Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Криптомайнер на сервере: находим, вычищаем, не пускаем обратно

Наш конвейер: Zabbix 7.0 LTS + Sysmon 15.20 + Wazuh 4.14, порядок зачистки и харденинг RDP

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сервер 1С или RDS месяцами молотит чужую криптовалюту: CPU держит полку 95–100%, проведение документа растягивается с 1 до 15–20 секунд, растут счета за электричество. Хуже того, майнер — маркер компрометации: тем же доступом заносят шифровальщик. Разбираем наш конвейер: обнаружение по телеметрии, демонтаж персистентности в правильном порядке и закрытие точки входа.

Почему это важно бизнесу

- Простой учёта: при полке CPU 99% документ в 1С проводится 15–20 с вместо 1 с — продажи и бухгалтерия фактически стоят
- Майнер = чужой админ-доступ к серверу: следующим шагом через ту же дыру приходит шифровальщик или выгрузка баз
- Прямые расходы: +30–50% к счёту за электричество серверной и ускоренный износ CPU и системы охлаждения
- Скомпрометированный сервер с базами клиентов — это уже инцидент с персональными данными по 152-ФЗ

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

7.0 LTS

Zabbix: шаблон Windows by Zabbix agent (active), триггер High CPU по макросу {$CPU.UTIL.CRIT}

по докам zabbix.com

70%/30 мин

наш доп-триггер вне рабочих часов: штатные 90% за 5 минут не ловят майнер с ограничением нагру...

наш стандарт

15.20

Sysmon: события ID 1 (ProcessCreate) и ID 3 (NetworkConnect) — связка процесс → исходящее соед...

Sysinternals, learn.microsoft.com

4.14

Wazuh: syscheck (FIM) в realtime на C:\ProgramData и ветках Run — новый exe и автозапуск видны...

documentation.wazuh.com

5 / 30 мин

GPO Account Lockout: порог 5 неудачных входов, блокировка на 30 минут — брутфорс RDP умирает

параметры — learn.microsoft.com, значения — наш профиль

UDP 51820

WireGuard вместо проброса 3389: один UDP-порт, персональный ключ на сотрудника, отзыв за минуту

wireguard.com

РЕАЛИЗАЦИЯ 1 ИЗ 3

Обнаружение: телеметрия CPU, процессов и сети

Что настраиваем

Windows Server 2019/2022 — роли 1С, RDS, SQL; агенты мониторинга на каждом сервере клиента

Как мы это делаем

1. Zabbix agent 2 + шаблон Windows by Zabbix agent (active); штатный триггер CPU оставляем ({$CPU.UTIL.CRIT}=90, окно 5 мин)
2. Добавляем свой триггер: avg(/host/system.cpu.util,30m)>70 в окне 22:00–07:00 — ровная ночная «полка» и есть сигнатура майнера
3. Sysmon 15.20: ProcessCreate (ID 1) с хешами + NetworkConnect (ID 3) с фильтром по портам пулов 3333/5555/7777/14444
4. Журналы Sysmon и Security шлём в Wazuh 4.14; правило на исходящие к портам пулов = алерт дежурному в Telegram
5. Ручная проверка по вызову: Get-Process с сортировкой по CPU, Get-NetTCPConnection -OwningProcess, ревизия C:\ProgramData

РЕЗУЛЬТАТ

Майнер виден в первые 30–60 минут жизни, а не через месяц по жалобе «1С тормозит»: алерт сразу связывает процесс, путь к файлу, хеш и адрес пула — дежурный видит, что запущено, откуда и куда оно стучится.

КЛЮЧЕВОЙ НЮАНС

NetworkConnect (ID 3) в Sysmon по умолчанию выключен и без фильтра топит журнал: включаем его только правилами по DestinationPort и исключаем штатные процессы (1cv8, sqlservr).

РЕАЛИЗАЦИЯ 2 ИЗ 3

Зачистка: демонтаж персистентности по порядку

Что настраиваем

Заражённый Windows-сервер; работаем из сессии под отдельной чистой админ-учёткой

Как мы это делаем

1. Инвентаризация: Get-ScheduledTask вне \Microsoft*, Get-Service по недавно созданным службам, ключи Run/RunOnce в HKLM и HKU
2. Autoruns (autorunsc -a * -h): ловим WMI-подписки, IFEO-дебаггеры и службы с «системными» именами, сверяем хеши бинарей
3. Порядок строгий: Unregister-ScheduledTask → Stop-Service + sc delete → Remove-ItemProperty Run → Stop-Process → удаление каталога
4. Точка входа: Security 4624 LogonType 10 и 4625 за 35 дней, группировка по SourceIP — почти всегда это проброшенный наружу RDP
5. Решение о переустановке: если доступ был неделями — сервер перекатываем и восстанавливаем данные из бэкапа до даты первого входа

РЕЗУЛЬТАТ

CPU падает до штатных 8–15% и майнер не возвращается через 5 минут по планировщику; по журналам получаем дату и канал компрометации — понятно, что закрывать и с какой даты бэкап считать чистым.

КЛЮЧЕВОЙ НЮАНС

Убивать процесс первым нельзя: сторожевая задача перезапустит его раньше, чем дочистите файлы. Сначала все механизмы автозапуска, сам процесс — предпоследним, файлы — в конце.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Недопуск: периметр, GPO и контроль запуска

Что настраиваем

Роутер клиента (Mikrotik/Keenetic), GPO домена, серверы с ролями 1С/RDS

Как мы это делаем

1. Убираем NAT-проброс 3389; WireGuard на роутере: пир на сотрудника (AllowedIPs /32), RDP доступен только из VPN-подсети
2. GPO: Account Lockout Threshold 5 / Duration 30 мин, переименованный Administrator, пароли 18+ символов из генератора в Bitwarden
3. AppLocker: правила Executable по умолчанию + запрет запуска из C:\ProgramData и %TEMP% для не-администраторов
4. Wazuh syscheck realtime на ProgramData и ветки Run; ночной CPU-триггер Zabbix остаётся страховочной сеткой
5. Контрольный внешний скан периметра после работ и далее ежеквартально: наружу — только WireGuard UDP

РЕЗУЛЬТАТ

Брутфорс перестаёт быть возможным как класс: RDP снаружи не виден, подбор гасится локаутом, а даже занесённый файл не стартует из типовых каталогов майнеров без разрешающего правила AppLocker.

