



Schieb Report

Ausgabe 2024.01

Infostealer: Wie schützt du dich effektiv vor dieser digitalen Bedrohung?



Infostealer stellen eine ernsthafte Bedrohung für deine Daten und Informationen dar. Um dich effektiv davor zu schützen, gibt es verschiedene Maßnahmen, die du ergreifen kannst.

Dazu gehören beispielsweise die Nutzung von Cloud-Services, die Verwendung von Anti-Malware-Programmen und die Zusammenarbeit mit einem erfahrenen IT-Security-Partner. Informiere dich über aktuelle Trends und lerne, wie du dein System und Netzwerk sicherer machen kannst. Denn deine Daten sind wertvoll und sollten immer geschützt sein.

Was sind Infostealer und warum solltest du dich davor schützen?

Infostealer sind eine der größten digitalen Bedrohungen für die Sicherheit deiner Daten und Informationen. Diese Malware hat das Ziel, vertrauliche Daten wie Passwörter und Kreditkarteninformationen zu stehlen. Die Infostealer können auf

verschiedene Arten in dein System gelangen, zum Beispiel über E-Mails oder Downloads aus dem Internet.

Infostealer arbeiten im Hintergrund und sammeln Informationen, ohne dass du es bemerkst. Es ist wichtig, dich vor dieser Bedrohung zu schützen, da sie nicht nur deine persönlichen Informationen gefährdet, sondern auch Cloud-Daten und Netzwerke beeinträchtigen kann.

In diesem Artikel erfährst du alles Wichtige über Infostealer: Wie erkennst du sie? Welche Arten gibt es? Welche Daten werden gestohlen? Und vor allem: Wie kannst du dich effektiv davor schützen? Es ist von großer Bedeutung, dass du deine digitale Sicherheit ernst nimmst und Maßnahmen ergreifst, um dich vor den Gefahren der Infostealer zu schützen.



Neue Malware missbraucht Cookies und verschafft sich so Zugang zu Google Konten

Erkennungsmerkmale von Infostealern: Wie erkennst du, ob dein Gerät infiziert ist?

Infostealer stellen eine ernsthafte Bedrohung für die Sicherheit deiner Daten dar. Deshalb ist es wichtig, dass du weißt, wie du erkennen kannst, ob dein Gerät

infiziert ist. Ein Erkennungsmerkmal von Infostealern sind ungewöhnliche Aktivitäten auf deinem System oder Netzwerk.

Zum Beispiel kann ein Anstieg des Datenverkehrs oder der CPU-Auslastung ein Hinweis darauf sein, dass Malware im Hintergrund läuft und Informationen sammelt. Eine weitere Möglichkeit, um verdächtige Aktivitäten zu erkennen, besteht darin, deine Cloud-Dienste und -Konten regelmäßig zu überprüfen. Wenn du feststellst, dass sich unbekannte Dateien in der Cloud befinden oder Zugriffe auf deine Daten stattfinden, ohne dass du sie autorisiert hast, solltest du alarmiert sein und sofort Maßnahmen ergreifen.

Um dich effektiv vor Infostealern zu schützen, empfiehlt es sich auch immer aktuelle Antivirus-Software zu verwenden und regelmäßige Updates durchzuführen. Darüber hinaus solltest du sicherstellen, dass deine Passwörter sicher genug sind und immer auf dem neuesten Stand gehalten werden.

Indem du diese Vorsichtsmaßnahmen ergreifst und achtsam beim Umgang mit persönlichen Informationen bist, kannst du dich wirksam gegen die Bedrohung durch Infostealer schützen und deine digitalen Daten bewahren.



Die verschiedenen Arten von Infostealern und ihre

Funktionsweise

In diesem Abschnitt geht es um die verschiedenen Arten von Infostealern und ihre Funktionsweise. Es gibt eine Vielzahl von Infostealer-Malware, die alle unterschiedliche Funktionen haben.

Einige stehlen Daten aus der Cloud-Storage, während andere sich in das Netzwerk einklinken und Informationen über das System oder den Benutzer sammeln. Manche Infostealer-Stämme zielen auf spezifische Services ab, wie zum Beispiel Online-Banking-Dienste oder E-Mail-Clients. Die meisten Infostealer sammeln jedoch allgemeine Informationen wie Passwörter, Kreditkartennummern und persönliche Daten, um sie an einen Remote-Server zu senden.

Ein häufiger Typ von Infostealern ist der **Keylogger**. Diese Malware zeichnet Tastatureingaben auf und sendet sie an den Angreifer zurück. Andere Arten von Infostealern sind Formgrabber, die nach dem Ausfüllen eines Formulars im Browser die eingegebenen Informationen speichern und auch Screenshots machen können.

Eine weitere Art ist Backdoor-Infostealer, welche Hintertüren ins System öffnen können. Es gibt auch fortschrittlichere Varianten wie RATs (Remote Access Trojans), die einem Angreifer Zugriff auf ein infiziertes Gerät geben können.

Diese Art von Malware kann verwendet werden, um sensible Daten zu stehlen oder sogar das ganze System zu kontrollieren.

Um sich effektiv vor dieser digitalen Bedrohung zu schützen ist es wichtig zu verstehen, wie diese verschiedene Arten von Infostealern funktionieren und verbreitet werden könnten. Mit diesem Wissen kannst du geeignete Maßnahmen ergreifen um dich vor Infostealer-Angriffen zu schützen.



Trojaner: Kommen verdeckt - benannt nach dem berühmten Vorbild in der Antike

Welche Daten werden von Infostealern gestohlen?

Infostealer sind eine ernsthafte Bedrohung für unsere digitale Sicherheit. Sie können auf verschiedene Arten in unser System eindringen und vertrauliche Daten stehlen. Aber welche Daten werden von Infostealern gestohlen? Es gibt keine klare Antwort, da verschiedene Arten von Infostealern unterschiedliche Daten stehlen können.

In der Regel zielen sie jedoch auf unsere persönlichen Informationen ab, wie Login-Daten, Passwörter, Kontoinformationen und Kreditkartendaten. Einige können auch sensible Geschäftsdaten oder geistiges Eigentum stehlen.

Es ist wichtig zu verstehen, dass Infostealer nicht nur auf unseren lokalen Geräten agieren können, sondern auch über das Netzwerk oder die Cloud auf andere Systeme zugreifen können. Daher müssen wir uns bewusst sein, welche Art von

Daten wir speichern und wie wir diese schützen können.

Es ist ratsam, regelmäßig Backups unserer wichtigen Daten durchzuführen und starke Passwörter zu verwenden. Wir sollten auch sicherstellen, dass unsere Antivirus-Software immer auf dem neuesten Stand ist und alle Updates für unser Betriebssystem installiert wurden, um potenzielle Schwachstellen zu schließen und uns vor neuen Bedrohungen zu schützen.

