PERESVET LAB · КОНФИДЕНЦИАЛЬНО

# ОТЧЁТ ОБ УТЕЧКАХ ДАННЫХ

Физическое лицо · OSINT-расследование

| | |
|---|---|
| СУБЪЕКТ | Кузьмин Иван Дмитриевич |
| ТЕЛЕФОН | +79161396831 |
| EMAIL | kuzminivan2004@gmail.com |
| ID ОТЧЁТА | PVL-PHY-20260404 |
| ДАТА | 04.04.2026 |
| ТИП СУБЪЕКТА | Физическое лицо |

## 1. КРАТКОЕ РЕЗЮМЕ

В ходе автоматизированного OSINT-расследования, проведённого компанией Peresvet Lab 04.04.2026, были получены и верифицированы данные об утечках персональной информации субъекта. Выявлено **27 находок**: **9 критических**, **10 высоких**, **1 средних**, **7 низких**.

| 9 | 10 | 1 | 7 |
|---|---|---|---|
| КРИТИЧЕСКИХ | ВЫСОКИХ | СРЕДНИХ | НИЗКИХ |

## 2. СВЕДЕНИЯ О СУБЪЕКТЕ

| | |
|---|---|
| ФИО | Кузьмин Иван Дмитриевич |
| ТЕЛЕФОН | +79161396831 |
| EMAIL | kuzminivan2004@gmail.com |
| ТИП СУБЪЕКТА | Физическое лицо |
| ID ОТЧЁТА | PVL-PHY-20260404 |
| ДАТА ПРОВЕРКИ | 04.04.2026 |

## 3. РЕЗУЛЬТАТЫ РАССЛЕДОВАНИЯ

Находки отсортированы по степени критичности. Данные получены в режиме реального времени на дату формирования отчёта.

F-001 **Утечка из базы данных: BlankMediaGames** КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · BlankMediaGames | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «BlankMediaGames». В декабре 2018 года веб-сайт Town of Salem созданный BlankMediaGames подвергся утечке данных. Данные содержали 7,6 млн. уникальных адресов электронной почты. Также в утечке были имена, IP-адреса, истории покупок и пароли в виде хешей phpass. BlankMediaGames так и не ответила на многочисленные попытки связаться по поводу инцидента. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| IP-АДРЕС | 82.43.54.209 |
| ИМЯ ПОЛЬЗОВАТЕЛЯ | futureHacker |
| ПАРОЛЬ | $H$9w8yDhRszf25Ffd6LlMRFj2xWp2eRS. |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их.

### F-002 Утечка из базы данных: Cit0Day

КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Cit0Day | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Cit0Day». Cit0day - это ныне несуществующий сервис по поиску электронных почт среди различных утечек. После его закрытия в ноябре 2020 года в открытый доступ попала коллекция из более чем 23 000 взломанных сайтов. Данные были рассортированы на несколько десятков категорий и содержали более 226 миллионов почт и паролей к ним. Некоторые пароли были защищены при помощи хешей. Найдено записей: 1.

| | |
|---|---|
| CATEGORY | Entertainment |
| EMAIL | kuzminivan2004@gmail.com |
| LEAKSITE | pathtags.com |
| ПАРОЛЬ | 1ad7c58a50051456 |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их.

### F-003 Утечка из базы данных: Cloudata

КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Cloudata | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Cloudata». Большая коллекция данных email-pass. База была собрана из множества файлов 18 мая 2023 года. Изначально все базы весили 338 GB (11 миллиардов строк). После удаления дубликатов и данных из коллекций осталось около 2 миллиардов. Найдено записей: 3.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| ПАРОЛЬ | 1ad7c58a50051456 |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их.

F-004 **Утечка из базы данных: JoinPiggy.com** КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · JoinPiggy.com | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «JoinPiggy.com». JoinPiggy - кешбэк сервис. Он был взломан в сентябре 2020 года, пострадало 1.5 миллиона человек. Данные содержат почты, телефоны, имена, социальные сети и другую информацию о пользователях. Найдено записей: 1.

| | |
|---|---|
| BROWSER | Firefox |
| EMAIL | kuzminivan2004@gmail.com |
| IP-АДРЕС | 2.27.115.215 |
| LASTACTIVE | 2016-06-28 12:31:34 |
| OS | Mac |
| ПАРОЛЬ | f9900d15e65c29a91398e45abd5756da3dc2553a |
| REGDATE | 2016-06-28 12:32:05 |
| TYPE | Desktop |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их.

F-005 **Утечка из базы данных: TeraBase64** КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · TeraBase64 | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «TeraBase64». Огромная коллекция файлов, опубликованная в феврале 2020 года человеком с псевдонимом @HTTSMVKCOM. Она содержала 3.2 миллиарда строк с почтами и паролями в виде простого текста, однако уникальных строк было всего 1,28 миллиарда. Все эти данные скорее всего были получены из множества других утечек. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| ПАРОЛЬ | 1ad7c58a50051456 |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их.

F-006 **Утечка из базы данных: Wattpad** КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Wattpad | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Wattpad». В июне 2020 года сайт пользовательских историй Wattpad подвергся утечке, раскрывшей 270 млн. записей. Была раскрыта личная информация: имена, почты, IP, пол, даты рождения и пароли в виде хешей bcrypt. Найдено записей: 1.

| | |
|---|---|
| BDAY | 1978-01-30 |
| СТРАНА | GB |
| DATE | 2015-12-01 16:22:54 |
| EMAIL | kuzminivan2004@gmail.com |
| ИМЯ | ikuzmin |
| GENDER | M |
| IP-АДРЕС | 82.132.234.222 |
| ИМЯ ПОЛЬЗОВАТЕЛЯ | ikuzmin |
| ПАРОЛЬ | $2y$10$CeW8LhrQTO3YHqKsp20wleMeM/lNfyi4E4yCGU/irOFb4s55hGzGG |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их.

