Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Fail2ban для бизнеса: как защитить сервер 1С от перебора паролей

Почему боты круглосуточно ломятся в 1С, RDP и почту — и как закрыть эту угрозу малыми силами

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Ваши серверы — 1С, RDP, почта, сайт — круглосуточно обстреливают боты, перебирающие пароли по словарям и базам утечек. Это не целевая атака конкурентов: автоматика ломится во всё, что доступно из интернета. Один слабый пароль бухгалтера — и злоумышленник внутри: база 1С зашифрована, резервные копии уничтожены, контрагентам уходят письма с поддельными реквизитами, бизнес стоит…

Почему это важно бизнесу

- Брутфорс не выбирает жертв по имени: боты атакуют любой открытый сервер, а малый бизнес — чаще, потому что защита у него слабее
- Успешный подбор пароля означает простой на дни: шифрование 1С и файлов останавливает продажи, склад и бухгалтерию
- Взломанная почта — прямые потери: контрагенты переводят деньги по подменённым реквизитам, плюс риски по 152-ФЗ за утечку данных
- Восстановление на порядки дороже профилактики: выкуп, работа 1С-специалистов и упущенная выгода против пары часов настройки Fail2ban

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

5 за 10 мин

порог по умолчанию: maxretry = 5 неудачных входов за findtime = 10m — и Fail2ban блокирует IP...

jail.conf, Fail2ban 1.1

bantime.inc...

прогрессивный бан: каждое повторное попадание в блок удваивает срок — настойчивый бот выпадает...

jail.conf, Fail2ban 1.1

4625

Event ID неудачного входа в журнале Security — по нему на Windows/RDP строится автоблокировка...

Аудит входа Windows Server, learn.microsoft.com

10 попыток

рекомендуемое пороговое значение блокировки учётной записи в GPO — штатная защита доменных учё...

Account lockout threshold, learn.microsoft.com

22 и 3389

порты SSH и RDP — первые цели сканеров: на открытый порт летят тысячи попыток подбора в сутки,...

журналы серверов на нашем сопровождении

РЕАЛИЗАЦИЯ 1 ИЗ 3

Шифровальщик уничтожил и бэкапы: разбор инцидента у клиента

Что настраиваем

Дистрибьютор, около 40 рабочих мест: 1С, файловый сервер и резервные копии в одной сети; обратились к нам уже после взлома

Как мы это делаем

1. Порт RDP 3389 был проброшен наружу «для удалённой работы», лимита неудачных попыток входа не было
2. Пароль администратора подобран по словарю; в журнале Security — недели событий 4625 с сотен IP, которые никто не читал
3. Ночью запущен шифровальщик: база 1С, документы и бэкапы на сетевой шаре зашифрованы одним махом
4. Утром — файл с требованием выкупа; учёт, отгрузки и расчёты с контрагентами остановлены

РЕЗУЛЬТАТ

Около недели простоя: учёт восстанавливали по первичным документам и устаревшей копии. Бэкапы не помогли — они были доступны с того же сервера по SMB и зашифрованы вместе с базой.

КЛЮЧЕВОЙ НЮАНС

Шифровальщик уничтожает и резервные копии, если они доступны со взломанных серверов. Автоблокировка перебора и изолированный бэкап должны работать вместе — по отдельности они не спасают.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Стенд-ловушка: что прилетает на открытый RDP за неделю

Что настраиваем

Наш тестовый Windows-сервер с открытым портом 3389 без защиты — поднят специально, чтобы измерить фоновый поток атак

Как мы это делаем

1. Первые попытки подбора — в первые же часы после появления сервера в интернете: сканеры находят порт сами
2. За неделю — десятки тысяч событий 4625 с сотен IP: словари Administrator, admin, user, buh, 1c
3. Включаем автоблокировку: бан IP на брандмауэре по событиям 4625, порог 5 попыток — поток падает на порядки
4. Закрываем 3389 и переводим доступ на VPN — попытки прекращаются полностью

РЕЗУЛЬТАТ

Открытый RDP гарантированно находят и перебирают — вопрос только в стойкости паролей и времени. Каждый день без лимита попыток — тысячи бесплатных «выстрелов» по вашим учётным записям.

КЛЮЧЕВОЙ НЮАНС

Жертв выбирают сканером, а не по имени: открытый RDP со слабым паролем сам приглашает атакующего. Автоблокировка перебора и закрытый порт выводят сервер из «выборки» ботов.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Типовой сценарий: 1С на RDP-сервере со слабым паролем

Что настраиваем

Торговая компания на 20–30 рабочих мест: 1С, почта и файловая шара на одном сервере с RDP

Как мы это делаем

1. Бот находит открытый порт RDP и неделями перебирает пароли по словарям из утечек
2. Пароль сотрудника вида «Имя+год» подбирается — злоумышленник входит под легитимной учётной записью
3. Ночью запускается шифровальщик: база 1С, документы и бэкапы на той же шаре зашифрованы
4. Утром — требование выкупа; учёт, отгрузки и расчёты с контрагентами остановлены на дни

РЕЗУЛЬТАТ

Простой от нескольких дней до недели, восстановление учёта силами 1С-специалистов, риск невозврата данных даже после оплаты выкупа. Всё это против пары часов настройки лимита попыток входа.