Vorsichtsmaßnahmen gegen Infostealer: Wie kannst du dich effektiv schützen?

Um dich effektiv vor Infostealern zu schützen, gibt es einige Vorsichtsmaßnahmen, die du unbedingt beachten solltest. Eine davon ist das regelmäßige Updaten deines Systems und deiner Antivirus-Software. So können bekannte Schwachstellen geschlossen werden und dein Gerät wird weniger anfällig für Angriffe von Infostealern.

Außerdem solltest du darauf achten, sichere Passwörter zu verwenden und diese regelmäßig zu ändern. Ein weiterer wichtiger Punkt ist das sensibilisierte Surfen im Internet sowie der vorsichtige Umgang mit persönlichen Informationen in E-Mails oder sozialen Medien.

Auch der Einsatz von Cloud-Services, die eine hohe Sicherheit bieten, kann eine gute Möglichkeit sein, um deine Daten vor Infostealern zu schützen. Es empfiehlt sich außerdem immer auf dem neuesten Stand in Bezug auf die verschiedenen Arten von Infostealern zu bleiben und dank trendMicro oder anderen Partnern stets über aktuelle Bedrohungen informiert zu sein.

Mit diesen Vorsichtsmaßnahmen kannst du dich effektiv gegen Infostealer schützen und sicher im digitalen Raum agieren.



Antivirus-Software als Schutz vor Infostealern

Als effektive Vorsichtsmaßnahme gegen Infostealer empfiehlt sich der Einsatz von Antivirus-Software. Diese kann dabei helfen, Schadsoftware zu erkennen und zu blockieren, bevor sie Daten stehlen oder Schaden anrichten kann. Dabei sollte die Software regelmäßig aktualisiert werden, um auch gegen neue Bedrohungen gewappnet zu sein.

Zudem ist es wichtig, auf einen vertrauenswürdigen Anbieter zu setzen und dessen Support-Services in Anspruch nehmen zu können. Einige Antivirus-Programme bieten auch Cloud-basierte Services und Netzwerk-Security an, um das gesamte System vor Bedrohungen zu schützen.

Darüber hinaus können Nutzer durch den sensiblen Umgang mit persönlichen Informationen sowie sichere Passwörter weitere Angriffsmöglichkeiten von Infostealern minimieren. Mit diesen Maßnahmen lässt sich das Risiko eines erfolgreichen Angriffs durch Infostealer deutlich verringern und ein sicherer Umgang mit Daten und Informationen gewährleisten.

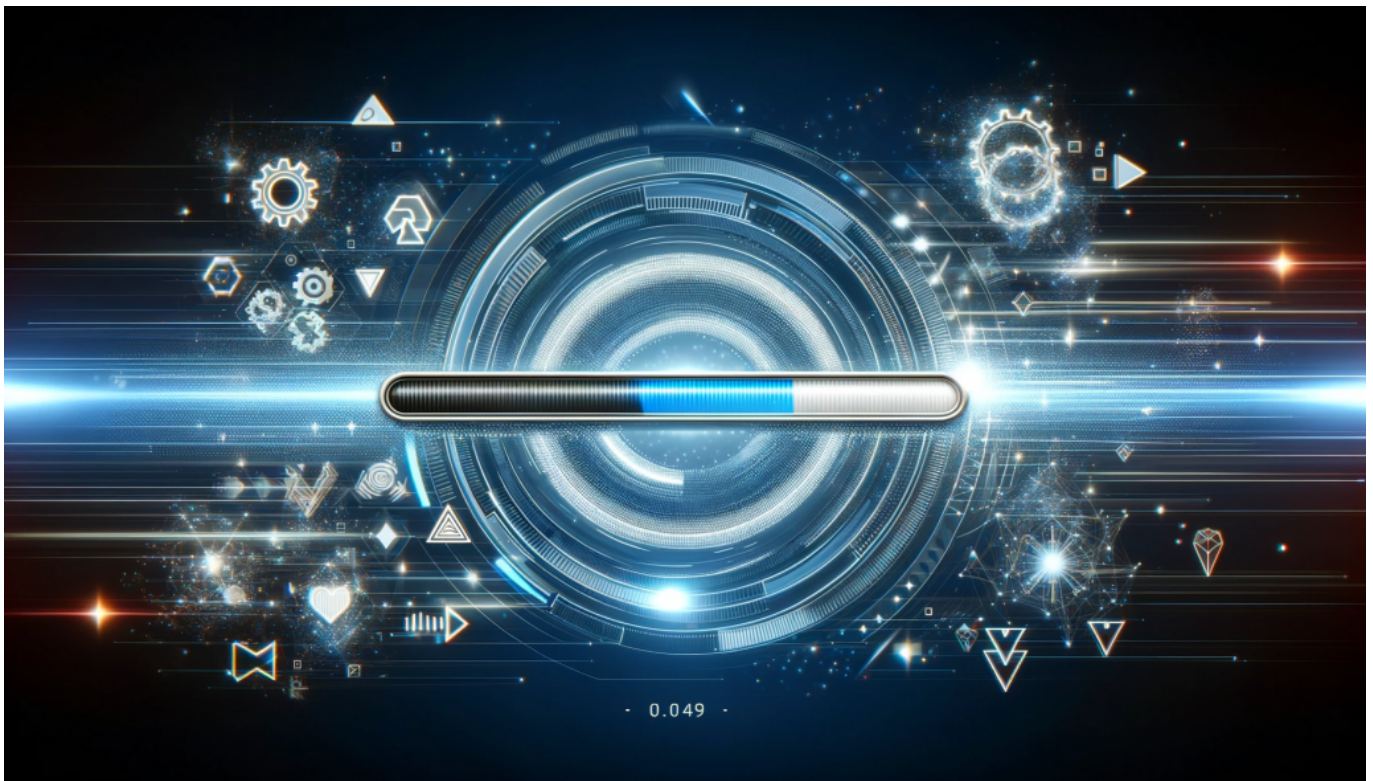
Regelmäßige Updates und sichere Passwörter zur Vermeidung von Angriffen durch Infostealer

Um sich effektiv vor Infostealern zu schützen, ist es wichtig regelmäßige Updates durchzuführen und sichere Passwörter zu verwenden. Denn Infostealer nutzen oft Sicherheitslücken in veralteter Software aus oder knacken schwache Passwörter, um an sensible Daten zu gelangen.

Regelmäßige Updates des Betriebssystems und der installierten Anwendungen können diese Lücken schließen und somit das Risiko eines Angriffs reduzieren. Auch die Verwendung von starken Passwörtern, die aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen, kann helfen, Angriffe durch Infostealer abzuwehren.

Zusätzlich empfiehlt es sich verschiedene Passwörter für unterschiedliche Dienste zu verwenden und diese regelmäßig zu ändern.

So wird das Risiko minimiert, dass ein Angreifer Zugang zu allen Konten erhält, wenn er nur ein Passwort knackt. Durch diese einfachen Vorsichtsmaßnahmen kannst du deine Daten besser schützen und dich vor den Gefahren der Infostealer bewahren.