F-007 **Домашняя сеть проиндексирована: 5.138.211.23** КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| Shodan Internet Scanner · 5.138.211.23 | 5.138.211.23 | 2026-04-04 |

IP-адрес 5.138.211.23 (провайдер: PJSC Rostelecom) проиндексирован Shodan и имеет 10 открытых портов, видимых из интернета. Потенциально опасные порты: 7547/TR-069/CWMP. Эти сервисы доступны любому пользователю интернета без ограничений.

| | |
|---|---|
| ПОРТ 81 | идентификатор |
| ПОРТ 82 | идентификатор |
| ПОРТ 83 | идентификатор |
| ПОРТ 84 | идентификатор |
| ПОРТ 86 | идентификатор |
| ПОРТ 88 | идентификатор |
| ПОРТ 554 | идентификатор |
| ПОРТ 6881 | идентификатор |
| ПОРТ 7547 | TR-069/CWMP ⚠ |
| ПОРТ 37777 | идентификатор |
| ПРОВАЙДЕР (ISP) | PJSC Rostelecom |
| ОРГАНИЗАЦИЯ | OJSC Rostelecom Macroregional Branch South |
| ГЕОЛОКАЦИЯ | Krasnodar, Russian Federation |
| ПОСЛЕДНЕЕ СКАНИРОВАНИЕ | 2026-04-02T23:03:41.704861 |
| ИСТОРИЯ: ПОРТ 554 / 2026-04-02 | tcp |
| ИСТОРИЯ: ПОРТ 88 / 2026-04-02 | Hikvision IP Camera (tcp) |
| ИСТОРИЯ: ПОРТ 81 / 2026-04-02 | Hikvision IP Camera (tcp) |
| ИСТОРИЯ: ПОРТ 37777 / 2026-04-02 | Dahua DH-IPC-HDBW1230EP-S-0360B (tcp) |
| ИСТОРИЯ: ПОРТ 84 / 2026-04-02 | Hikvision IP Camera (tcp) |

✓ **Рекомендация:** Немедленно смените пароль в скомпрометированном сервисе, а также во всех аккаунтах, где использовался тот же или похожий пароль. Включите двухфакторную аутентификацию (предпочтительно через приложение-аутентификатор, не SMS). Проверьте историю входов и активные сессии в затронутых аккаунтах — при обнаружении чужих сеансов немедленно завершите их. Закройте все неиспользуемые порты в настройках роутера. Для портов 22/3389 настройте белый список IP или используйте VPN.

## F-008 Известные уязвимости (NIST NVD): 85.172.12.163

КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| NIST NVD · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

Для IP-адреса «85.172.12.163» обнаружено 47 уязвимостей (CVE), зарегистрированных в Национальной базе данных уязвимостей США (NVD).

| | |
|---|---|
| CVE-2020-20262 | CVSS 6.5 (MEDIUM) [CWE-617] — Mikrotik RouterOs до 6.47 (стабильное дерево) страдает от уязвимости отказа утверждения в процессе /ram/pckg/security/nova/bin/ipsec. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за отказа утверждения через созданный пакет. |
| CVE-2023-32154 | CVSS 7.5 (HIGH) [CWE-787] — Mikrotik RouterOS RADVD Out-Of-Bounds Write Remote Code Execution Vulnerability. Эта уязвимость позволяет сетевым злоумышленникам выполнять произвольный код на затронутых установках Mikrotik RouterOS. Аутентификация не требуется для использования этой уязвимости. Конкретный изъян существует в рамках рекламы маршрутизатора Daemon. Проблема возникает из-за отсутствия надлежащей проверки предоставленных пользователем данных, что может привести к записи после окончания выделенного буфера. Злоумышленник может использовать эту уязвимость для выполнения кода в контексте root. Был ZDI-CAN-19797. |
| CVE-2020-20266 | CVSS 6.5 (MEDIUM) [CWE-476, CWE-787] — Mikrotik RouterOs до 6.47 (стабильное дерево) страдает от уязвимости к повреждению памяти в процессе /nova/bin/dot1x. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). |
| CVE-2020-20267 | CVSS 6.5 (MEDIUM) [CWE-787] — Mikrotik RouterOs до 6.47 (стабильное дерево) страдает от уязвимости к повреждению памяти в процессе /nova/bin/resolver. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за недействительного доступа к памяти. |
| CVE-2020-20264 | CVSS 6.5 (MEDIUM) [CWE-369] — Mikrotik RouterOs до 6.47 (стабильное дерево) в процессе /ram/pckg/advanced-tools/nova/bin/netwatch. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за деления на нулевую ошибку. |
| CVE-2020-20265 | CVSS 6.5 (MEDIUM) [CWE-787] — Mikrotik RouterOs до 6.47 (стабильное дерево) страдает от уязвимости повреждения памяти в процессе /ram/pckg/wireless/nova/bin/wireless. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании через созданный пакет. |
| CVE-2019-13074 | CVSS 7.5 (HIGH) [CWE-770] — Уязвимость в демоне FTP на маршрутизаторах MikroTik через 6.44.3 может позволить удаленным злоумышленникам исчерпать всю доступную память, в результате чего устройство перезагрузится из-за неконтролируемого управления ресурсами. |
| CVE-2021-36613 | CVSS 6.5 (MEDIUM) [CWE-476] — Mikrotik RouterOs до стабильного 6.48.2 страдает от уязвимости к повреждению памяти в процессе ptp. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). |
| CVE-2020-20225 | CVSS 6.5 (MEDIUM) [CWE-617] — Mikrotik RouterOs до 6.47 страдает от уязвимости отказа утверждения в процессе /nova/bin/user. |

