Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Взлом сервера: наш регламент реагирования в первые часы

Как мы изолируем узел без потери улик, снимаем память и журналы, находим точку входа и восстан…

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Утром база 1С не открывается, файлы на шарах переименованы, на экране — требование выкупа. Мы решаем задачу первых часов: изолировать сервер без выключения, снять ОЗУ и журналы до того, как их затрут, найти точку входа и восстановиться из чистого бэкапа. Без отработанного регламента компания получает 2–5 дней простоя и повторный взлом через оставленные закладки.

Почему это важно бизнесу

- Простой офиса на 20–30 РМ — остановка отгрузок, продаж и бухгалтерии на 2–5 дней; каждый день без 1С — прямые потери выручки
- Выключение сервера «выдёргиванием шнура» стирает ОЗУ — без неё не доказать точку входа и не гарантировать, что атака не повторится
- Утечка персданных = уведомление РКН в 24 часа; без зафиксированных улик и акта экспертизы защищаться от претензий нечем
- Оплата выкупа не гарантирует расшифровку и помечает компанию как «платящую» — восстановление из изолированного бэкапа всегда дешевле
- «Почищенный», а не пересобранный сервер возвращает атакующего через закладки — и весь бюджет восстановления сгорает второй раз

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

60 мин

Наш норматив от звонка до изоляции: блок WAN-трафика узла на шлюзе, карантин, старт снятия пам…

наш стандарт SLA

0.77

Velociraptor: offline-коллектором одним exe снимаем артефакты Windows без установки ПО на узел

по докам docs.velociraptor.app

1 ГБ

Размер журнала Security вместо ~20 МБ по умолчанию — иначе следы входа затираются ротацией за…

наш стандарт для серверов и DC

×2

Сброс пароля krbtgt дважды при компрометации домена — иначе краденые Kerberos-билеты остаются…

по докам Microsoft AD DS

7 дней

Минимум immutability бэкап-копии в Veeam Hardened Repository — шифровальщик её не удалит даже…

Veeam B&R 12.x

15.2

Sysmon на пересобранных серверах: журнал процессов и сетевых соединений для будущих разборов

Sysinternals, learn.microsoft.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Изоляция и снятие улик без выключения сервера

Что настраиваем

Скомпрометированный Windows Server (файловый / 1С): первые 60–90 минут, удалённо через VPN или с выездом инженера

Как мы это делаем

1. Фиксируем время обнаружения и фото экрана; на шлюзе (pfSense/Keenetic) блокируем WAN-трафик узла правилом deny, внутреннюю сеть и наш VPN оставляем
2. Не перезагружаем и лишний раз не логинимся: активные сессии, ключи шифровальщика и сетевые соединения атакующего живут только в ОЗУ
3. Снимаем образ ОЗУ WinPmem (winpmem_mini_x64.exe mem.raw) на внешний USB-диск, затем триаж Velociraptor Offline Collector (артефакт Windows.KapeFiles.Targets)
4. Выгружаем журналы: wevtutil epl Security/System плюс копия каталога winevt\Logs целиком; каждую копию хэшируем Get-FileHash SHA256 для акта
5. До любого «лечения» сохраняем срез системы: netstat -ano, tasklist /svc, автозагрузку через Autoruns — сравним с эталоном при расследовании

РЕЗУЛЬТАТ

Через 1,5–2 часа у нас неизменяемый комплект улик: образ памяти, артефакты, журналы с хэшами. Расследование и восстановление идут параллельно, не мешая друг другу, а акт с хэшами используется для РКН, полиции и страховой.