Regelmäßige Updates helfen, Sicherheitslücken zu schließen

Sicherheitsbewusstes Surfen im Internet: Tipps zum

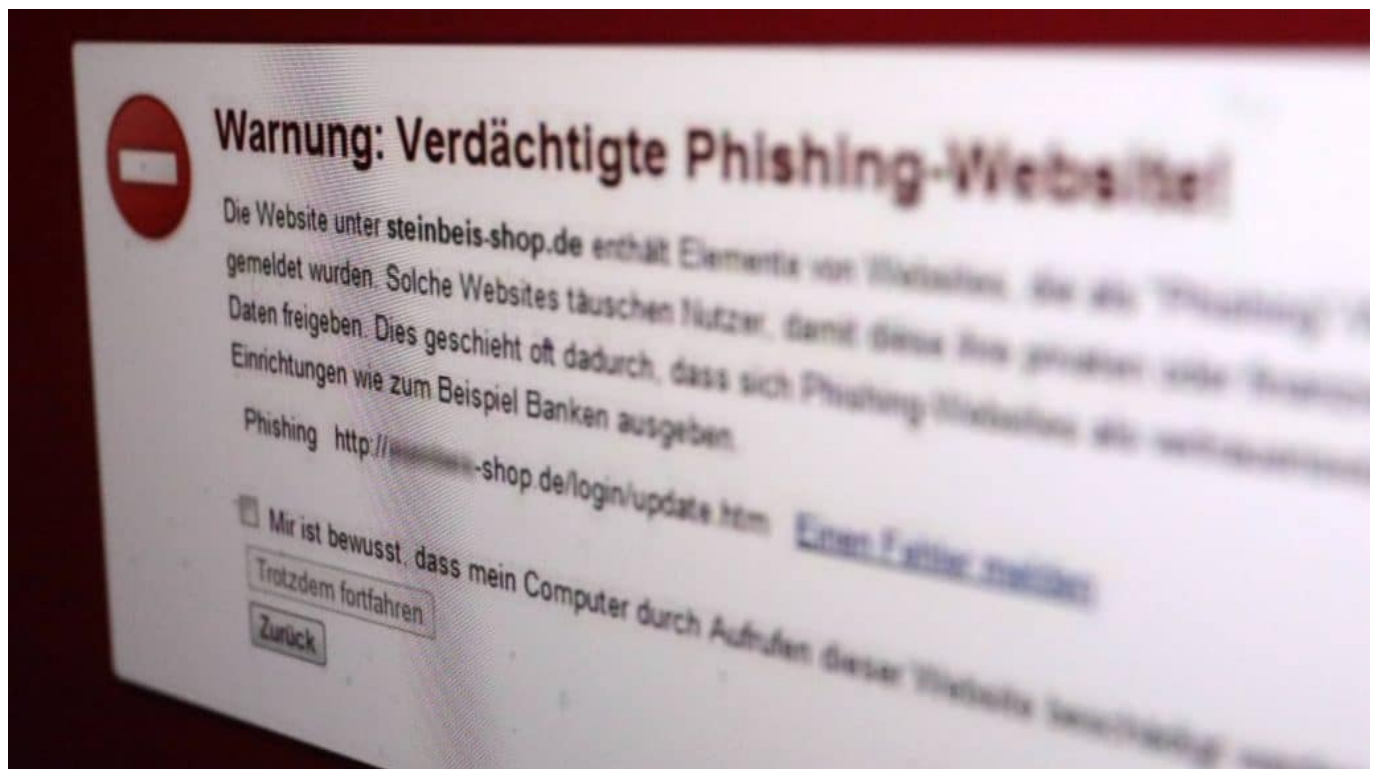
Schutz vor Phishing-Angriffen durch Infostealer

Ein weiterer wichtiger Aspekt, um sich vor Infostealern zu schützen, ist das Bewusstsein für Phishing-Angriffe. Dabei versuchen Cyberkriminelle, über gefälschte E-Mails oder Websites an persönliche Informationen wie Passwörter oder Kreditkartennummern zu gelangen.

Um dich davor zu schützen, solltest du immer misstrauisch sein bei E-Mails von unbekannten Absendern und niemals auf Links in solchen Nachrichten klicken. Auch wenn die Website vertraut aussieht, solltest du sicherstellen, dass die URL korrekt geschrieben ist und nicht irgendwelche Tippfehler oder zusätzliche Buchstaben enthält.

Um zusätzlichen Schutz zu bieten, kannst du auch eine Antiphishing-Software installieren. Es ist wichtig zu verstehen, dass Infostealer eine ernsthafte Bedrohung darstellen und sie können dein Leben stark beeinträchtigen, wenn sie erfolgreich sind.

Indem du diese Tipps befolgst und deinen digitalen Sicherheitsplan regelmäßig aktualisierst und überprüfst, kannst du sicherstellen dass deine Daten und Informationen geschützt bleiben und deine digitale Identität intakt bleibt.



Sensibler Umgang mit persönlichen Informationen in E-Mails und sozialen Medien, um nicht Opfer eines Datenlecks zu werden.

Ein weiterer wichtiger Faktor bei der Vermeidung von Datenlecks durch Infostealer ist der sorgsame Umgang mit persönlichen Informationen in E-Mails und sozialen Medien. Infostealer nutzen oft Phishing-Methoden, um Zugriff auf vertrauliche Daten wie Passwörter oder Bankdaten zu erhalten.

Achte darauf, keine verdächtigen Links anzuklicken oder auf Anfragen von unbekannten Personen zu antworten. Es ist auch ratsam, sensible Informationen nicht über unsichere Netzwerke oder Cloud-Services zu teilen.

Ein weiterer hilfreicher Tipp ist die Überprüfung von Datenschutzrichtlinien und Nutzungsbedingungen von Online-Diensten und -Partnern, um sicherzustellen, dass deine Daten sicher sind.

Eine regelmäßige Überprüfung deiner Kontoinformationen kann ebenfalls dazu beitragen, mögliche Angriffe frühzeitig zu erkennen und abzuwehren. Bleibe wachsam und achte darauf, wer Zugriff auf deine persönlichen Informationen hat - so kannst du dich effektiv vor den Gefahren von Infostealern schützen!

Effektiver Schutz vor digitaler Bedrohung: So bleibst du sicher vor den Gefahren der Infosteler!

Um dich effektiv vor den Gefahren der Infostealer zu schützen, gibt es einige Vorsichtsmaßnahmen, die du ergreifen kannst. Eine Möglichkeit ist die Verwendung von Antivirus-Software, um dein System auf mögliche Infektionen durch Malware und andere Bedrohungen zu überprüfen.