| | |
|---|---|
| | Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за отказа утверждения через созданный пакет. |
| **CVE-2020-10364** | CVSS 7.5 (HIGH) [CWE-770] — Демон SSH на маршрутизаторах MikroTik через v6.44.3 может позволить удаленным злоумышленникам генерировать активность процессора, вызывать отказ от новых авторизованных соединений и вызывать перезагрузку через подключение и запись системных вызовов из-за неконтролируемого управления ресурсами. |
| **CVE-2021-36614** | CVSS 6.5 (MEDIUM) [CWE-476] — Mikrotik RouterOs до стабильного 6.48.2 страдает уязвимостью к повреждению памяти в процессе tr069-клиента. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). |
| **CVE-2020-20220** | CVSS 6.5 (MEDIUM) [CWE-119] — Mikrotik RouterOs до стабильного 6.47 страдает от уязвимости к повреждению памяти в процессе /nova/bin/bfd. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). |
| **CVE-2020-20221** | CVSS 6.5 (MEDIUM) [CWE-400] — Mikrotik RouterOs до 6.44.6 страдает от неконтролируемой уязвимости потребления ресурсов в процессе /nova/bin/cerm. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за перегрузки систем ЦПУ. |
| **CVE-2019-15055** | CVSS 6.5 (MEDIUM) [CWE-22] — MikroTik RouterOS через 6.44.5 и 6.45.x через 6.45.3 неправильно обрабатывает имя диска, что позволяет аутентифицированным пользователям удалять произвольные файлы. Злоумышленники могут использовать эту уязвимость для сброса хранилища учетных данных, что позволяет им получить доступ к интерфейсу управления в качестве администратора без аутентификации. |
| **CVE-2022-45315** | CVSS 9.8 (CRITICAL) [CWE-125] — Было обнаружено, что Mikrotik RouterOs до стабильного v7.6 содержал несвязанное считывание в процессе snmp. Эта уязвимость позволяет злоумышленникам выполнять произвольный код через созданный пакет. |
| **CVE-2025-6443** | CVSS 7.2 (HIGH) [CWE-284] — Mikrotik RouterOS VXLAN Source IP Improper Access Control Vulnerability. Эта уязвимость позволяет удаленным злоумышленникам обходить ограничения доступа на затронутые установки Mikrotik RouterOS. Аутентификация не требуется для использования этой уязвимости. Конкретный недостаток существует в обработке удаленных IP-адресов при обработке трафика VXLAN. Проблема возникает из-за отсутствия проверки удаленного IP-адреса на сконфигурированные значения, прежде чем разрешить входящий трафик во внутреннюю сеть. Злоумышленник может использовать эту уязвимость для получения доступа к внутренним сетевым ресурсам. ZDI-CAN-26415. |
| **CVE-2022-45313** | CVSS 8.8 (HIGH) [CWE-125] — Было обнаружено, что Mikrotik RouterOs до стабильного v7.5 содержал несвязанное считывание в процессе горячей точки. Эта уязвимость позволяет злоумышленникам выполнять произвольный код через созданное сообщение nova. |
| **CVE-2018-14847** | CVSS 9.1 (CRITICAL) [CWE-22] — MikroTik RouterOS через 6.42 позволяет неавторизованным удаленным злоумышленникам читать произвольные файлы, а удаленным аутентифицированным злоумышленникам - писать произвольные файлы из-за уязвимости обхода каталогов в интерфейсе WinBox. |

| | |
|---|---|
| **CVE-2019-16160** | CVSS 7.5 (HIGH) [CWE-191] — Целый недоток в сервере SMB MikroTik RouterOS до 6.45.5 позволяет удаленным неавторизованным злоумышленникам сбить службу. |
| **CVE-2019-3977** | CVSS 7.5 (HIGH) [CWE-494] — RouterOS 6.45.6 Стабильный маршрутизатор 6.44.5 Долгосрочные и ниже недостаточно проверенные, где пакеты обновления загружаются при использовании функции автоматического обновления. Таким образом, удаленный злоумышленник может обмануть маршрутизатор в «обновлении» до более старой версии RouterOS и, возможно, сбросить все имена пользователей и пароли системы. |
| **CVE-2023-30800** | CVSS 7.5 (HIGH) [CWE-787] — На веб-сервер, используемый MikroTik RouterOS версии 6, влияет проблема повреждения памяти. Удаленный и неавторизованный злоумышленник может повредить кучу памяти сервера, отправив обработанный HTTP-запрос. В результате веб-интерфейс ломается и немедленно перезапускается. Проблема была исправлена в RouterOS 6.49.10. RouterOS версии 7 не пострадает. |
| **CVE-2019-3978** | CVSS 7.5 (HIGH) [CWE-306] — RouterOS версии 6.45.6 Стабильный, 6.44.5 Долгосрочные и ниже позволяют удаленным неавторизованным злоумышленникам запускать DNS-запросы через порт 8291. Запросы отправляются с маршрутизатора на сервер по выбору злоумышленника. Ответы DNS кэшируются маршрутизатором, что потенциально приводит к отравлению кэшем. |
| **CVE-2019-3979** | CVSS 7.5 (HIGH) [CWE-345] — RouterOS версии 6.45.6 Стабильный, 6.44.5 Долгосрочные и ниже уязвимы для DNS-атаки, не связанной с данными. Маршрутизатор добавляет все записи A в свой кэш DNS, даже если записи не связаны с доменом, который был задан. Таким образом, DNS-сервер, управляемый удаленным злоумышленником, может отравить кэш DNS маршрутизатора с помощью вредоносных ответов с дополнительными и неверными записями. |
| **CVE-2020-20021** | CVSS 7.5 (HIGH) [CWE-400] — Проблема, обнаруженная в MikroTik Router v6.46.3, позволяет злоумышленнику вызвать отказ в обслуживании через неправильную конфигурацию в демоне SSH. |
| **CVE-2020-20253** | CVSS 6.5 (MEDIUM) [CWE-369] — Mikrotik RouterOs до 6.47 страдает от деления на нулевую уязвимость в процессе /nova/bin/lcdstat. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за деления на нулевую ошибку. |
| **CVE-2020-20252** | CVSS 6.5 (MEDIUM) [CWE-476, CWE-787] — Mikrotik RouterOs до стабильной версии 6.47 страдает от уязвимости повреждения памяти в процессе /nova/bin/lcdstat. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). |
| **CVE-2020-20250** | CVSS 6.5 (MEDIUM) [CWE-476, CWE-787] — Mikrotik RouterOs до стабильной версии 6.47 страдает от уязвимости повреждения памяти в процессе /nova/bin/lcdstat. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). Примечание: это отличается от CVE-2020-20253 и CVE-2020-20254. Все четыре уязвимости в процессе /nova/bin/lcdstat обсуждаются в ссылке CVE-2020-20250 github.com/cq674350529. |
| **CVE-2021-3014** | CVSS 6.1 (MEDIUM) [CWE-79] — В MikroTik RouterOS до 2021-01-04 страница входа в горячую точку уязвима для отражения XSS через целевой параметр. |

