очень велик: Cryptowall, Chimera, CoinVault, Bitcryptor, Cryptolocker. Он далеко не полон (кстати, компания «Доктор Веб» для всех шифровальщиков использует наименование Trojan.Encoder. Например, под названием Cryptowall различают четыре варианта Trojan.Encoder — 741, 453, 398, 293).

КОГДА НЕ СПАСАЕТ «ГРУДЬ В КРЕСТАХ»

Оборотной стороной таких публикаций стало подтверждение (для читателей новостей, естественно) старого мифа о якобы немногочисленности вредоносных программ. Конечно, ведь антивирусные вендоры должны уведомлять пользователей обо всех новых угрозах! На самом деле это далеко не так. Если, например, зайти на информационный ресурс нашей компании о вредоносных программах, попавших в вирусные базы, то можно увидеть, что в базы добавляется информация о нескольких десятках шифровальщиков. Ежедневно — и это не считая огромного количества других типов вредоносных программ, остающихся в тени звезд новостей. Эти программы, как и шифровальщики, до добавления в базу не распознаются системой защиты (точнее, конечно, не распознаются компонентами антивируса, работающими на основе знаний из вирусной базы, о поведенческом анализаторе разговор особый).

Почему же шифровальщики стали такой глобальной угрозой? Ведь вопрос создания антивирусной системы защиты для подавляющего большинства компаний давно закрыт и не является насущным – на большинстве мероприятий обсуждаются совсем иные проблемы. Проблема защиты от вирусов не становится больше центром внимания и для руководства компаний, и для системных администраторов. Вопрос немного философский, поэтому поговорим о том, почему вредоносные программы вообще стали в последнее время головной болью для многих — несмотря на то, что системы защиты строятся на основе годами проверенных принципов.

Современные злоумышленники, создавая вредоносные программы, не хотят оставить свое имя в истории. Они хотят заработать. Логично, что рассчитывать на то, что в атакуемой системе не установлен антивирус, было бы как минимум наивно. Поэтому для того, чтобы начать работать, вредоносная программа должна пройти через сито защиты. И это вполне реально, к сожалению.

Дело в том, что в подавляющем большинстве случаев антивирусная система защиты состоит из одного только антивируса, а пользователи работают с правами администраторов, используют (практически все) один и тот же

набор программ и не любят перезагружаться для установки обновлений. Причем антивирус обычно устанавливается с настройками по умолчанию (без настройки белого списка разрешенных к использованию программ, без использования проактивной защиты и т.д.). Соответственно, злоумышленникам достаточно установить антивирусы по умолчанию и тестировать на них свои разработки. Вредоносное ПО, которое пройдет через их тесты, пройдет и через защиту компаний, как нож сквозь масло.

Системы защиты, рассчитанные на противодействие хакерам, единственной целью которых являлась слава, не могут противостоять криминальным группировкам, имеющим в своем распоряжении все возможности черного рынка и поставившим грабеж на промышленную основу.

ЕСТЬ ЛИ ВЫХОД?

Сложившаяся ситуация мгновенно обесценила все системы тестирования антивирусов (кроме систем самозащиты и лечения активных заражений — но это особый и редко встречающийся вид тестирования). Даже если «грудь в крестах», что толку, если победитель тестирования гарантированно пропустит специально разработанный вирус? Но этого никто не заметил. Выбор антивирусов (что в большинстве случаев равноценно созданию антивирусной системы защиты) все так же происходит на основе результатов популярных тестов.

Нужны инициативы по разработке рекомендаций по усовершенствованию систем защиты, основательная переработка курсов для системных администраторов и специалистов по безопасности – но вместо этого широко распространились призывы к соглашательству – от статьи с названием «Мы решили платить» до призывов платить из уст представителя ФБР США Джозефа Бонаволонта: «Честно говоря, мы часто советуем обратившимся просто заплатить выкуп за расшифровку. Опыт показывает, что специалистам ФБР приходится тратить огромные усилия в попытках расшифровать заблокированные файлы без всякой гарантии успеха». И информацию о необходимости платить с удовольствием распространяют СМИ. Кому это выгодно? И почему информация о контрнаступлениях антивирусных вендоров куда менее известна?

Злоумышленники стараются сделать необнаруживаемое ПО. Можно ли усложнить им жизнь? Да, если антивирус развивает технологии антивирусного ядра. Создать программу, которая не будет обнаруживаться антивирусом, сложно. Куда проще зашифровать уже имеющегося троянца или обработать его упаковщиком так, чтобы получился файл с никому не известным форматом. Технология Dr.Web Fly-Code позволяет антивирусу находить вредоносные файлы даже в этом случае. Пользователи других продуктов остаются без защиты до загрузки обновления, содержащего информацию о новом троянце (точнее, об упакованном файле) – а это, по статистике, в среднем два часа без защиты. Fly-Code фактически является водоразделом между антивирусами, для которых создавать вредоносные программы выгодно, и продуктами, обойти которые сложно.