КЛЮЧЕВОЙ НЮАНС

Один слабый пароль обесценивает все остальные вложения в ИТ. Лимит попыток входа, VPN и изолированный бэкап закрывают этот сценарий почти полностью.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **RDP и SSH открыты всему интернету**
  Сервер отвечает любому IP в мире на портах 3389 и 22. Боты находят его сканером за часы, дальше — тысячи попыток подбора пароля в сутки, пока не пове...

- ✕ **Нет лимита на неудачные попытки входа**
  Система позволяет перебирать пароли бесконечно. На Linux не настроен Fail2ban (maxretry = 3–5, findtime = 10m), на Windows — политика блокировки учёт...

- ✕ **Бэкапы доступны с рабочих серверов**
  Копии лежат на той же шаре или соседнем диске. Получив доступ, шифровальщик уничтожает их вместе с данными — восстанавливать нечего.

- ✕ **Словарные пароли и учётки из утечек**
  «Имя+год», «Q1w2e3r4», пароли, уже засветившиеся в утечках, перебираются по готовым словарям за минуты — стойкость такой защиты нулевая.

- ✕ **Защищён только один сервис из многих**
  SSH прикрыли и забыли, а почта (SMTP/IMAP), веб-публикация 1С, FTP и админки сайтов открыты. У Fail2ban есть готовые фильтры и для них, но jail'ы не...

- ✕ **Логи никто не читает**
  Всплеск неудачных входов (Failed password в auth.log, события 4625 в Security) виден за недели до взлома, но уведомлений нет — об атаке узнают уже по...

- ✕ **Нет второго фактора аутентификации**
  Подобранный пароль сразу даёт полный доступ: ни VPN, ни MFA на пути атакующего нет, легитимный вход неотличим от взлома.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Закрыть RDP (TCP 3389) и SSH (TCP 22) от прямого доступа из интернета или ограничить…
- Включить автоблокировку перебора: Fail2ban с jail sshd на Linux; на Windows — бан IP…
- Заменить словарные пароли, отключить неиспользуемые учётные записи

НОРМАЛЬНО

- Удалённый доступ только через VPN с двухфакторной аутентификацией; для RDP — обязате…
- Уведомления о банах и всплесках неудачных входов — в Telegram или на почту (action в…
- Изолированный бэкап: копия, недоступная со взломанного сервера ни по SMB, ни под учё…
- Включить jail'ы Fail2ban на всех сервисах: почта (postfix, dovecot), веб-публикация…

ХОРОШО

- Централизованный сбор логов (auth.log, журнал Security) и мониторинг входов по всем…
- Регулярный тест восстановления базы 1С из бэкапа и аудит открытых портов периметра
- Парольная политика в GPO, менеджер паролей, контроль утечек; ignoreip и bantime.incr…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Вы знаете, какие ваши серверы и сервисы (RDP, SSH, почта, веб-1С) доступны из интернета прямо сейчас?
- [ ] Есть ли автоблокировка IP после нескольких неудачных попыток входа на каждом из них — Fail2ban или его аналог?
- [ ] Удалённый доступ сотрудников идёт только через VPN с двухфакторной аутентификацией?
- [ ] Хранится ли хотя бы одна резервная копия там, куда не дотянется взломанный сервер?
- [ ] Узнаете ли вы о всплеске попыток подбора пароля в тот же день, а не после взлома?
- [ ] Запрещены ли словарные пароли и проверяются ли учётные записи по базам утечек?
- [ ] Отключаются ли учётные записи уволенных сотрудников в день увольнения?
- [ ] Проверяли ли вы за последний год, что база 1С реально восстанавливается из бэкапа?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Бесплатный аудит логов: за 1–2 дня покажем по auth.log и журналу Security, сколько попыток подбора летит на ваши с…
- Внедрение Fail2ban на Linux и автоблокировки по событию 4625 на Windows/RDP: пороги, ignoreip, Telegram-уведомления
- Настройка периметра: VPN с двухфакторкой, закрытие лишних портов, изолированные резервные копии
- Сопровождение по абонентке: мониторинг атак, реакция на инциденты, регулярные проверки защиты

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

Техническая база

01 jail.conf: параметры bantime, findtime, maxretry, ignoreip, bantime.increm… (fail2ban.org — 2024)

02 man 5 jail.conf и man fail2ban-client — справочник конфигурации и управлен… (fail2ban.org — 2024)

03 Account lockout threshold — политика блокировки учётных записей Windows Se… (learn.microsoft.com — 2025)

04 Аудит входа: событие 4625 (An account failed to log on) (learn.microsoft.com — 2025)

05 Network Level Authentication для подключений к удалённому рабочему столу (learn.microsoft.com — 2025)

06 sshd_config: MaxAuthTries, PasswordAuthentication, PermitRootLogin (openssh.com — 2024)

07 Публикация информационных баз на веб-сервере — руководство администратора,… (its.1c.ru — 2025)

08 Наши шаблоны jail.local, фильтров и Telegram-действий для серверов на сопр… (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.