

OSINT

LIVE CONNECTIONS VIEWER — ANZEIGE DER AKTIVEN VERBINDUNGEN

Die kostenlosen Schlüssel, die die tiefen Prüfungen einschalten — wo du sie bekommst, wie du sie hinzufügst, wie du sie benutzt.

GETTING YOUR KEYS — DEINE SCHLÜSSEL BEKOMMEN

SCHLÜSSEL-ANLEITUNG · OKTOBER 2026

777 SOFTWARE

KOSTENLOS — UND ES BLEIBT KOSTENLOS

1 — WARUM ÜBERHAUPT SCHLÜSSEL?

OSINT funktioniert in dem Moment, in dem du es öffnest. Die Tafel füllt sich mit deinen aktiven Verbindungen, die Listen bekannter schlechter Adressen werden dagegen geprüft, und jede Zeile bekommt eine Bewertung in klaren Worten. Für all das brauchst du keinen Schlüssel, und es gibt kein Konto zu erstellen — nicht bei uns, nicht bei jemandem.

Was ein Schlüssel hinzufügt, ist Tiefe. Vier fremde Dienste führen jeder eine andere Art von Gedächtnis über Internetadressen — wer wegen Missbrauchs gemeldet wurde, was Dutzende Scanner denken, ob eine Adresse Teil des Hintergrundrauschens des Internets ist, ob ein Host Malware-Links ausgeliefert hat. Jeder Dienst gibt dir einen kostenlosen persönlichen Schlüssel — eine kurze geheime Textzeile — und wenn du diesen Schlüssel in OSINT einfügst, kann die App diesen Dienst in deinem Namen, auf deinem Kontingent, zu den Adressen auf deiner Tafel befragen.

Jeder Schlüssel in dieser Anleitung ist kostenlos, direkt vom Dienst selbst. Wenn dich eine Seite jemals nach einer Karte fragt, bist du im falschen Tarif — schließe sie und nimm den kostenlosen, der in den Schritten genannt wird.

VirusTotal	Wie viele Sicherheitsscanner markieren diese Adresse Ja — ein kostenloser Schlüssel schaltet seine Schaltfläche ein
AbuseIPDB	Wurde diese Adresse wegen Missbrauchs gemeldet, und wie stark Ja — ein kostenloser Schlüssel schaltet sie ein (dann läuft sie von selbst)
abuse.ch — URLhaus	Hat dieser Host Malware-Links ausgeliefert Ja — ein kostenloser Auth-Key schaltet seine Schaltfläche ein

Deine Schlüssel sind deine. OSINT speichert sie in einer einzigen Einstellungsdatei auf deinem eigenen Computer, gesperrt auf dein eigenes Konto. Sie werden niemals hochgeladen, niemals an 777 Software gesendet und niemals in irgendeinen Download aufgenommen. Wenn eine Prüfung läuft, sendet die App die Adresse, die geprüft wird — und deinen Schlüssel — an den eigenen Dienst dieses Schlüssels, und nirgendwo sonst hin. Das ist die ganze Vereinbarung, und §6 zeigt dir genau, wohin die Schlüssel gehen.

2 — VIRUSTOTAL

Was es beantwortet: Dutzende Sicherheitsscanner stimmen über eine Adresse ab. OSINT zeigt ihre Zahl in klaren Worten — wie viele sagen bösartig, wie viele verdächtig, wie viele harmlos.

Wohin du gehst: virustotal.com

1. Wähle auf der Startseite von VirusTotal Join us (Mach mit), um ein kostenloses Konto zu beginnen.
2. Fülle das Formular aus: dein Vorname, Nachname, deine E-Mail-Adresse, ein Benutzername und ein Passwort. (Sie bieten auch eine Google-Anmeldung an — das schriftliche Formular funktioniert genauso.)
3. Bestehe die Prüfung „I'm not a robot“ („Ich bin kein Roboter“) und sende das Formular ab. Die Seite antwortet „Signed up successfully.“ („Erfolgreich angemeldet.“)
4. Öffne die E-Mail, die sie dir senden, und klicke auf den Aktivierungslink. Ohne diesen Klick bleibt das Konto im Schlaf.
5. Melde dich an. Öffne dein Profilmenü und wähle die Seite API key (API-Schlüssel) — dein persönlicher Schlüssel wird dort gezeigt.
6. Kopiere den ganzen Schlüssel. §6 zeigt dir, wohin er in OSINT gehört.