Regelmäßige Updates deiner Systeme und sichere Passwörter können auch dazu beitragen, Angriffe durch Infostealer zu vermeiden. Ein weiterer wichtiger Punkt ist das Bewusstsein für Sicherheit beim Surfen im Internet sowie ein sensibler Umgang mit persönlichen Informationen in E-Mails und sozialen Medien.

Durch diese Schritte kannst du bereits einen großen Schritt hin zu einem effektiven Schutz vor digitalen Bedrohungen machen.

Aber auch der Einsatz von Cloud-Services oder Netzwerksicherheits-Services kann dir helfen, deine Daten sicher zu halten und somit mögliche Diebstähle durch Infostealer zu verhindern. Zusammenfassend lässt sich sagen, dass es viele Möglichkeiten gibt, um dich gegen die Bedrohung durch Infostealer zu schützen - sei es durch den Einsatz von Software oder das Bewusstsein für Sicherheit im Umgang mit Daten und Informationen.

Neue Malware (Infostealer) ermöglicht Missbrauch von Google-Konten



Eine neue entdeckte schädliche Software (Malware) umgeht den Passwortschutz von Google-Konten durch unbemerkte Übernahme von Google-Cookies – Passwortwechsel bleibt ohne Effekt.

Der Lumma-Trojaner greift auf Browser-Daten und eine unbekannte Google-Funktion zu, um sich fortwährenden Zugang zu Nutzerkonten zu verschaffen.

Lumma Trojaner wendet neuen Trick an

Wird ein Computer von Schadsoftware befallen, gilt es als eine der ersten Maßnahmen, sämtliche Passwörter neu zu setzen. Doch es zeigt sich, dass diese Aktion nicht immer geeignet ist, um Online-Konten vor unbefugtem Zugriff zu schützen. Aktuelle Versionen unterschiedlicher Malware-Typen haben die Fähigkeit entwickelt, die verschlüsselten Authentifizierungszusätze für Google-Konten wiederherzustellen, sogar nachdem Nutzer ihr Passwort geändert haben könnten.

Schon im letzten Herbst starteten mehrere Gruppen aus dem cyberkriminellen Milieu den Verkauf einer innovativen Funktion ihrer Diebstahl-orientierten Schadprogramme. Nach der Einrichtung sammeln diese Programme gezielt sensible Informationen wie Anmeldedaten und Authentifizierungszusätze. Einige Entwickler solcher Schadsoftware preisen nun eine Fähigkeit an, die die Authentifizierungszusätze aktualisieren kann, was Änderungen am Passwort nutzlos macht.



Malware nutzt Schwachstelle in Google API

Eine Untersuchung von IT-Sicherheitsexperten bestätigt, dass diese Fähigkeit keine Finte ist. Mithilfe einer nicht öffentlich dokumentierten Schnittstelle von Google, die ursprünglich für die Synchronisation von Konteninformationen über verschiedene Endgeräte hinweg vorgesehen ist, kann die Malware gültige Cookies für entwendete Konten generieren.

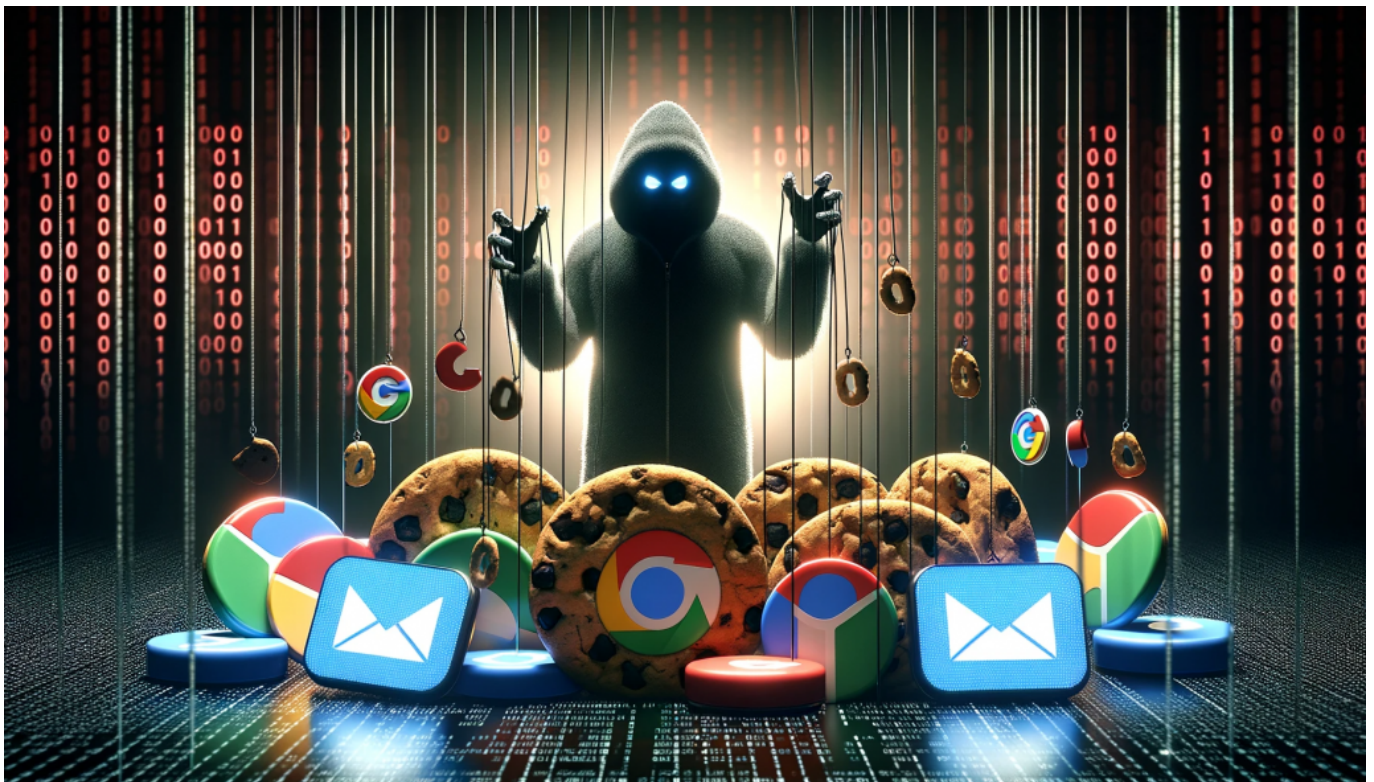
Die Schadsoftware lädt verschlüsselte Zugangstokens durch das API herunter und entschlüsselt sie, wobei sie die im Browser des Opfers entwendeten Schlüssel verwendet.

Passwortwechsel bieten keinen Schutz

Da die Authentifizierungstokens nicht an das Google-Passwort des Nutzers geknüpft sind, bleibt auch ein Passwortwechsel ohne Auswirkung und Täter erlangen weiterhin Zugang zu allen Google-Konten des Opfers, die während der Infektion aktiv waren.

