Текст · 3 апреля 2024, 11:50
Давид Френкель,

Выгоревший программист и токсичные коллеги. Как не случилась одна из самых масштабных хакерских атак в мире

Злоумышленники едва не получили возможность контролировать большинство серверов в мире. Для этого им понадобилось найти выгоревшего создателя небольшой программы для сжатия данных *xz* — и затравить его токсичными комментариями о некачественной и медленной работе.

Краткое содержание

Что мы знаем о попытке одной из самых масштабных хакерских атак в мире. Коротко

- Неизвестные пока хакеры едва не получили контроль над 80% серверов в мире.
- Для атаки использовался широко распространенный пакет *xz* — набор программ для сжатия данных, который много лет обновлял разработчик-энтузиаст Лассе Коллин.
- Готовили атаку около двух лет.
- Коллин передал контроль над пакетом после того, как хакеры затравили его в сети за медлительность в работе; он думал, что отдает проект в руки более мотивированных разработчиков.
- Атаку раскрыли в самом начале, когда уязвимость еще не успела распространиться достаточно широко.

- Обнаружили ее случайно — после того, как программист Андрес Фройнд заметил, что подключение к его серверу стало происходить на полсекунды дольше обычного.
- Кто стоит за атакой, пока неясно: хакер выдавал себя за китайца, но, вероятнее всего, работал по восточноевропейскому времени (и отмечал католическое Рождество и Новый год).

---

28 марта программист Андрес Фройнд, один из разработчиков популярнейшей системы управления базами данных *Postgres* и сотрудник *Microsoft*, заметил, что его компьютер работает чуть медленнее, чем обычно. Если быть точным, подключение к серверу занимало на полсекунды дольше. На компьютере Фройнда стояла самая свежая версия *Debian*[1].

Андрес решил разобраться в этом и обнаружил, что необычно много ресурсов его компьютера тратится на *sshd* — это одна из самых распространенных[2] программ для подключения к серверу через интернет.

Он вспомнил, что недавно читал о других странностях в последних версиях *Debian*. Андрес начал изучать изменения в этих версиях — и обнаружил хакерскую атаку, которая готовилась больше двух лет и могла бы взломать миллионы серверов по всему миру.

Что такое xz и почему почти все им пользуются

Вскоре Андрес Фройнд обнаружил, что в свежих версиях пакета *xz* [3]— эта программа входит в стандартную комплектацию *Debian* — появился бэкдор. Бэкдор — это заложенная разработчиком уязвимость, которая позволяет обойти механизмы защиты и получить доступ к компьютеру. Версия с бэкдором начала распространяться в феврале 2024 года.

Xz — это набор программ для сжатия или распаковки данных, использующий алгоритм *LZMA*[4]. В определенных ситуациях этот алгоритм работает значительно эффективнее, чем другие методы сжатия. Пользователям *Windows* может быть знакома программа *7-Zip*[5]. Автор этой программы Игорь Павлов и придумал алгоритм *LZMA*. По сути, *xz* — это версия *7-Zip* для операционных систем на базе *Linux*.

Разработал *xz* программист и «шифропанк» Лассе Коллин. В 2005 году он хотел сделать свою версию *Linux*[6], которая могла бы поместиться на компакт-диск емкостью в 700 мегабайт.

Сборка *Linux* от Коллина не стала популярной, но в процессе работы над ней он создал набор удобных инструментов для сжатия и распаковки данных — как раз на основе алгоритма Игоря Павлова. Этот набор — *xz utils* — оказался настолько удачным, что вошел в стандартную комплектацию большинства популярных дистрибутивов *Linux*, в том числе *Debian*-

, *Fedora*, *Ubuntu* и *Gentoo*. Код *xz* даже входит в ядро операционной системы *Linux*.

Кроме того, *xz* начали использовать в работе других ключевых программ, например, в уже упомянутой выше программе для подключения к серверам *sshd*.

Подготовка к атаке: как затравить разработчика

Код *xz* был опубликован на сервисе *GitHub*, это крупнейшее сообщество разработчиков программ с открытым исходным кодом. Любой желающий мог прислать Лассе изменения или улучшения для *xz*, которые он должен был одобрить и опубликовать, после этого новая версия попадала в состав операционных систем.