Der kostenlose Tarif: ein normales kostenloses Konto. Die Seite API key sagt das, und das kostenlose öffentliche Kontingent beträgt 500 Nachforschungen pro Tag — weit mehr, als eine Person, die Verbindungen von Hand prüft, je brauchen wird.

Eine ehrliche Anmerkung, ganz im Sinne von VirusTotal: Jede Adresse, die über ihre API geprüft wird, wird zum VirusTotal-Datensatz hinzugefügt und kann von ihrer Gemeinschaft gesehen werden. OSINT sagt dasselbe direkt in seinen Settings (Einstellungen), neben dem VirusTotal-Feld. Wenn dir dieser Tausch nicht behagt, lasse das Feld leer — der Rest von OSINT funktioniert ohne ihn.

3 — ABUSEIPDB

Was es beantwortet: Wurde diese Adresse wegen Missbrauchs gemeldet — Spam, Angriffe, Abtasten — und wie sicher ist sich die Menge? OSINT zeigt es als Missbrauchs-Vertrauenswert von

100, mit der Zahl der Meldungen. Von den vier Schlüsseln ist dies derjenige, den die App selbst die beste Bewertung für „wurde diese Adresse als sich danebennehmend gemeldet?“ nennt.

Wohin du gehst: abuseipdb.com

1. Wähle Register (Registrieren) und nimm den Tarif Individual FREE (Einzelperson KOSTENLOS). Kostenlos heißt kostenlos — keine Karte, niemals.
2. Fülle deinen Vornamen, Nachnamen, deine E-Mail-Adresse und dein Land aus, registriert als Individual (Einzelperson). Das Feld für den Benutzernamen kann leer bleiben.
3. Setze dein Passwort und bestehe die Prüfung „I'm not a robot“ („Ich bin kein Roboter“). Die Seite antwortet: „Your account has been created.“ („Dein Konto wurde erstellt.“)
4. Bestätige deine E-Mail, bevor du irgendetwas anderes tust. Öffne die Bestätigungs-E-Mail, die sie dir senden, und klicke auf ihren Link. Die Seite Keys (Schlüssel) bleibt gesperrt, bis du das tust — das ist der Schritt, den alle verpassen.
5. Zurück auf der Seite, öffne dein Account (Konto), dann API Keys (API-Schlüssel). Erstelle einen Schlüssel (der Name liegt bei dir — „My App“ ist in Ordnung).
6. Drücke Show (Zeigen), um den Schlüssel zu enthüllen, und kopiere das Ganze. §6 zeigt dir, wohin er in OSINT gehört.

Der kostenlose Tarif: Der Tarif Individual ist für immer kostenlos — 1.000 Prüfungen und Meldungen — und die Registrierungsseite sagt das in klaren Worten, bevor du dich anmeldest.

Später keine Schaltfläche zu drücken: Sobald dein AbuseIPDB-Schlüssel in OSINT gespeichert ist (§6), führt die App diese Prüfung von selbst für die fremden Adressen auf deiner Tafel aus. Ihre Antwort erscheint in der Detailansicht unter WHAT THE CHECKS SAID (WAS DIE PRÜFUNGEN GESAGT HABEN), in der Zeile AbuseIPDB — Wert, Meldungen und wann sie zuletzt gesprochen hat.

4 — GREYNOISE

Was es beantwortet: Ist diese Adresse Teil des Hintergrundrauschens des Internets — das endlose Abtasten, das über alle hinwegspült — oder ist sie etwas Selteneres? GreyNoise führt außerdem eine Menge bekannter harmloser Dienste, so dass eine berühmte, wohlerzogene Adresse genau als das gelesen wird.

Wohin du gehst: greynoise.io

1. Wähle Sign Up (Anmelden) und nimm die kostenlose Option Personal email (Private E-Mail).
2. Gib deine E-Mail-Adresse ein und setze ein Passwort.
3. Vervollständige dein Profil — Vorname und Nachname (das Feld für den Titel kann leer bleiben). Die Seite öffnet den Rest nicht, bevor das gespeichert ist.
4. Klicke auf den Bestätigungslink, den sie dir per E-Mail senden. Dein kostenloses Konto ist jetzt aktiv.