Es ist bisher nicht bekannt, ob und wann Google diese Schwachstelle beheben wird, ebenso unklar ist, ob Nutzer effektive Schutzmaßnahmen ergreifen könnten. Angesichts der Tatsache, dass nun mehrere Schadsoftware-Varianten diesen Exploit nutzen, dürfte bei den Entwicklern von Google Alarmstimmung herrschen.

Probleme mit der Implementierung von OAuth oder das Abfangen von OAuth-Tokens haben bereits in der Vergangenheit zu Sicherheitsproblemen geführt, wie bei einem schwerwiegenden Angriff auf Github im Jahr 2022 deutlich wurde.



Selbst der Wechsel eines Passwortes macht keinen Unterschied

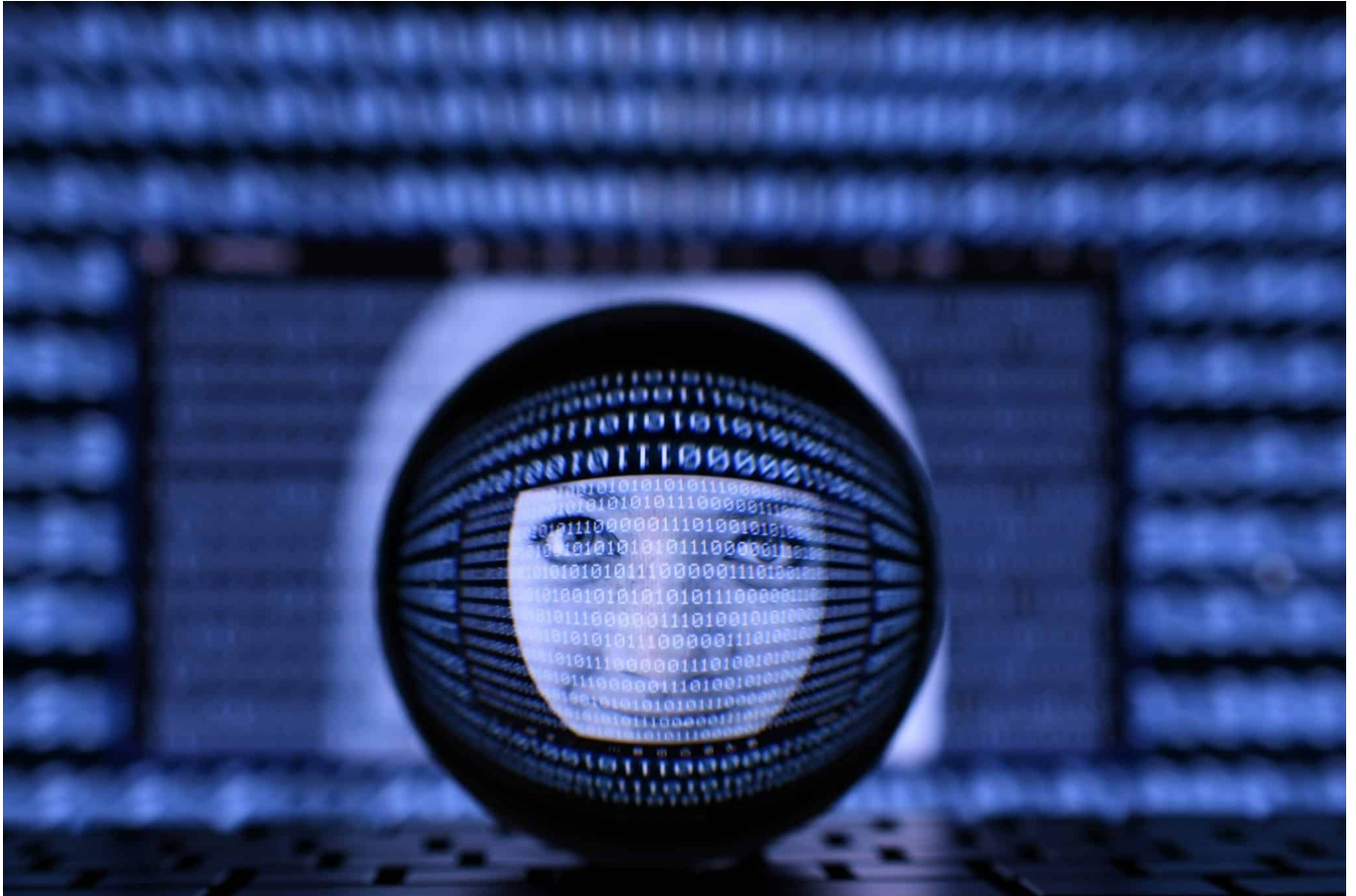
Das müssen Google-Nutzer jetzt tun

Es ist wichtiger denn je, darauf zu achten, sich keine Malware einzufangen. Also: Keine bedenklichen oder unsicheren Webseiten aufrufen, am besten Antiviren-Software benutzen und bei Bedenken mal den Rechner scannen. Sofern Malware entdeckt wurde, diese entfernen und anschließend die Passwörter aller Google-

Konten erneuern.

Ganz besonders wichtig: Multifaktor-Authentifizierung verwenden. Wer seine Online-Konten durch einen zweiten Code oder einen Hardware-Key absichert - was Google schon lange anbietet und auch empfiehlt -, kann seine Online-Konten deutlich besser schützen.

Bilder generieren mit Midjourney



Wolltet ihr immer schon mal hochwertige Bilder einfach "denken" können? Dann ist Midjourney eine tolle Alternative, die dem Wunsch sehr nah kommt. Formuliert in ein paar Worten den Inhalt, und schon bekommt ihr [KI-generiert](#) ein Bild.

Anlegen eines Kontos

Midjourney ist zwar ein eigenes Unternehmen, nutzt aber [Discord](#) als Oberfläche für die Generierung von Bildern. Vor allem deshalb, weil die Eingabemethoden des Chat-Dienstes dafür genutzt werden. Ihr müsst also als erstes ein Konto bei Discord anlegen:

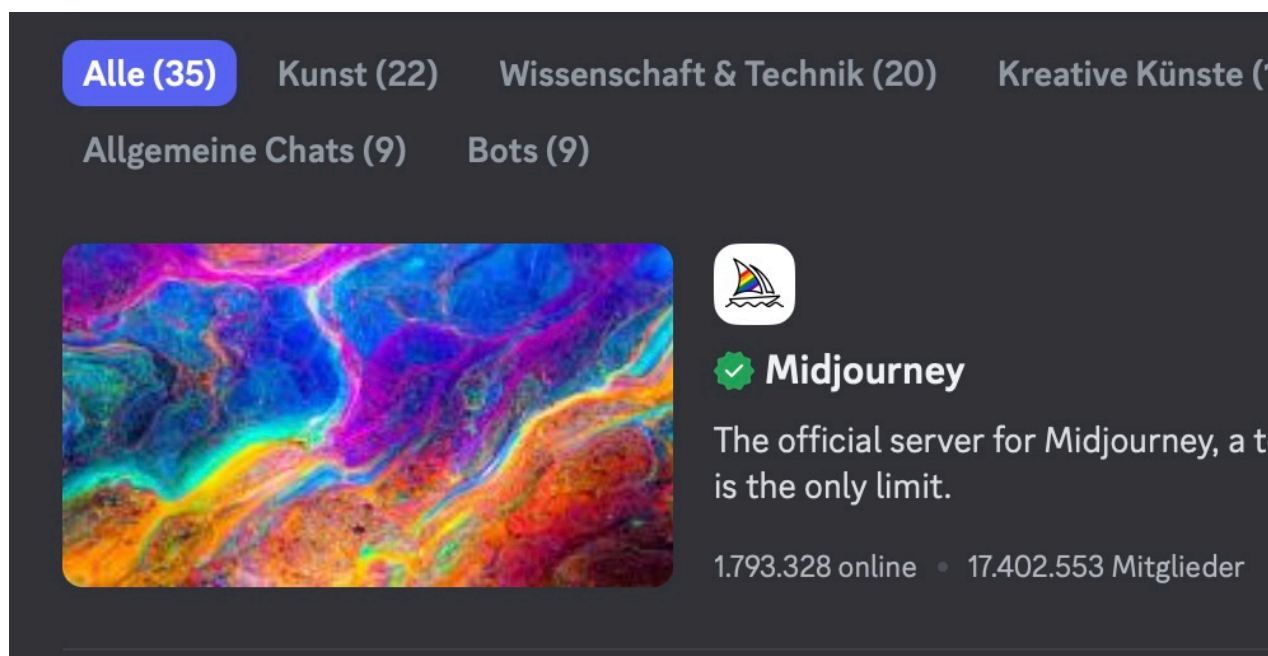
- Ruft die [Discord-Seite](#) auf, dann klickt auf **Login**.
- Wenn ihr noch kein Discord-Konto habt, dann klickt unten auf den kleinen Link **Registrieren**.

- Gebt dann eure E-Mail-Adresse, euren frei wählbaren Benutzer- und Anzeigenamen, euer Passwort und Geburtsdatum ein.
- Wenn der gewünschte Benutzername noch frei ist, dann bekommt ihr eine E-Mail von Discord, aus der ihr durch einen Klick auf einen Link eure Adresse bestätigen müsst.

Hinzufügen von Midjourney zu Discord

Midjourney ist für den normalen Benutzer über die Discord-Kanäle zu finden. Dazu müsst ihr einmal den Kanal suchen, dann wird er automatisch zu euren Kanälen in der Übersicht eures Kontos bei Discord hinzugefügt:

- Klickt in der Seitenleiste von Discord auf **Freunde**.
- Statt den Namen eines Discord-Benutzers einzugeben, klickt auf **Erkunde entdeckbare Server**.
- Gebt dort **Midjourney** ein.
- Klickt den Midjourney-Server an, um in dessen Kanäle zu wechseln.
- Um einen ersten Überblick zu bekommen, klickt auf den Kanal #getting-started, dieser enthält eine Vielzahl von hilfreichen Erklärungen, wie Midjourney funktioniert.

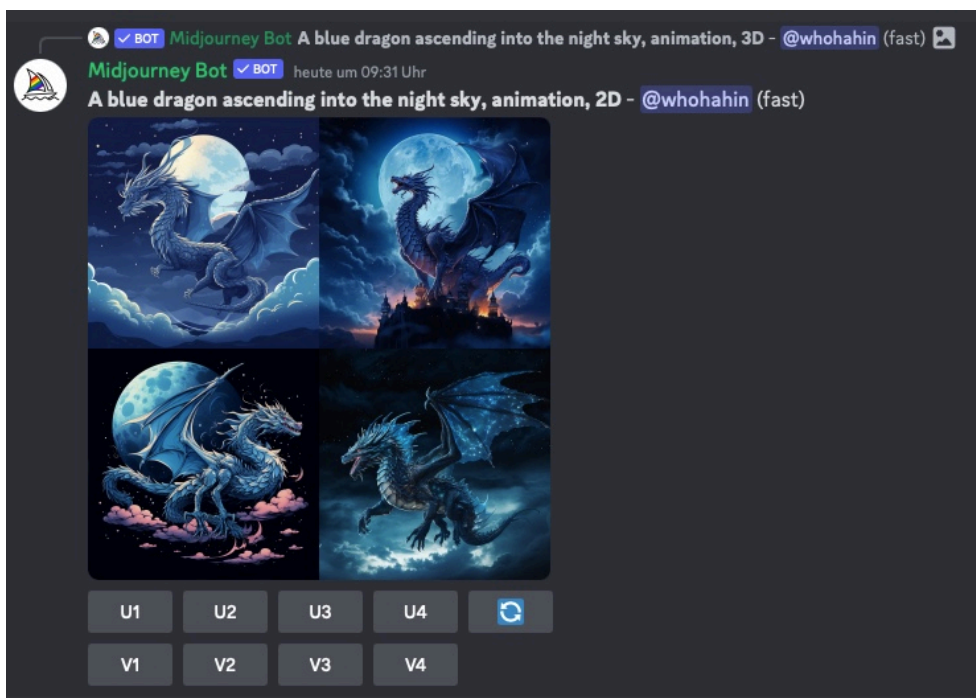


Bilder verwenden/eigene Bilder erstellen

Midjourney selbst empfiehlt dem Einsteiger, seine Bilder in den Newbie-Kanälen

zu erzeugen. Die findet ihr in der Seitenleiste unter **Newcomer Rooms**. Dort findet Ihr auch schon eine Vielzahl von anderen Anwendern erzeugten Bildern, die ihr herunterladen könnt. Um nun ein eigenes Bild zu erzeugen, geht so vor:

- Klickt in das Eingabefeld für eine neue Nachricht unten am Bildschirmrand.
- Gebt als Befehl **/imagine** und dann eine (englische) Beschreibung des Bildes, so wie ihr es gestaltet haben wollt, ein. Beispielsweise **/imagine a blue dragon ascending into the night sky**.
- Midjourney generiert euch nun vier Versionen dieses Bildes, so wie der Dienst die Eingabe interpretiert.
- Wenn ihr auf die Schaltflächen mit **V** klickt, dann erzeugt Midjourney Variationen davon.
- Klickt ihr auf die Schaltflächen mit **U**, dann erzeugt der Dienst das Bild in höherer Auflösung. Die Bilder könnt ihr dann herunterladen.
- Die Anpassungen funktionieren auch mit den Bildern anderer Benutzer.



Je nach Auslastung des Dienstes steht die kostenlose Funktion nicht immer zur Verfügung. Wenn ihr Midjourney häufiger nutzen wollt, dann könnt ihr ein kostenpflichtiges Abo abschließen, das ab USD 8,- im Monat [zu bekommen ist](#).