В истории уже случались хакерские атаки, в ходе которых злоумышленники получали доступ к репозиторию[7] на *GitHub*, в том числе с помощью социальной инженерии.

В истории с бэкдором в *xz* хакеры использовали как раз психологическое состояние создателя программы, к расшатыванию которого сами явно приложили руку.

29 октября 2021 года разработчик с ником *Jia Tan* прислал Лассе Коллину свою первую правку для *xz*-, ровно через месяц — вторую, а в апреле 2022-го — еще несколько. Тогда же в почтовой рассылке *xz*[8] стали появляться письма от пользователя с ником

Jigar Kumar: он жаловался, что Коллин слишком долго принимает исправления от разработчика *Jia Tan*.

«Ты, конечно, молодец, но с таким медленным графиком обновлений, к сожалению, пройдут годы, прежде чем сообщество получит это улучшающее жизнь исправление», — писал *Jigar Kumar*.

К нему присоединился еще один пользователь, *Dennis Ens*, который был недоволен тем, что никто не поддерживает версию *xz* для языка *Java*. Лассе Коллин в ответах извинялся за задержки и сетовал на свое психологическое состояние, усталость и выгорание, но *Jigar* и *Dennis* продолжали травить его за медлительность и стали намекать, что неплохо было бы передать управление проектом кому-то более активному.

«С твоей текущей скоростью я сомневаюсь, что версия 5.4.0 выйдет в этом году. Единственный прогресс с апреля — несколько небольших изменений в тестах. Ты игнорируешь то, что куча исправлений гниют в этой рассылке. Ты душишь свой проект. Почему надо ждать 5.4.0, чтобы сменить управляющего проектом? Зачем откладывать то, что необходимо проекту?» — писал *Jigar Kumar* в июне 2022 года.

Уже после раскрытия готовившейся через *xz* атаки выяснилось, что пользователей *Jigar Kumar* и *Dennis Ens*, вероятно, никогда не существовало: они не оставили вообще никаких следов в интернете, их электронные почты на домене *Mailhost* нигде больше не использовались, они не участвовали ни в каких других почтовых рассылках, кроме *xz*. Единственное,

что делали эти пользователи — жаловались на медлительность Лассе Коллина и давили на него.

В конце июня 2022 года разработчик сдался и согласился, что *Jia Tan* больше подходит на роль руководителя проекта. К этому моменту создатель *xz* уже принял множество патчей от *Jia Tan* и написал в рассылке, что этот пользователь «получит большую роль в проекте в будущем». В конце ноября 2022 года Лассе Коллин частично передал тому права доступа и указал его почтовый адрес в форме для обратной связи.

11 января 2023 года Коллин опубликовал свою последнюю версию *xz* под номером 5.4.1; версия 5.4.2 в марте 2023 года вышла уже под авторством *Jia Tan*.

Получив контроль над xz, взломщики добавляют туда уязвимость

Jia Tan действительно продолжал работать над *xz*: он вносил и свои, и чужие изменения и даже благодарил других разработчиков за их вклад. Сам Лассе Коллин тоже продолжал иногда работать над пакетом, но стал уходить на регулярные каникулы без интернета. Основные решения теперь принимал уже новый владелец. *Jia Tan* даже перенес веб-страницу проекта с домашнего сайта Лассе на *GitHub*.

Современные разработчики стараются автоматизировать тестирование своих программ, чтобы не зависеть от человеческих ошибок и не тратить время на рутину. Лассе Коллин был разработчиком старой школы и тестировал все сам.

Jia Tan же написал для *xz* автоматические тесты. Именно под видом одного из тестов 23 февраля 2024 года он добавил туда файлы, содержавшие бэкдор. На следующий день *Jia Tan* опубликовал уязвимую версию 5.6.0, и она начала расходиться по дистрибутивам *Linux*.

Первая версия бэкдора столкнулась с проблемой: перестали выполняться автоматические тесты в двух дистрибутивах *Linux* — *Gentoo* и *Fedora*. Это привлекло внимание к изменениям и вызвало обсуждения в сообществе программистов. Именно эти обсуждения вспомнил Андрес Фройнд, когда заметил замедление скорости работы своего компьютера.

Нестабильную версию *xz* стали исключать из других популярных библиотек, и *Jia Tan* пришлось поторопиться. 9 марта он выпустил исправленную версию 5.6.1.