Jetzt der ehrliche Teil — lies das, bevor du nach einem Schlüssel suchst: Ein Konto mit privater E-Mail enthält keinen API-Schlüssel. GreyNoise sagt das auf der eigenen Seite des Kontos: Schlüssel werden an Konten mit Arbeits-E-Mail gegeben. Das ist ihre Regel, und es gibt keine Seite mit kostenlosem Schlüssel, die sich irgendwo versteckt und die du verpasst hättest.

Und die gute Nachricht: OSINT braucht keinen. Die Schaltfläche Check with GreyNoise (Mit GreyNoise prüfen) funktioniert ganz ohne Schlüssel, innerhalb eines kleinen kostenlosen Tageskontingents. Ist das Tageskontingent aufgebraucht, sagt die Ansicht das in klaren Worten — „Free allowance used up — press the button again tomorrow“ („Kostenloses Kontingent aufgebraucht — drücke die Schaltfläche morgen wieder“) — und jede andere Prüfung arbeitet weiter.

Wenn du eine Arbeits-E-Mail hast (die Adresse deiner eigenen Firma oder Organisation — nicht Gmail): Du kannst damit ein GreyNoise-Konto erstellen, und dieses Konto kommt mit einem Schlüssel, der in seinen Kontoeinstellungen gezeigt wird. Füge ihn genauso in OSINT ein wie die anderen (§6). Alles, was er kauft, ist ein wenig mehr Kontingent — die App selbst sagt es klar: Ein Schlüssel „erhöht das winzige kostenlose GreyNoise-Kontingent ein wenig“ (kostenlose Schlüssel reichen für etwa 50 Nachforschungen pro Woche). Niemand braucht ihn; er ist da, falls du ihn je willst.

5 — ABUSE.CH (DER URLHAUS-SCHLÜSSEL)

Was es beantwortet: abuse.ch betreibt URLhaus, eine Liste von Hosts, die dabei erwischt wurden, Malware-Links auszuliefern. OSINT fragt: Hat dieser Host Malware-Links ausgeliefert? Ein Ja hier ist eine laute Antwort — die Ansicht zeigt eine Warnzeile, die die Bedrohung benennt.

Wohin du gehst: auth.abuse.ch — das Anmeldehaus für abuse.ch.

1. Tippe deine E-Mail-Adresse in das Feld sign-in link by email (Anmeldelink per E-Mail).
2. Bestehe die Prüfung „Verify you are human“ („Bestätige, dass du ein Mensch bist“) — ein echter Mensch besteht sie in einer Sekunde; sie ist da, um Roboter aus einem kostenlosen Dienst herauszuhalten.
3. Drücke „Email me a sign-in link.“ („Sende mir einen Anmeldelink per E-Mail.“)
4. Öffne die E-Mail, die ankommt, und klicke auf ihren Anmeldelink. Es gibt kein Passwort zu erfinden — der Link ist der Schlüssel zur Tür.
5. Deine Profilseite zeigt deinen Auth-Key. Kopiere das Ganze. §6 zeigt dir, wohin er in OSINT gehört — in das Feld mit der Beschriftung abuse.ch Auth-Key.

Der kostenlose Tarif: Ein abuse.ch-Konto ist kostenlos. Der Auth-Key auf deinem Profil ist das einzige Zugangsmittel, das OSINT von ihnen braucht.

6 — DEINE SCHLÜSSEL IN OSINT EINTRAGEN

Derselbe Weg für jeden Schlüssel. Tu es einmal pro Dienst, in beliebiger Reihenfolge, wann immer du jeden Schlüssel bekommst — OSINT braucht nicht alle vier, und jeder schaltet sich in dem Moment ein, in dem er gespeichert wird.