КЛЮЧЕВОЙ НЮАНС

Порядок жёсткий: сначала память, потом диск, потом всё остальное — любая перезагрузка или «проверка антивирусом» уничтожает самые ценные данные. Изоляцию делаем правилом на шлюзе, а не кнопкой питания.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Поиск точки входа по журналам Windows

Что настраиваем

Security/System/RDP-журналы пострадавшего сервера и контроллера домена, глубина 30–90 дней

Как мы это делаем

1. Ищем брутфорс: серии 4625 (Logon Type 3/10) и итоговый успешный 4624 с того же IP — Get-WinEvent с фильтром по EventID и выгрузка в таблицу
2. RDP-хронология: журнал TerminalServices-LocalSessionManager, события 21/24/25 — кто, когда и с какого адреса входил и переподключался
3. Следы закрепления: 4720 (новая учётка), 4728/4732 (включение в группу), 7045 (новая служба), 4698 (задача планировщика) — всё в таймлайн
4. Проверяем 1102 (очистка журнала Security): если логи затёрты, восстанавливаем картину по DC, шлюзу и соседним узлам сети
5. Сводим события с поправкой на NTP-смещение узлов и строим таймлайн: вход → повышение прав → распространение → шифрование

РЕЗУЛЬТАТ

Точка входа определяется в 9 из 10 инцидентов за 2–4 часа: как правило, опубликованный RDP, слабый пароль или непропатченный сервис. На выходе — конкретный список дыр, которые закрываем до возврата сервера в прод; без этого пересборка бессмысленна.

КЛЮЧЕВОЙ НЮАНС

Журнал Security по умолчанию крошечный и перезаписывается — на контрактах сопровождения мы заранее поднимаем его до 1 ГБ и дублируем события в Wazuh/syslog, чтобы в инциденте было что читать.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Пересборка и закрытие точки входа

Что настраиваем

Пострадавшие серверы и доменные учётные записи; параллельно с расследованием, до возврата в прод

Как мы это делаем

1. Данные восстанавливаем только из изолированного бэкапа (Veeam Hardened Repository / отключаемый NAS), ОС ставим начисто — закладки не переносим
2. Пароли меняем с заведомо чистой машины: все административные и сервисные учётки; krbtgt — дважды, с интервалом больше времени жизни TGT (10 ч по умолчанию)
3. RDP из интернета закрываем навсегда; доступ — только VPN (WireGuard/IPsec на шлюзе) + 2FA, на серверах NLA и lockout-политика (5 попыток / 30 мин)
4. Ставим контроль повторного входа: Sysmon 15.2 с конфигом по процессам и сети, экспорт в Wazuh, алерты на 4625/7045/1102 в Telegram
5. Финал: отчёт с таймлайном атаки, акт с хэшами улик и план закрытия остальных находок аудита со сроками внедрения

РЕЗУЛЬТАТ

Компания возвращается в работу за 1–2 суток без риска повторного входа тем же путём: старые билеты и пароли недействительны, периметр закрыт, а повторная попытка входа видна в алертах в первые минуты, а не через месяц.

КЛЮЧЕВОЙ НЮАНС

Пересборка без смены krbtgt и сервисных паролей — самообман: атакующий вернётся по краденым учёткам в «чистую» систему. Скомпрометированными считаем все учётные данные, а не только явно засвеченные.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Сервер выключили питанием**
  Инстинкт «выдернуть шнур» стирает ОЗУ с ключами и сессиями атакующего. Мы изолируем правилом на шлюзе: блок WAN, узел остаётся включённым

- ✕ **Антивирус запустили до снятия образа**
  Сканер удаляет и переименовывает вредоносные файлы — таймлайн атаки разваливается. Сначала WinPmem и триаж-коллектор, лечение потом

- ✕ **Пароли сменили со взломанного хоста**
  Кейлоггер или дамп LSASS тут же отдаёт новые пароли атакующему. Меняем только с заведомо чистой машины и только после изоляции узла

- ✕ **Бэкапы лежали в том же домене**
  Шифровальщик с правами админа удаляет и их. Держим копию в Hardened Repository с immutability или на физически отключаемом носителе

- ✕ **krbtgt сбросили один раз**
  Пароль учётки хранится в двух версиях: старые Kerberos-билеты живы до второго сброса. Делаем два сброса с интервалом больше 10 часов