| | |
|---|---|
| **CVE-2022-36522** | CVSS 6.5 (MEDIUM) [CWE-617] — Было обнаружено, что Mikrotik RouterOs через стабильный v6.48.3 содержит отказ утверждения в компоненте /advanced-tools/nova/bin/netwatch. Эта уязвимость позволяет злоумышленникам вызвать отказ в обслуживании (DoS) через созданный пакет. |
| **CVE-2020-20254** | CVSS 6.5 (MEDIUM) [CWE-787] — Mikrotik RouterOs до 6.47 (стабильное дерево) страдает от уязвимости к повреждению памяти в процессе /nova/bin/lcdstat. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании (NULL pointer dereference). |
| **CVE-2020-20217** | CVSS 6.5 (MEDIUM) [CWE-400] — Mikrotik RouterOs до 6.47 страдает от неконтролируемой уязвимости потребления ресурсов в процессе /nova/bin/route. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за перегрузки систем ЦПУ. |
| **CVE-2018-7445** | CVSS 9.8 (CRITICAL) [CWE-119] — В сервисе MikroTik RouterOS SMB при обработке сообщений запроса сессии NetBIOS был обнаружен переполненный буфер. Удаленные злоумышленники с доступом к сервису могут воспользоваться этой уязвимостью и получить выполнение кода в системе. Переполнение происходит до того, как происходит аутентификация, поэтому неавторизованный удаленный злоумышленник может использовать его. Все архитектуры и все устройства, работающие под управлением RouterOS до версий 6.41.3/6.42rc27, уязвимы. |
| **CVE-2020-20230** | CVSS 6.5 (MEDIUM) [CWE-400] — Mikrotik RouterOs до стабильного 6.47 страдает от неконтролируемого потребления ресурсов в процессе sshd. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании из-за перегрузки систем ЦПУ. |
| **CVE-2019-3981** | CVSS 3.7 (LOW) [CWE-300] — MikroTik Winbox 3.20 и ниже уязвим для атак среднего уровня. Человек в середине может понизить протокол аутентификации клиента и восстановить имя пользователя и хешированный пароль MD5. |
| **CVE-2018-5951** | CVSS 7.5 (HIGH) — Проблема была обнаружена в Mikrotik RouterOS. Создание пакета размером 1 байт и отправка его на IPv6-адрес коробки RouterOS с IP-протоколом 97 приведет к немедленной перезагрузке RouterOS. Все версии RouterOS, поддерживающие EoIPv6, уязвимы для этой атаки. |
| **CVE-2019-3976** | CVSS 8.8 (HIGH) [CWE-23, CWE-22] — RouterOS 6.45.6 Стабильный маршрутизатор 6.44.5 Долгосрочные и ниже уязвимы для произвольной уязвимости создания каталогов через поле имени пакета обновления. Если аутентифицированный пользователь устанавливает вредоносный пакет, то может быть создан каталог и включена оболочка разработчика. |
| **CVE-2019-3943** | CVSS 8.1 (HIGH) [CWE-23, CWE-22] — Версии MikroTik RouterOS Stable 6.43.12 и ниже, Longterm 6.42.12 и ниже, а также Testing 6.44beta75 и ниже уязвимы для аутентифицированного удаленного обхода каталогов через интерфейсы HTTP или Winbox. Эта уязвимость может использоваться для чтения и записи файлов за пределами каталога песочницы (/rw/disk). |
| **CVE-2023-30799** | CVSS 9.1 (CRITICAL) [CWE-269] — MikroTik RouterOS, стабильная до 6,49,7 и долгосрочная до 6,48,6, уязвима к проблеме эскалации привилегий. Удаленный и аутентифицированный злоумышленник может увеличить привилегии от администратора до супер-администратора в интерфейсе Winbox или HTTP. Злоумышленник может злоупотреблять этой уязвимостью для выполнения произвольного кода в системе. |

| | |
|---|---|
| **CVE-2018-1159** | CVSS 6.5 (MEDIUM) [CWE-119] — Mikrotik RouterOS до 6.42.7 и 6.40.9 уязвима для повреждения памяти. Аутентифицированный удаленный злоумышленник может сбить HTTP-сервер, быстро проверяя и отключая его. |
| **CVE-2018-1158** | CVSS 6.5 (MEDIUM) [CWE-674] — Mikrotik RouterOS до 6.42.7 и 6.40.9 уязвима для стека. Аутентифицированный удаленный злоумышленник может сбить HTTP-сервер с помощью рекурсивного анализа JSON. |
| **CVE-2019-13954** | CVSS 6.5 (MEDIUM) [CWE-770] — Mikrotik RouterOS до 6.44.5 (долгосрочное дерево выпуска) уязвим к истощению памяти. Отправляя созданный HTTP-запрос, аутентифицированный удаленный злоумышленник может сбить HTTP-сервер и в некоторых случаях перезагрузить систему. Вредоносный код вводить нельзя. |
| **CVE-2019-13955** | CVSS 6.5 (MEDIUM) [CWE-674] — Mikrotik RouterOS до 6.44.5 (долгосрочное дерево выпуска) уязвим к истощению стека. Отправляя созданный HTTP-запрос, аутентифицированный удаленный злоумышленник может сбить HTTP-сервер с помощью рекурсивного анализа JSON. Вредоносный код вводить нельзя. |
| **CVE-2019-3924** | CVSS 7.5 (HIGH) [CWE-441] — MikroTik RouterOS до 6.43.12 (стабильный) и 6.42.12 (долгосрочный) уязвим для промежуточной уязвимости. Программное обеспечение будет выполнять пользовательские сетевые запросы как для клиентов WAN, так и для клиентов LAN. Удаленный неавторизованный злоумышленник может использовать эту уязвимость для обхода брандмауэра маршрутизатора или для общего сканирования сети. |
| **CVE-2018-1157** | CVSS 6.5 (MEDIUM) [CWE-400] — Mikrotik RouterOS до 6,42,7 и 6,40,9 уязвим для истощения памяти. Аутентифицированный удаленный злоумышленник может сбить HTTP-сервер и в некоторых случаях перезагрузить систему с помощью созданного HTTP POST-запроса. |
| **CVE-2018-1156** | CVSS 8.8 (HIGH) [CWE-787] — Mikrotik RouterOS до 6.42.7 и 6.40.9 уязвим для переполнения буфера стека через интерфейс обновления лицензии. Эта уязвимость теоретически может позволить удаленному аутентифицированному злоумышленнику выполнять произвольный код в системе. |
| **CVE-2020-20249** | CVSS 6.5 (MEDIUM) [CWE-787] — Mikrotik RouterOs до стабильного 6.47 страдает от уязвимости повреждения памяти в процессе разрешителя. Отправляя обработанный пакет, аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании. |
| **CVE-2020-20247** | CVSS 6.5 (MEDIUM) [CWE-787] — Mikrotik RouterOs до 6.46.5 (стабильное дерево) страдает от уязвимости к повреждению памяти в процессе /nova/bin/traceroute. Аутентифицированный удаленный злоумышленник может вызвать отказ в обслуживании через переменную счетчика циклов. |