Все так же уязвимое, но менее подозрительное обновление 5.6.1 тоже начало проникать в тестовые версии дистрибутивов *Linux*. Иногда *Jia Tan* сам просил включить ее в обновления, иногда это делал другой пользователь, *Hans Jansen*. Как и в случае с комментаторами Лассе Коллина, этот пользователь больше нигде не засветился; единственная его активность, помимо таких комментариев, — это исправления к *xz*, на первый взгляд безобидные, но заложившие основу, на которой работает бэкдор от *Jia Tan*.

К тому моменту, когда разработчик *Microsoft* Андрес Фройнд обнаружил этот бэкдор, он уже был опубликован в бета-версиях *Debian* и *Fedora*. Фройнд

сначала непублично связался с разработчиками дистрибутивов, а на следующий день опубликовал пост, из которого о хакерской атаке узнал весь мир.

Как работает этот бэкдор

Изменения, которые *Jia Tan* внес в код *xz*, влияют на работу программы *sshd*, которая позволяет посылать серверам любые команды.

Для логина на сервер используют либо имя пользователя и пароль, либо — что происходит чаще — заранее известные серверу сертификаты или ключи клиента, которые практически невозможно подобрать.

Бэкдор же заставлял *sshd* принимать не только оригинальные сертификаты, но и специально подготовленные *Jia Tan* сертификаты, которые давали бы ему неограниченный доступ к любой системе, где установлена его версия пакета *xz*.

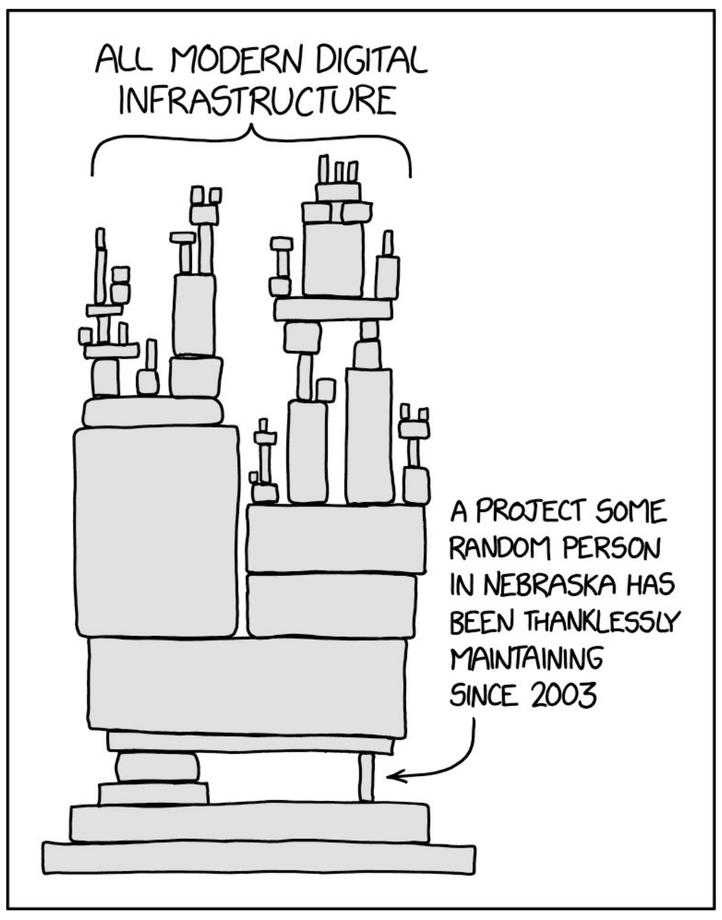
По сути, отправитель такого сертификата становился полноценным владельцем любого уязвимого сервера: он мог изменять, копировать и удалять любые данные на нем, устанавливать и удалять программы. Неограниченный доступ позволяет хакеру еще и скрыть все свои следы, так что долгое время владельцы не замечали бы вторжения.

В случае же если специальный сертификат не был получен, *sshd* работал как обычно.

Кроме того, после установки зараженной версии вредоносный код мог обновляться сам — вне

зависимости от того, будет ли пользователь обновлять пакет *xz* в дальнейшем.