- ✕ **Логи Security затёрлись ротацией**
  Журнал по умолчанию ~20 МБ и перезаписывается за часы активной атаки. Заранее ставим 1 ГБ и выносим копию событий в Wazuh/syslog

- ✕ **Сервер «почистили» вместо пересборки**
  Закладки — службы, задачи планировщика, скрытые учётки — находят не все. Правило: пересборка с нуля, данные только из проверенного бэкапа

- ✕ **RDP вернули «на время» после инцидента**
  Опубликованный 3389 снова брутфорсят через считанные часы. Только VPN + 2FA; периметр контролируем внешним сканом портов раз в месяц

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Закрыть RDP/SSH из интернета, удалённый доступ — только через VPN с 2FA
- Бэкап-копия вне домена: отключаемый диск или NAS с отдельной учёткой
- Журнал Security 1 ГБ + включённый аудит входов на серверах и DC
- Напечатанный план первого часа: кого звать, что не выключать и не трогать

НОРМАЛЬНО

- Veeam с Hardened Repository, immutability 7–14 дней, тест восстановления в месяц
- Sysmon на серверах + сбор событий в Wazuh/syslog, алерты на 4625/7045/1102
- Lockout-политика, LAPS для локальных админов, NLA на всех RDP-узлах
- Договор IR с SLA: реакция 1 час, готовый комплект триажа (Velociraptor)

ХОРОШО

- EDR на серверах и PC, сегментация VLAN: серверы, PC и бэкапы — отдельно
- Ежемесячный внешний скан периметра и регулярный патч-цикл по расписанию
- Учения раз в квартал: восстановление инфраструктуры из бэкапа на стенде
- Tier-модель админских прав и отдельные чистые станции для администрирования

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знает ли каждый сотрудник, кому звонить при записке о выкупе — и что сервер выключать нельзя?
- [ ] Есть ли копия бэкапов, которую нельзя удалить даже с правами доменного админа (immutability/офлайн)?
- [ ] Восстанавливали ли вы файл из бэкапа за последние 30 дней своими руками, а не «по отчёту»?
- [ ] Закрыт ли RDP/SSH из интернета — и проверялось ли это внешним сканом портов, а не по памяти?
- [ ] Хватит ли журналов на разбор атаки: Security ≥1 ГБ, аудит входов включён, копия событий вне узла?
- [ ] Есть ли заведомо чистая машина для смены паролей и админских работ во время инцидента?
- [ ] Прописан ли в плане восстановления двойной сброс krbtgt и смена всех сервисных учёток?
- [ ] Успеете ли уведомить РКН за 24 часа: кто пишет, какие данные утекли, где лежат доказательства?
- [ ] Есть ли договорной SLA на реагирование: удалённое подключение за час, выезд инженера за 4 часа?

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).

- Экстренное реагирование: изоляция узла, снятие памяти и триаж Velociraptor удалённо в течение часа после звонка
- Расследование: таймлайн атаки по журналам, точка входа, акт с хэшами улик для РКН, полиции и страховой
- Пересборка серверов, восстановление из бэкапа, двойной сброс krbtgt и смена всех учётных данных с чистой машины
- Закрытие периметра: VPN с 2FA вместо открытого RDP, hardened-бэкапы Veeam, Sysmon + Wazuh с алертами в Telegram
- Сопровождение с IR-SLA: реакция 1 час, ежемесячный скан периметра, квартальный тест восстановления

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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Velociraptor: Offline Collector и артефакты триажа (docs.velociraptor.app — 0.77)

02 Sysmon — System Monitor (Sysinternals) (learn.microsoft.com — v15.2)

03 Windows Security Auditing: события 4624/4625/1102/7045 (learn.microsoft.com — 2025)

04 AD DS: сброс учётной записи krbtgt (learn.microsoft.com — 2025)

05 Veeam B&R: Hardened Repository и immutability (helpcenter.veeam.com — 12.x)

06 Volatility 3 Framework: анализ образов памяти (volatility3.readthedocs.io — v2.x)

07 Наш шаблон IR-регламента и чек-лист первого часа (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.