✓ **Рекомендация:** Обновите программное обеспечение на всех затронутых сервисах до последних версий. Для критических CVE примените патчи незамедлительно.

F-009 **Вероятность эксплуатации (EPSS): 85.172.12.163** КРИТИЧЕСКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| FIRST EPSS · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

Для IP-адреса «85.172.12.163» получены оценки EPSS (Exploit Prediction Scoring System) по 47 уязвимостям. EPSS показывает вероятность эксплуатации CVE в ближайшие 30 дней.

| | |
|---|---|
| CVE-2018-14847 | EPSS 93.64% (percentile 99.8%) |
| CVE-2018-7445 | EPSS 87.56% (percentile 99.5%) |
| CVE-2019-3978 | EPSS 16.61% (percentile 94.9%) |
| CVE-2018-5951 | EPSS 15.50% (percentile 94.6%) |
| CVE-2022-45313 | EPSS 12.92% (percentile 94.0%) |
| CVE-2019-3924 | EPSS 10.79% (percentile 93.3%) |
| CVE-2023-30800 | EPSS 10.37% (percentile 93.2%) |
| CVE-2023-32154 | EPSS 3.07% (percentile 86.7%) |
| CVE-2022-45315 | EPSS 2.95% (percentile 86.4%) |
| CVE-2018-1156 | EPSS 2.64% (percentile 85.7%) |
| CVE-2018-1157 | EPSS 2.36% (percentile 84.9%) |
| CVE-2020-10364 | EPSS 2.15% (percentile 84.2%) |
| CVE-2020-20217 | EPSS 1.94% (percentile 83.4%) |
| CVE-2020-20264 | EPSS 1.56% (percentile 81.4%) |
| CVE-2020-20250 | EPSS 1.36% (percentile 80.1%) |
| CVE-2019-16160 | EPSS 1.28% (percentile 79.6%) |
| CVE-2018-1158 | EPSS 1.22% (percentile 79.1%) |
| CVE-2020-20230 | EPSS 1.21% (percentile 79.0%) |
| CVE-2020-20266 | EPSS 1.14% (percentile 78.4%) |
| CVE-2020-20221 | EPSS 1.11% (percentile 78.1%) |
| CVE-2018-1159 | EPSS 1.07% (percentile 77.7%) |
| CVE-2020-20220 | EPSS 1.05% (percentile 77.5%) |
| CVE-2020-20252 | EPSS 1.01% (percentile 77.1%) |

| | |
|---|---|
| CVE-2020-20267 | EPSS 1.01% (percentile 77.1%) |
| CVE-2019-13955 | EPSS 0.97% (percentile 76.6%) |
| CVE-2021-36613 | EPSS 0.91% (percentile 75.7%) |
| CVE-2021-36614 | EPSS 0.91% (percentile 75.7%) |
| CVE-2019-13954 | EPSS 0.87% (percentile 75.2%) |
| CVE-2019-3977 | EPSS 0.86% (percentile 75.0%) |
| CVE-2019-13074 | EPSS 0.85% (percentile 74.9%) |
| CVE-2020-20253 | EPSS 0.84% (percentile 74.7%) |
| CVE-2020-20254 | EPSS 0.84% (percentile 74.7%) |
| CVE-2019-3976 | EPSS 0.83% (percentile 74.4%) |
| CVE-2020-20247 | EPSS 0.65% (percentile 70.7%) |
| CVE-2023-30799 | EPSS 0.64% (percentile 70.5%) |
| CVE-2021-3014 | EPSS 0.58% (percentile 68.8%) |
| CVE-2019-3943 | EPSS 0.57% (percentile 68.7%) |
| CVE-2019-15055 | EPSS 0.45% (percentile 63.6%) |
| CVE-2022-36522 | EPSS 0.44% (percentile 63.1%) |
| CVE-2020-20265 | EPSS 0.40% (percentile 60.8%) |
| CVE-2020-20262 | EPSS 0.35% (percentile 57.3%) |
| CVE-2019-3981 | EPSS 0.32% (percentile 55.4%) |
| CVE-2020-20249 | EPSS 0.31% (percentile 54.2%) |
| CVE-2020-20225 | EPSS 0.25% (percentile 48.0%) |
| CVE-2019-3979 | EPSS 0.22% (percentile 44.9%) |
| CVE-2025-6443 | EPSS 0.15% (percentile 36.2%) |
| CVE-2020-20021 | EPSS 0.07% (percentile 21.2%) |

✓ **Рекомендация:** Приоритизируйте устранение CVE с высоким показателем EPSS (>10%). Эти уязвимости активно эксплуатируются или имеют высокую вероятность эксплуатации.