1. Öffne OSINT.
2. Drücke die Schaltfläche Settings (Einstellungen, untere Leiste). Das Fenster OSINT — Settings öffnet sich.
3. Finde das Feld für deinen Dienst. Das Fenster zeigt vier, in dieser Reihenfolge: AbuseIPDB key, VirusTotal key, abuse.ch Auth-Key, GreyNoise key. Jedes Feld versteckt, was du tippst, hinter Punkten, und unter jedem erinnert dich die App: „Key saved on this computer only.“ („Schlüssel nur auf diesem Computer gespeichert.“)
4. Füge den ganzen Schlüssel in sein Feld ein — keine Leerzeichen am Anfang oder Ende.
5. Drücke Save Settings (Einstellungen speichern). Das Fenster antwortet: „Saved — on this computer only.“ („Gespeichert — nur auf diesem Computer.“) Das ist erledigt — der Schlüssel bleibt über Neustarts hinweg gespeichert; du fügst ihn nicht noch einmal ein.

Die Feldnamen, zugeordnet zu §2–§5:

- VirusTotal key (§2) → das Feld VirusTotal key
- AbuseIPDB key (§3) → das Feld AbuseIPDB key
- GreyNoise key (§4, nur Konten mit Arbeits-E-Mail) → das Feld GreyNoise key
- abuse.ch Auth-Key (§5) → das Feld abuse.ch Auth-Key — das ist der Schlüssel, der die URLhaus-Prüfung einschaltet

Die Produktwahrheiten, klar gesagt

- **Speichern heißt gespeichert.** Save Settings schreibt jedes Feld im Fenster — dauerhaft, bis du es änderst.
- **Eine Datei, dein Computer, dein Konto.** Die Schlüssel leben nur in OSINTs lokaler Einstellungsdatei, so gesperrt, dass nur dein eigenes Benutzerkonto sie lesen kann (Dateiberechtigungen 0600). Die Datei wird niemals irgendwohin hochgeladen und ist niemals Teil irgendeines Downloads.
- **Ein Schlüssel ist ein Geheimnis.** Behandle ihn wie einen Hausschlüssel: Poste ihn nicht, schicke ihn nicht herum, füge ihn nicht in Webseiten ein, die aus dem Nichts danach fragen. Die einzigen Orte, an die er je gelangt, sind der Dienst, der ihn ausgestellt hat, und OSINTs Feld in den Settings.
- Einen Schlüssel entfernen: Öffne Settings, leere das Feld, drücke Save Settings. Diese Prüfung schaltet sich wieder aus (bei GreyNoise kehrt die Schaltfläche einfach zu ihrem kostenlosen schlüssellosen Kontingent zurück).
- Einen Schlüssel ändern: Füge den neuen über den alten ein und speichere. Erledigt.

7 — DIE PRÜFUNGEN LAUFEN LASSEN

1. Klicke auf der Tafel auf eine Verbindung. Die Detailansicht unter der Tafel zeigt diese Verbindung — wer sie ist und was die Prüfungen über sie gesagt haben.
2. Unter der Ansicht sitzen die Prüfungsschaltflächen: Copy IP (IP kopieren), Check with GreyNoise, Check with VirusTotal, Check with URLhaus. Drücke die, die du willst.

3. Die Ansicht sagt dir, dass die Prüfung läuft, und ihre Antwort landet in derselben Ansicht, unter WHAT THE CHECKS SAID (WAS DIE PRÜFUNGEN GESAGT HABEN).

Die Schaltflächen wirken nur auf die Verbindung, die du ausgewählt hast, und nur, wenn du sie drückst — und sie funktionieren bei Verbindungen nach draußen (öffentlichen). Wähle eine Zeile innerhalb deines eigenen Heimnetzwerks, und die Ansicht wird dir sagen: „Pick an outside connection first.“ („Wähle zuerst eine Verbindung nach draußen.“) Über deine eigenen privaten Adressen wird niemals etwas hinausgesendet.

Was jede Antwort bedeutet, in einer Zeile

- **VirusTotal:** „N engines say malicious · N suspicious · N harmless“ („N Engines sagen bösartig · N verdächtig · N harmlos“) — die Abstimmung der Scanner, offen gezählt.
- **AbuseIPDB:** „Abuse confidence N/100 · N reports“ („Missbrauchs-Vertrauen N/100 · N Meldungen“) — wie stark die meldende Menge glaubt, dass sich diese Adresse danebenbenimmt. Keine Schaltfläche: Mit gespeichertem Schlüssel läuft diese Prüfung von selbst, und ihre Zeile erscheint mit den anderen.
- **GreyNoise:** ob die Adresse als „seen scanning the internet“ („beim Abtasten des Internets gesehen“) gilt, als was sie eingestuft ist und ob sie in der Menge der bekannten harmlosen Dienste sitzt — Hintergrundrauschen gegenüber etwas, auf dem dein Name steht.
- **URLhaus:** still, wenn es nichts zu sagen gibt; eine ■-Warnzeile — „This host has served malware links“ („Dieser Host hat Malware-Links ausgeliefert“) — wenn es etwas gibt.