А что делать, если вредоносная программа может обойти антивирус (напоминаем – установленный с настройками по умолчанию)?

Необходимо переходить от антивируса к антивирусной системе защиты. Работать только под ограниченными правами (да, и это тоже антивирусная защита), ограничить и жестко контролировать список установленных и пытающихся запуститься программ, ограничить права доступа к Интернету и ресурсам локальной сети. В обязательном порядке использовать резервное копирование. И этот список рекомендаций можно продолжать – в зависимости от списка актуальных угроз.

ВАЖНОСТЬ СИСТЕМНОГО ПОДХОДА

Все эти меры по отдельности защиты не дают. Например, многие рассматривают резервное копирование в качестве идеального решения от потери данных. Немало в сети Интернет и ресурсов, описывающих настройку теневого копирования именно для противодействия шифровальщикам. Но создатели вредоносных программ определенно тоже читают такие рекомендации – и, например, Trojan.Encoder.1064 (он же AlphaCrypt) первым делом удаляет теневые копии. Шифровать данные по сети, копировать их на сменные носители – тоже не панацея, поскольку большинство шифровальщиков обрабатывают все доступные ресурсы. А учитывая, что далеко не все шифровальщики требуют выкуп в день заражения и могут работать месяцами – очень велик шанс, что все резервные копии содержат троянца и не содержат незашифрованных файлов.

Современный антивирус не равен файловому антивирусу девяностых годов. Проверка входящего и исходящего трафика, ограничение прав доступа к ресурсам (включая сменные носители), резервное копирование – все это компоненты современного антивируса. И, конечно же, поведенческий анализатор. Что делать, если вредоносная программа неизвестна вирусным базам? Контролировать запросы запущенных программ к различным ресурсам и анализировать, что делает тот или иной процесс. При этом здесь также возможно два пути. Можно сравнивать поведение процесса с известными моделями поведения популярных программ. Это требует базы данных признаков всех программ мира и не дает гарантии для неизвестного процесса (к тому же эта база требует постоянного обновления из-за контролируемых программ, что в закрытых сетях может привести к рассогласованию поведения обновленной программы и мнения о ней системы защиты). А можно сравнивать поведение процесса с моделями поведения вредоносных программ, что в случае отсутствия базы данных признаков всех программ мира дает еще и рост скорости проверки.

Но даже лучший поведенческий анализатор начинает свой анализ после начала работы программы. А это приводит к тому, что шифровальщик до своего обнаружения успевает зашифровать до десятка файлов. Что делать? Платить выкуп?

Очень важна готовность к возникновению вирусозависимого компьютерного инцидента. На фоне новостей

об успехах злоумышленников немногие знают, что не все шифровальщики так хороши, как хотелось бы их создателям. Вероятность расшифровки составляет от 10 до 90%. Компания «Доктор Веб» только за последний месяц объявила о возможности расшифровки двух представителей Trojan.Encoder — в том числе Trojan.Encoder.2843, известного также под именем Vault.

К сожалению, большинство пострадавших к моменту инцидента не знают, что им нужно делать. Обычно в подобных случаях в службу технической поддержки приходит невнятный запрос с сообщением «нас зашифровали». В лучшем случае прикладывают один файл. До момента получения техподдержкой всей необходимой информации (или неполучения: многие первым делом запускают штатный антивирусный сканер или скачивают Dr.Web CureIt!, который находит и уничтожает троянца) пострадавшие успевают обменяться со специалистами более чем десятком сообщений. А это время и деньги пострадавшей компании. Для повышения шансов на расшифровку пострадавших файлов важно прислать специалистам не один, а три-пять файлов разных типов (pdf, doc и т.д.), а также письмо с требованием выкупа (при наличии), описание процесса заражения, тело троянца (подумайте, у всех ли по умолчанию вредоносная программа при обнаружении перемещается в карантин, а не уничтожается?). Должно быть как можно больше информации для анализа. И даже в этом случае служба технической поддержки не всегда может отреагировать мгновенно: во время эпидемии количество запросов о расшифровке многократно возрастает.

Для восстановления информации прежде всего нужна информация, и преступники об этом тоже знают. Поэтому зараженный компьютер нельзя выключать (для преступника не составляет особого труда установить на зараженном компьютере программу для уничтожения информации на жестком диске или в расшаренных папках). Но и продолжать работать на зараженном компьютере тоже нельзя, ведь это модификация места совершения инцидента безопасности. К потере информации может привести даже загрузка с внешнего носителя. Поэтому остается только варварский способ – выдернуть вилку из сети до получения рекомендаций.

Грядут Новый год и зимние каникулы – время, когда системные администраторы и специалисты в области безопасности отдыхают, а злоумышленники традиционно выходят на охоту. Вы и ваша дежурная смена знаете, кому звонить в случае возникновения компьютерного инцидента, как собрать информацию и как правильно составить заявление в полицию? NBJ