F-010 **Утечка из базы данных: Auchan** ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Auchan | kuzminivan2004@gmail.com, +79161396831 | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Auchan». 6 июня 2023 года хакерская группировка NLB опубликовала базу данных клиентов торговой сети «Ашан». Данные содержат 4.7 миллиона электронных почт, 7.7 миллиона телефонов, а так же имена, адреса доставки и другие технические детали. Судя по данным, сам взлом произошёл 18 мая 2023 года. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| ИМЯ | Иван |
| ИМЯ | Кузьмин |
| ТЕЛЕФОН | +79161396831 |
| REGDATE | 2022-10-02 14:04:47 |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

F-011 **Утечка из базы данных: ChitaiGorod** ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · ChitaiGorod | kuzminivan2004@gmail.com, +79161396831 | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «ChitaiGorod». 9 июня 2023 года хакерская группа NLB выложила в открытый доступ базу российского книжного магазина «Читай город». Данные содержат почты, телефоны, имена, даты рождения, города проживания и номера скидочных карт покупателей. Всего 9.8 миллиона записей. Найдено записей: 1.

| | |
|---|---|
| ГОРОД | Город Москва |
| СТРАНА | Россия |
| EMAIL | kuzminivan2004@gmail.com |
| ИМЯ | Иван |
| LASTACTIVE | 2022-11-14 19:32:11.000 |
| ИМЯ | Кузьмин |
| ИМЯ ПОЛЬЗОВАТЕЛЯ | kuzminivan2004@gmail.com |
| ТЕЛЕФОН | +79161396831 |
| REGDATE | 2022-11-14 19:32:11.000 |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

### F-012 Утечка из базы данных: Gemini

ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Gemini | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Gemini». В конце 2022 года данные, вероятно взятые с криптобиржи Gemini, были размещены на хакерском форуме. Данные состояли из адресов электронной почты и номеров телефонов, которые Gemini позже приписали инциденту у стороннего поставщика. Номера были указаны в формате 123-XXX-7890. Они являются частичными числами и не включают средние 3 цифры. Всего пострадало 5,7 миллиона пользователей. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| ТЕЛЕФОН | 789-XXX-5875 |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

### F-013 Утечка из базы данных: Gravatar scrape 2023

ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Gravatar scrape 2023 | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Gravatar scrape 2023». Сервис Gravatar позволяет пользователям использовать один аватар на множестве сервисов. В январе 2023 года при помощи скрапинга с него были собраны данные 61 миллиона пользователей. Они включали почты, ники и аватары. Найдено записей: 1.

| | |
|---|---|
| AVATAR | https://secure.gravatar.com/avatar/162547dbcba916859e2cc52bfdc54b01 |
| EMAIL | kuzminivan2004@gmail.com |
| ИМЯ ПОЛЬЗОВАТЕЛЯ | sirivankuzmin |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

### F-014 Утечка из базы данных: Have I Been Drained Crypto

ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Have I Been Drained Crypto | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Have I Been Drained Crypto». Эта база является компиляцией из нескольких крупных утечек, связаных с криптовалютой. В базе содержится около 12 миллионов электронных почт, а так же, в некоторых случаях, почты, имена, телефоны, адреса проживания и данные баланса. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| ТЕЛЕФОН | 789-XXX-5875 |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

### F-015 Утечка из базы данных: Mathway

ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Mathway | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Mathway». В январе 2020 года веб-сайт решения математических задач Mathway пострадал от утечки данных. В результате неё было раскрыто более 25 миллионов записей. Впоследствии данные были проданы на рынке даркнета и включали имена, идентификаторы Google и Facebook, адреса электронной почты и хеши паролей MD5 с солью, закодированные алгоритмом base64. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| ИМЯ | Иван |
| LASTACTIVE | 2019-07-12 07:06:07.823 |
| ИМЯ | Кузьмин |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

F-016 **Утечка из базы данных: MyFitnessPal** ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · MyFitnessPal | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «MyFitnessPal». В феврале 2018 года сервис диеты и физических упражнений MyFitnessPal подвергся утечке данных. Инцидент раскрыл 144 миллиона уникальных почт вместе с именами, IP и паролями в виде хешей SHA-1 и bcrypt. Все данные, кроме хешей bcrypt, позже были выложены в открытый доступ. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| IP-АДРЕС | 2.28.26.3 |
| ИМЯ ПОЛЬЗОВАТЕЛЯ | ivankuzmin |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

F-017 **Утечка из базы данных: Twitter 200M**

ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · Twitter 200M | kuzminivan2004@gmail.com | 2026-04-04 |

Идентификатор «kuzminivan2004@gmail.com» (email) обнаружен в базе «Twitter 200M». В январе 2022 года уязвимость в платформе Twitter позволила хакеру создать базу данных почт и номеров телефонов 200 миллионов пользователей социальной платформы. В августе 2022 года Twitter сообщил, что уязвимость связана с ошибкой, появившейся в июне 2021 года. Данные включали электронные почты, номера телефонов, имя пользователя, биографию, местоположение и фотографию профиля. Найдено записей: 1.

| | |
|---|---|
| EMAIL | kuzminivan2004@gmail.com |
| FOLLOWERS | 1 |
| ИМЯ | John Smith |
| ИМЯ ПОЛЬЗОВАТЕЛЯ | futurehacker23 |
| REGDATE | 28.11.2017 19:37:14 |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

F-018 **Утечка из базы данных: 2GIS 2025** ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| LeakOSINT · 2GIS 2025 | +79161396831 | 2026-04-04 |

Идентификатор «+79161396831» (телефон) обнаружен в базе «2GIS 2025». В начале августа 2025 года данные с онлайн-карт 2GIS были собраны при помощи парсинга, выполнялся поиск профилей по всем существующим телефонам России и Казахстана. На сайте оказалось зарегистрировано чуть меньше 20 миллионов аккаунтов. Таблица содержала номер телефона, никнейм, ссылку на аватар и ссылку на профиль. 99% пользователей были из России, а остальные из Казахстана. Найдено записей: 1.

| | |
|---|---|
| ИМЯ | Ivan Kuzmin |
| LINK | 2gis.ru/user/00d7e673b0794cb6893a2b0548d9c257 |
| ТЕЛЕФОН | 79161396831 |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов.