Сам бэкдор был тщательно замаскирован и использовал несколько слоев, чтобы спрятать опасный код.



Комикс Рендела Монро «Зависимости» стал иллюстрацией к подавляющему большинству заметок о взломе *xz*.

Надпись на картинке: «Вся современная цифровая инфраструктура» — «Проект, который какой-то неизвестный чувак из Небраски безвозмездно поддерживает с 2003 года».

Возможные последствия: полный доступ к миллионам серверов

Таким образом, потенциально хакеры могли получить неограниченный доступ к миллионам серверов по всему миру, использующих *sshd*. Намерения хакеров неизвестны, но они могли стать катастрофическими для интернета.

По оценке *W3techs*, более 80% сайтов в мире работает на серверах с операционными системами, основанными на *Linux*. Все они могли бы стать уязвимы для хакеров, если бы бэкдор попал в основные ветки обновлений. По счастливой случайности бэкдор удалось обнаружить на раннем этапе, когда он

попал лишь в самые ранние тестовые версии нескольких крупных дистрибутивов. Например, самый популярный дистрибутив *Ubuntu* не успел добавить его.

«*OpenSSH*[9] работает на почти 20 млн *IP*-адресов сегодня, он почти в десять раз популярнее *RDP*[10].

. Если бы кто-то смог создать для него широко распространенный бэкдор, было бы плохо», — написал в своем блоге специалист по безопасности Кевин Бомон.

После обнаружения эта уязвимость была внесена в Национальную базу уязвимостей *(NVD)* США с максимально возможным уровнем опасности (10 из 10). Крупнейшие дистрибутивы *Linux* выпустили исправления, которые возвращали версию *xz* к тому моменту, когда *Jia Tan* еще не получил контроль над проектом. Лассе Коллину пришлось вернуться из «цифрового отпуска», чтобы восстановить доступ к проекту и заблокировать *Jia Tan*.

Кто стоит за атакой? Пока неясно

Неизвестно, кто скрывался за псевдонимом *Jia Tan*, и неясно даже, один это человек или группа хакеров. На *GitHub* этот пользователь вносил изменения в десятки других программ — сейчас их изучают специалисты по безопасности.

Одно из первых действий этого пользователя на *GitHub* — изменения к библиотеке *libarchive*[11] еще

в 2021 году. Это мелкое и безобидное на первый взгляд исправление: оно изменяет выводимое на

экран пользователя сообщение об ошибке — такие мелочи часто принимаются без должного внимания. Однако вместе с этим *Jia Tan* заменил функцию *safe_fprintf* на ее небезопасный аналог *fprintf*, позже это могло бы быть использовано хакером. Уязвимость исправили 29 марта уже после обнаружения бэкдора в *xz*.

Исследователи изучили время работы *Jia Tan* — все его изменения в *xz* сделаны на *GitHub*, то есть публичны. Хакер пытался выдать себя за китайца: он выбрал похожее на китайское имя и использовал в большинстве коммитов китайскую часовую зону.

Несмотря на это, в его коде обнаружили и правки, сделанные по восточноевропейскому времени, причем с такими промежутками, за которые человек, очевидно, не мог добраться до Восточной Европы. Обратили внимание исследователи и на то, что автор работал во время главных китайских праздников, но никогда — в католическое Рождество 25 декабря или в новогодние праздники 31 декабря и 1 января.

Редакторы: Максим Литаврин, Егор Сковорода

1. Один из самых распространенных дистрибутивов операционной системы Linux.
2. Она входит в стандартный набор большинства современных серверных операционных систем.
3. Конкретнее, речь идет о библиотеке liblzma, которая входит в пакет xz. В xz также входят программы для работы с архивами. В тексте для простоты мы будем везде говорить об xz как о целом.
4. Lempel-Ziv-Markov chain algorithm.

5. Аналог архиваторов WinZip или WinRar, но, в отличие от этих программ, с открытым исходным кодом.

6. Если быть точным, свою версию дистрибутива Slackware.

7. Хранилищу кода программы и всех его версий. Сейчас репозиторий xz заблокирован.

8. Аналог форума на базе электронной почты, популярный у разработчиков программ с открытым кодом.

9. Он же sshd.

10. Альтернативный протокол доступа.

11. Библиотека на языке C для работы с разными популярными форматами архивов.