Über diesen Zeilen gibt die Ansicht die Bewertung — die schlechteste ehrliche Lesart von allem, was die Prüfungen gesagt haben: KNOWN BAD, SUSPICIOUS, KNOWN SAFE oder NO BAD REPORTS (von der die App sorgfältig sagt, dass sie kein Versprechen ist, dass es sicher ist) — gefolgt von einem Abschnitt WHAT SHOULD I DO? (WAS SOLLTE ICH TUN?) in klaren Worten.

Noch keinen Schlüssel? Die Schaltflächen sagen dir die Wahrheit, statt still zu fehlschlagen. Drücke Check with VirusTotal, ohne dass ein Schlüssel gespeichert ist, und die Ansicht antwortet: „VirusTotal is OFF — add your own free key in Settings to turn it on.“ („VirusTotal ist AUS — füge deinen eigenen kostenlosen Schlüssel in den Settings hinzu, um es einzuschalten.“) URLhaus antwortet auf dieselbe Weise: „URLhaus needs your free abuse.ch key — add it in Settings.“ („URLhaus braucht deinen kostenlosen abuse.ch-Schlüssel — füge ihn in den Settings hinzu.“) GreyNoise fragt nach nichts — es läuft einfach.

8 — SCHLÜSSELSICHERHEIT + WENN ETWAS FALSCH AUSSIEHT

- **Ein Schlüssel ist durchgesickert?** Gehe zurück zu diesem Dienst, erstelle einen frischen Schlüssel und lösche den alten — jeder Dienst in dieser Anleitung lässt dich beides tun — und füge dann den neuen Schlüssel in OSINT ein (§6). Der alte Schlüssel stirbt beim Dienst, also ist eine durchgesickerte Kopie wertlos.
- **„Free allowance used up“ (Kostenloses Kontingent aufgebraucht, GreyNoise):** kein Fehler. Die Prüfungen des kostenlosen Tages sind ausgegeben; die Schaltfläche funktioniert morgen wieder, und alles andere arbeitet heute Nacht weiter.

- **Eine Prüfung sagt „failed“ (fehlgeschlagen):** Der Dienst hat nicht geantwortet — die Ansicht zeigt die Adresse als für diese Prüfung unbekannt, niemals als freigegeben. Versuche es später erneut; ein ehrliches „keine Antwort“ ist das Design, kein Fehler.
- **Irgendwo wirst du nach einer Karte gefragt:** Halte an. Jeder Schlüssel in dieser Anleitung ist kostenlos. Eine Kartenanfrage bedeutet, dass aus Versehen ein bezahlter Tarif gewählt wurde — steige aus und wähle den kostenlosen, der in den Schritten genannt wird.
- **Den Schlüssel verloren, den du erstellt hast?** Melde dich wieder beim Dienst an — VirusTotal und abuse.ch zeigen deinen Schlüssel auf deiner Profil-/API-Seite; bei AbuseIPDB drückst du Show (Zeigen) neben dem Schlüssel, den du erstellt hast. Dann wieder §6.

Das ist alles. Vier kostenlose Schlüssel, jeder von seinem eigenen Dienst geholt, einmal in die Settings eingefügt, von deinem eigenen Computer aus arbeitend — und eine App, die dir klar sagt, was sie sendet, was sie gefunden hat und was sie nicht weiß. Prüfe, mit wem dein Rechner spricht. Dafür ist OSINT da.

OSINT — Live Connections Viewer · 777 Software. Diese Anleitung wird mit der App ausgeliefert. Die hier genannten Dienste werden von ihren eigenen Leuten betrieben; ihre Anmeldeseiten mögen ihre Möbel mit der Zeit umräumen, aber die Form — kostenloses Konto, E-Mail bestätigen, Schlüssel auf deinem Profil finden — ändert sich nicht.