Probleme mit Apple CarPlay lösen



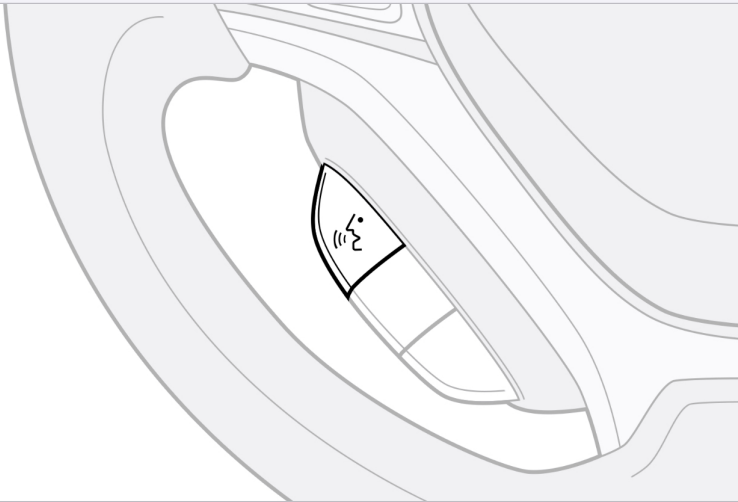
Fast alle Autohersteller haben eine eigene Multimediaoberfläche für Musikwiedergabe und Navigation. Das kann man mögen, als iPhone-Besitzer aber gibt es mit CarPlay eine Alternative im Apple-Kosmos. Die hat die eine oder andere Macke, wir aber Lösungen dazu.

Kabellos oder kabelgebunden?

CarPlay ist im Standard erst einmal eine kabelgebundene Verbindung: Da iPhone wird mit einem USB-Kabel mit dem Fahrzeug (mit einer CarPlay-fähigen USB-Buchse) verbunden und dann konfiguriert. Mehr und mehr Fahrzeuge bieten aber eine kabellose Verbindung über eine Kombination von WLAN und Bluetooth an, das so genannte [Wireless Carplay](#).

< Allgemein

CarPlay



Wenn dein Auto drahtloses CarPlay unterstützt, halte die Taste für die Sprachsteuerung am Lenkrad gedrückt, um die CarPlay-Konfiguration zu starten.

Wenn die kabellose Verbindung zwischen dem Fahrzeug und dem [iPhone](#) abbricht, die Qualität von Gesprächen oder der Musikwiedergabe unterbrochen oder verzerrt ist, dann liegt das oft an Störsendern im Auto oder Steuergeräten, die überlastet sind. Das könnt Ihr meist nicht direkt beeinflussen, wohl aber Abhilfe schaffen:

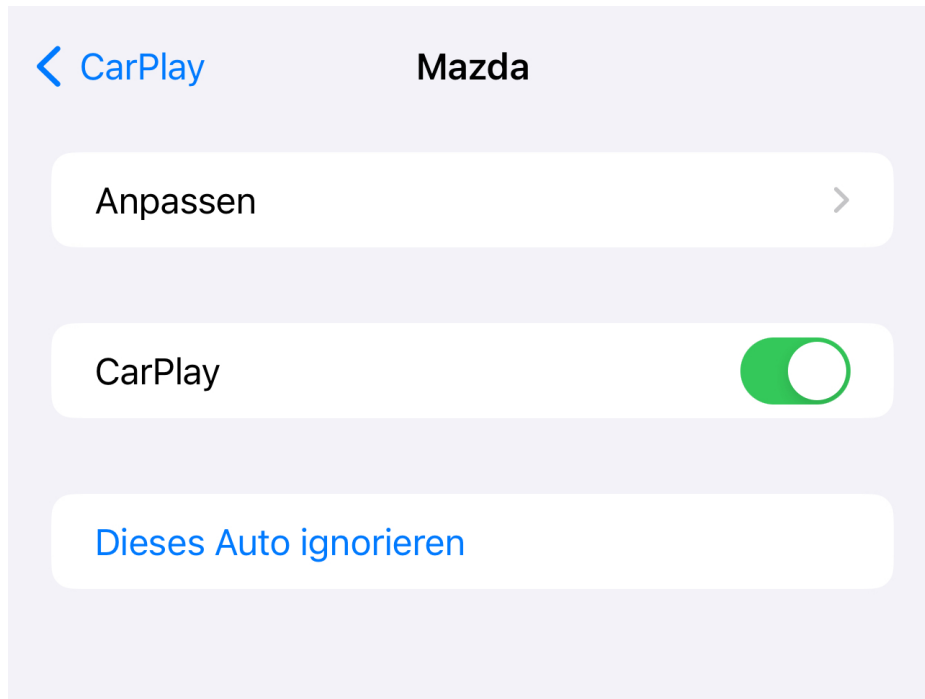
- Schaltet die Zündung des Fahrzeugs aus und das iPhone einmal kurz in den Flugmodus.
- Verbindet das Kabel zwischen USB-Schnittstelle des Fahrzeugs und dem iPhone.
- CarPlay baut die Verbindung über das Kabel auf, was die Verbindungsprobleme meist direkt behebt.
- Ihr könnt bei den neueren CarPlay-Versionen entscheiden, ob die Verbindung beim nächsten Mal wieder kabellos versucht werden soll oder nicht.

CarPlay funktioniert gar nicht

Was aber, wenn CarPlay gar nicht funktioniert? Das kann mehrere Gründe haben:

- Unterstützt das Fahrzeug überhaupt CarPlay? Auch wenn CarPlay über den in nahezu allen Fahrzeugen vorhandenen USB-Anschluss betrieben wird, muss CarPlay explizit im Fahrzeug vorhanden sein!

- Kontrolliert auf dem iPhone unter **Einstellungen > Allgemein > CarPlay**, ob das Fahrzeug in der Liste der verfügbaren CarPlay-Partner auftaucht.
- Ist das nicht der Fall, dann versucht die Verbindung erneut herzustellen.
- Wenn das Fahrzeug in der Liste auftaucht, dann tippt es an und kontrolliert, ob CarPlay aktiviert ist.