F-019 **Домашняя сеть проиндексирована: 85.172.12.163** ВЫСОКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| Shodan Internet Scanner · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

IP-адрес 85.172.12.163 (провайдер: PJSC Rostelecom) проиндексирован Shodan и имеет 4 открытых портов, видимых из интернета. Shodan зафиксировал 47 известных CVE: CVE-2020-20262, CVE-2023-32154, CVE-2020-20266, CVE-2020-20267, CVE-2020-20264....

| | |
|---|---|
| ПОРТ 53 | идентификатор |
| ПОРТ 161 | идентификатор |
| ПОРТ 2000 | идентификатор |
| ПОРТ 8291 | идентификатор |
| CVE / УЯЗВИМОСТИ | CVE-2020-20262, CVE-2023-32154, CVE-2020-20266, CVE-2020-20267, CVE-2020-20264, CVE-2020-20265, CVE-2019-13074, CVE-2021-36613, CVE-2020-20225, CVE-2020-10364, CVE-2021-36614, CVE-2020-20220, CVE-2020-20221, CVE-2019-15055, CVE-2022-45315, CVE-2025-6443, CVE-2022-45313, CVE-2018-14847, CVE-2019-16160, CVE-2019-3977, CVE-2023-30800, CVE-2019-3978, CVE-2019-3979, CVE-2020-20021, CVE-2020-20253, CVE-2020-20252, CVE-2020-20250, CVE-2021-3014, CVE-2022-36522, CVE-2020-20254, CVE-2020-20217, CVE-2018-7445, CVE-2020-20230, CVE-2019-3981, CVE-2018-5951, CVE-2019-3976, CVE-2019-3943, CVE-2023-30799, CVE-2018-1159, CVE-2018-1158, CVE-2019-13954, CVE-2019-13955, CVE-2019-3924, CVE-2018-1157, CVE-2018-1156, CVE-2020-20249, CVE-2020-20247 |
| ОС УСТРОЙСТВА | MikroTik RouterOS 6.40.8 |
| ПРОВАЙДЕР (ISP) | PJSC Rostelecom |
| ОРГАНИЗАЦИЯ | OJSC Rostelecom Macroregional Branch South |
| ГЕОЛОКАЦИЯ | Sochi, Russian Federation |
| ПОСЛЕДНЕЕ СКАНИРОВАНИЕ | 2026-04-04T07:19:11.335241 |
| CPE (ИДЕНТИФИКАТОРЫ УСТРОЙСТВ) | cpe:/o:mikrotik:routeros:6.40.8, cpe:2.3:o:mikrotik:routeros:6.40.8 |
| ИСТОРИЯ: ПОРТ 8291 / 2026-04-04 | MikroTik Winbox (tcp) |
| ИСТОРИЯ: ПОРТ 53 / 2026-04-03 | udp |
| ИСТОРИЯ: ПОРТ 8291 / 2026-04-03 | MikroTik Winbox (tcp) |

| | |
|---|---|
| ИСТОРИЯ: ПОРТ 2000 / 2026-04-03 | MikroTik bandwidth-test server (tcp) |
| ИСТОРИЯ: ПОРТ 8291 / 2026-04-02 | MikroTik Winbox (tcp) |

✓ **Рекомендация:** Утекшие персональные данные (телефон, адрес, ФИО) могут использоваться для социальной инженерии и восстановления доступа к аккаунтам. Проверьте, не привязаны ли эти данные к функциям восстановления пароля в важных сервисах (Госуслуги, банки, почта). Рассмотрите смену номера телефона или email для критически важных аккаунтов. Регулярно проверяйте домашний IP на shodan.io и обновляйте прошивку роутера.

## F-020 Публичный профиль Gravatar

СРЕДНИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| Gravatar · kuzminivan2004@gmail.com | kuzminivan2004@gmail.com | 2026-04-04 |

Email «kuzminivan2004@gmail.com» привязан к публичному профилю Gravatar. Профиль содержит персональную информацию, доступную любому, кто знает адрес электронной почты.

| | |
|---|---|
| ОТОБРАЖАЕМОЕ ИМЯ | Ivan Kuzmin |
| URL ПРОФИЛЯ | https://gravatar.com/sirivankuzmin |
| О СЕБЕ | https://кузьмин.рус && https://eyeofliberty.com && https://peresvetlab.ru |
| МЕСТОПОЛОЖЕНИЕ | Moscow, Russia |
| ПРИВЯЗАННЫЕ АККАУНТЫ | youtube: https://www.youtube.com/channel/UC2iry7DDtrdrRUz9m0XdwDQ |

✓ **Рекомендация:** Проверьте настройки конфиденциальности профиля Gravatar на gravatar.com. Удалите лишнюю персональную информацию и отвяжите неиспользуемые аккаунты.

### F-021 Репутация IP-адреса: AbuseIPDB

НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| AbuseIPDB · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

IP-адрес «85.172.12.163» проверен по базе AbuseIPDB, содержащей жалобы на вредоносную активность. Рейтинг угрозы: 0%.

| | |
|---|---|
| РЕЙТИНГ УГРОЗЫ (ABUSEIPDB) | 0% |
| ТИП ИСПОЛЬЗОВАНИЯ (ABUSEIPDB) | Fixed Line ISP |

✓ **Рекомендация:** Высокий рейтинг угрозы означает, что с этого IP фиксировалась вредоносная активность. Если это ваш IP — проверьте все устройства в домашней сети на наличие вирусов и ботнет-агентов, обновите прошивку роутера и смените пароль от Wi-Fi. Если IP динамический — он мог быть скомпрометирован предыдущим пользователем.

### F-022 Антивирусный анализ IP: VirusTotal

НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| VirusTotal · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

IP-адрес «85.172.12.163» проверен через VirusTotal — агрегатор антивирусных движков. 0 движков считают адрес вредоносным.

| | |
|---|---|
| ДЕТЕКЦИИ (VIRUSTOTAL) | 0 malicious, 1 suspicious / 94 engines |

✓ **Рекомендация:** Антивирусные движки VirusTotal отметили этот IP как подозрительный. Проверьте все устройства в вашей сети антивирусом, обновите прошивку роутера и убедитесь, что пароль от панели управления роутером не стоит по умолчанию. При наличии вредоносных детекций рассмотрите смену IP у провайдера.