КЛЮЧЕВОЙ НЮАНС

AppLocker включаем сначала в режиме Audit only на 1–2 недели: смотрим события 8003 (что было бы заблокировано), вносим исключения (обновления 1С пишут в ProgramData) и лишь потом Enforce — блокировки там видны…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Процесс убит первым**
  Сторожевая задача планировщика возвращает майнер за 5 минут. Мы сначала снимаем задачи, службу и Run-ключи, процесс — в конце.

- ✕ **Чистка по имени файла**
  Имя всегда «системное» (WindowsHostHelper и т.п.). Опираемся на путь, хеш и издателя через autorunsc -h, а не на название.

- ✕ **Забытые WMI-подписки**
  Персистентность в __EventFilter/__EventConsumer переживает удаление задач и служб. Проверяем вкладку WMI в Autoruns.

- ✕ **Порог CPU 90% за 5 минут**
  Штатный {$CPU.UTIL.CRIT} не ловит майнер с ограничением нагрузки. Добавляем триггер avg за 30 мин > 70% вне рабочих часов.

- ✕ **Антивирус удалил только exe**
  Задача-загрузчик скачает свежий бинарь за сутки. Чистим механизм доставки и блокируем адреса и порты пулов на шлюзе.

- ✕ **VPN поставили, 3389 остался**
  Старое NAT-правило часто забывают. После работ снимаем внешний скан периметра: наружу — только UDP-порт WireGuard.

- ✕ **Нет переката после долгого доступа**
  Если злоумышленник сидел неделями, гарантий отсутствия бэкдора нет. Переустанавливаем ОС, данные — из бэкапа до даты входа.

- ✕ **Журнал Security на 20 МБ**
  При брутфорсе события 4625 затирают историю за часы. Ставим 1 ГБ на Security и выгружаем в Wazuh — расследование не слепнет.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Закрыть 3389/5900 наружу; удалённый доступ — только через VPN (WireGuard)
- GPO Account Lockout 5/30 мин + админ-пароли 16–18 символов из генератора
- Zabbix-триггер на ночную «полку» CPU > 70% дольше 30 минут

НОРМАЛЬНО

- Sysmon 15.20 (ID 1/3) + выгрузка журналов Security и Sysmon в Wazuh 4.14
- Wazuh syscheck realtime на ProgramData, Temp и ветки автозапуска
- Ежеквартальный аудит паролей и внешний скан периметра
- Бэкапы в две локации с квартальным тестовым восстановлением

ХОРОШО

- AppLocker (Audit → Enforce): запрет запуска из ProgramData и %TEMP%
- Блокировка исходящих на порты пулов 3333/5555/7777/14444 на шлюзе
- Алерты дежурной смене 24/7 в Telegram + регламент реагирования
- Переименованный Administrator; старое имя — отключённая учётка-ловушка с аудитом

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] RDP-порт 3389 недоступен из интернета — проверено внешним сканом, а не «по памяти»?
- [ ] Есть триггер на аномальный CPU вне рабочих часов, а не только штатные 90% за 5 минут?
- [ ] Собираются ли Sysmon ID 1/3 и Security 4624/4625 в SIEM, а не только локально на сервере?
- [ ] Журнал Security увеличен до 1 ГБ и переживёт сутки брутфорса без затирания истории?
- [ ] Включена ли блокировка учётки после 5 неудачных входов (Account Lockout Policy)?
- [ ] Админ-пароли 16+ символов, уникальны между серверами и хранятся в менеджере паролей?
- [ ] Запрещён ли запуск exe из C:\ProgramData и %TEMP% для обычных пользователей?
- [ ] Известно ли, какие процессы штатно в топе CPU на каждом сервере (1cv8, sqlservr)?
- [ ] Есть ли бэкап в двух локациях и известна дата последнего тестового восстановления?

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).

- Экстренный выезд: диагностика, зачистка майнера и поиск точки входа за один визит
- Перевод удалённого доступа с проброса RDP на WireGuard с персональными ключами
- Мониторинг 24/7: Zabbix 7.0 LTS + Sysmon + Wazuh с алертами дежурной смене
- Харденинг GPO: локаут, пароли, AppLocker с обкаткой в режиме Audit only
- Регулярные аудиты: пароли ежеквартально, периметр и отчёт по ИБ раз в полгода

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 Sysmon: события ProcessCreate (ID 1), NetworkConnect (ID 3) (learn.microsoft.com — v15.20)

02 Шаблон Windows by Zabbix agent (active), макрос {$CPU.UTIL.CRIT} (zabbix.com — 7.0 LTS)

03 Wazuh: syscheck (FIM), rootcheck, realtime-мониторинг (documentation.wazuh.com — 4.14)

04 Account Lockout Policy: Threshold / Duration (learn.microsoft.com — 2025)

05 AppLocker: правила Executable, режим Audit only, события 8003/8004 (learn.microsoft.com — 2025)

06 WireGuard: конфигурация пиров, AllowedIPs (wireguard.com — 1.0)

07 Шаблон харденинга удалённого доступа ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.