### F-023 Геолокация и сеть: ipinfo.io

НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| ipinfo.io · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

Сетевая информация об IP-адресе «85.172.12.163» получена из ipinfo.io.

| | |
|---|---|
| ASN (IPINFO) | AS25490 |
| ОРГАНИЗАЦИЯ (IPINFO) | PJSC Rostelecom |
| СТРАНА (IPINFO) | Russia |

✓ **Рекомендация:** Убедитесь, что геолокация и провайдер соответствуют вашему реальному местоположению. Несовпадение может указывать на использование вашего IP третьими лицами или на подмену данных в утечке. Если вы не используете VPN, а страна/город не совпадают — это повод для дополнительной проверки.

### F-024 Репутация IP-адреса: AbuseIPDB

НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| AbuseIPDB · 5.138.211.23 | 5.138.211.23 | 2026-04-04 |

IP-адрес «5.138.211.23» проверен по базе AbuseIPDB, содержащей жалобы на вредоносную активность. Рейтинг угрозы: 0%.

| | |
|---|---|
| РЕЙТИНГ УГРОЗЫ (ABUSEIPDB) | 0% |
| ТИП ИСПОЛЬЗОВАНИЯ (ABUSEIPDB) | Fixed Line ISP |

✓ **Рекомендация:** Высокий рейтинг угрозы означает, что с этого IP фиксировалась вредоносная активность. Если это ваш IP — проверьте все устройства в домашней сети на наличие вирусов и ботнет-агентов, обновите прошивку роутера и смените пароль от Wi-Fi. Если IP динамический — он мог быть скомпрометирован предыдущим пользователем.

### F-025 Антивирусный анализ IP: VirusTotal

НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| VirusTotal · 5.138.211.23 | 5.138.211.23 | 2026-04-04 |

IP-адрес «5.138.211.23» проверен через VirusTotal — агрегатор антивирусных движков. 0 движков считают адрес вредоносным.

| | |
|---|---|
| ДЕТЕКЦИИ (VIRUSTOTAL) | 0 malicious, 0 suspicious / 94 engines |

✓ **Рекомендация:** Антивирусные движки VirusTotal отметили этот IP как подозрительный. Проверьте все устройства в вашей сети антивирусом, обновите прошивку роутера и убедитесь, что пароль от панели управления роутером не стоит по умолчанию. При наличии вредоносных детекций рассмотрите смену IP у провайдера.

### F-026 Геолокация и сеть: ipinfo.io

НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| ipinfo.io · 5.138.211.23 | 5.138.211.23 | 2026-04-04 |

Сетевая информация об IP-адресе «5.138.211.23» получена из ipinfo.io.

| | |
|---|---|
| ASN (IPINFO) | AS12389 |
| ОРГАНИЗАЦИЯ (IPINFO) | PJSC Rostelecom |
| СТРАНА (IPINFO) | Russia |

✓ **Рекомендация:** Убедитесь, что геолокация и провайдер соответствуют вашему реальному местоположению. Несовпадение может указывать на использование вашего IP третьими лицами или на подмену данных в утечке. Если вы не используете VPN, а страна/город не совпадают — это повод для дополнительной проверки.

F-027 **Сетевое сканирование (Nmap): 85.172.12.163** НИЗКИЙ

| ИСТОЧНИК | ЗАПРОС | ДАТА ПРОВЕРКИ |
|---|---|---|
| Nmap · 85.172.12.163 | 85.172.12.163 | 2026-04-04 |

Активное сканирование IP-адреса «85.172.12.163» обнаружило 2 открытых портов. Уязвимости не обнаружены.

| | |
|---|---|
| PORT 53/TCP | domain |
| PORT 2000/TCP | bandwidth-test (MikroTik bandwidth-test server) |

✓ **Рекомендация:** Закройте все неиспользуемые порты. Обновите сервисы с обнаруженными уязвимостями. Ограничьте доступ к административным портам через межсетевой экран.

## 4. ОБЩИЕ РЕКОМЕНДАЦИИ

| | |
|---|---|
| **Управление паролями** | Никогда не используйте один и тот же пароль для разных сервисов. Это защитит вас от массовых взломов (credential stuffing), когда злоумышленники используют пароль из одной утечки для входа на другие сайты. Начните использовать надежный менеджер паролей (например, KeePassXC, Bitwarden, Kaspersky Password Manager) для генерации и безопасного хранения уникальных паролей. |
| **Защита аккаунтов** | Немедленно смените пароли, скомпрометированные в данном отчете. Включите двухфакторную аутентификацию (2FA) везде, где это возможно (Госуслуги, почта, мессенджеры). Отдавайте предпочтение приложениям-аутентификаторам (Aladdin 2FA, Google Authenticator), так как коды из SMS злоумышленнику легче перехватить. |
| **Цифровая гигиена** | Для служб доставки, маркетплейсов и бонусных карт используйте виртуальные (дополнительные) номера телефонов и отдельные email-адреса. При отсутсвии возможности зарегестрировать виртуальный номер, рекомендуем завести отдельную СИМ-карту для самых важных сервисов и её не вводить ни на каких сторонних сайтах. Свои личные профили в соцсетях, при наличии, рекомендуем скрыть от посторонних. |
| **Защита от мошенников** | Учитывайте, что утекшие данные (ваши ФИО, телефон, адрес, состав заказов) могут использоваться для социальной инженерии. Критически относитесь к любым звонкам «из службы безопасности», «полиции» или «Госуслуг». Знание мошенниками ваших личных данных не делает их официальными лицами. |
| **Регулярный контроль** | Периодически проверяйте раздел «Активные сессии» («Связанные устройства») в Telegram, WhatsApp, Max — завершайте все незнакомые сеансы. Настройте уведомления о новых утечках через специализированные сервисы мониторинга (напр., Have I Been Pwned). Особенно рекомендуем приобрести услугу постоянного мониторинга от Лаборатории Пересвет |

## 5. ПРАВОВАЯ ОГОВОРКА

Настоящий отчёт носит исключительно информационный характер. Все данные получены из общедоступных источников в рамках законодательства Российской Федерации. Peresvet Lab не несёт ответственности за использование сведений, содержащихся в данном документе, третьими лицами. Отчёт предназначен только для субъекта персональных данных или его законного представителя. Несанкционированное копирование, распространение или публикация данного документа запрещены. Политика конфиденциальности Лаборатории Пересвет доступна по адресу https://peresvetlab.ru/privacy.html