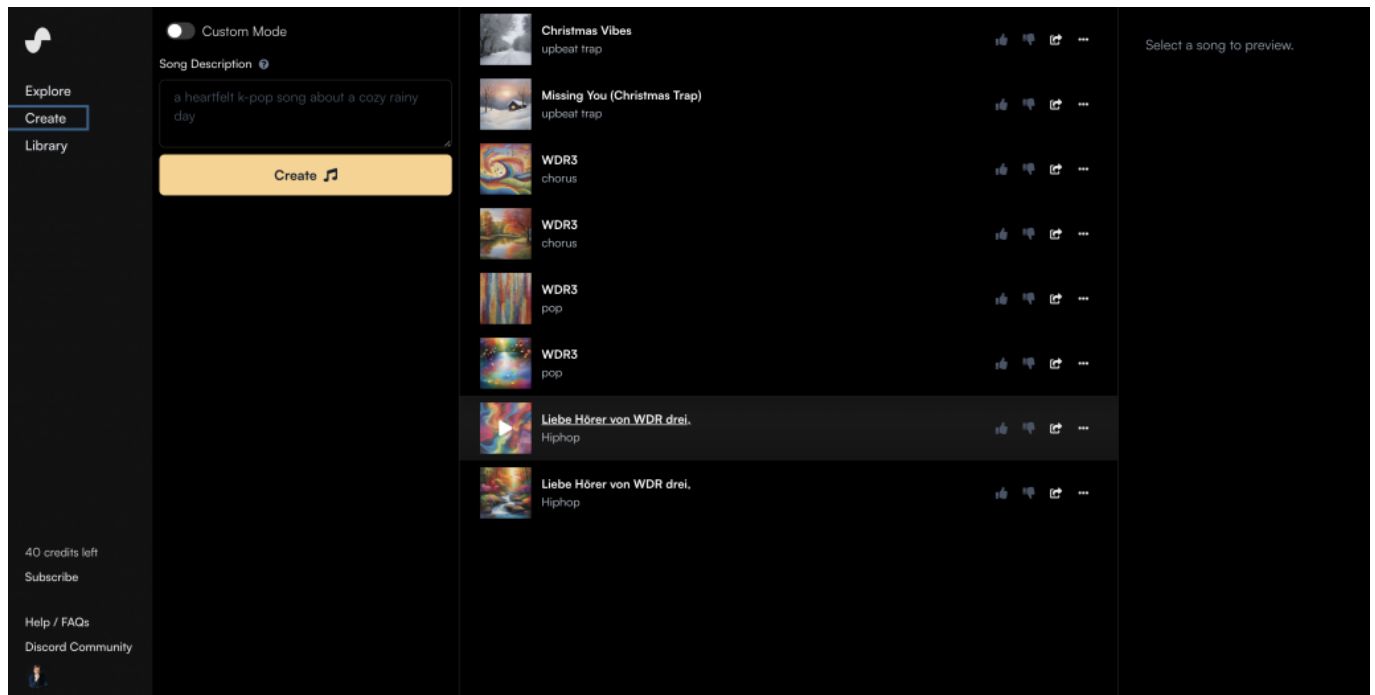
Suno App: KI kann jetzt auch Musik und Gesang erzeugen



Generative KI kann nicht mehr nur länger Texte, Audios und Bilder erzeugen, sondern nun auch Musik und sogar Gesang. Die Suno App macht vor, wie sich das anhört.

Was Künstliche Intelligenz (KI) heute nicht alles schon kann: Texte schreiben, Excel-Tabellen sortieren, Grafiken und sogar Bilder und Fotos erzeugen, Stimmen imitieren... Und jetzt kommt der nächste Schritt: KI kann auch Musik und sogar Gesang erzeugen.

Und damit ist nicht der Synthesizer gemeint, den gibt es seit den 60er Jahren und ersetzt lediglich Instrumente, nicht das Komponieren und Abmischen von Musik. KI von heute erzeugt auf Knopfdruck Musik und passenden Gesang. Und das kann jeder herstellen.



Die Suno App erzeugt vollständig automatisch Musik und Gesang

Generative KI erzeugt Musik und Gesang

KI kann jetzt auch Musik machen. Und zwar so, wie es bei KI immer ist: Man schreibt auf, was man haben möchte – und die KI erzeugt die Musik. Man braucht nicht die geringste Ahnung davon zu haben, man muss keine Noten lesen können oder anderweitig begabt sein.

Mit **Suno AI** ist jetzt eine solche generative KI am Start, die das für jedermann möglich macht. Ein Beispiel: Ich sage der KI, ich möchte, dass ein Chor meinen Text singt – klassisch zum Beispiel, Und dieser Chor soll auch noch einen Text singen, den ich selbst geschrieben habe, als Begrüßung für, die gerne Klassik hören. Das klingt dann zum Beispiel so:

[audio mp3="https://www.schieb.de/wp-content/uploads/2024/01/wdr3-chorus.mp3"][/audio]

Erstaunlich, oder? Nicht perfekt, gar keine Frage. Aber das waren die ersten Texte von ChatGPT vor einem Jahr auch nicht. Doch KIs entwickeln sich rasant.

KI kann auch Pop und Hiphop

Die KI erzeugt die Musik so, wie das verlange. Das Ganze ginge auch in Pop oder

Hiphop.

Das ist sogar noch einfacher, weil die App darauf spezialisiert ist. Einfach denselben Text nehmen oder etwas anpassen, damit es cooler klingt – und „Hiphop“ als Musikrichtung wählen. Die KI passt auf Wunsch sogar auch den eingegebenen Text so an, dass es passt. Das Ergebnis klingt dann zum Beispiel so:

[audio mp3="https://www.schieb.de/wp-content/uploads/2024/01/liebe-hoerer-von-wdr-drei.mp3"][/audio]

Ein paar Songs und Titel kann man kostenlos erzeugen. Wenn man mehr will, wird das Ganze kostenpflichtig. Doch es zeigt, in welche Richtung die Reise geht. KI kann heute nicht nur einfache Texte oder überzeugende Bilder erstellen, sondern auch Musik und sogar Gesang.

Stichwort Kreativität

Nicht unbedingt. Das hat man anfangs von Synthesizer-Musik oder anderen Techniken auch gesagt. Komponieren muss man trotzdem. Und seien wir ehrlich: Vieles, was in den Charts ist und rauf und runter läuft, ist weit davon entfernt, wirklich kreativ oder originell zu sein.

Wir bekommen mit den neuen KIs ganz sicher eine neue Form von Musik – und nur die wirklich Kreativen können damit auch etwas Neues und womöglich Einzigartiges schaffen. Ganz sicher noch nicht mit den KIs in Kinderschuhen wie jetzt. Aber das wird sich schnell entwickeln und dann womöglich ein ernsthaftes Werkzeug im ganz normalen Musik-Business sein, so wie heute im Computer erzeugte Instrumente und Rhythmen.



Urheberrecht und KI

Aber wie sieht es mit dem Urheberrecht aus? Die KIs erzeugen nichts wirklich Neues, sondern werden mit Musik trainiert und wiederholen das nur...

Das Thema Urheberrecht spielt bei allen generativen KI-Modellen eine große Rolle, keine Frage. Genau darüber muss diskutiert werden: Das Urheberrecht muss im 21. Jahrhundert ankommen. Es muss für alle klar sein, wo die Grenzen sind – und welche Lizenzen möglicherweise zu zahlen sind, etwa an die GEMA.

Aber wir dürfen auch nicht vergessen, dass Kultur sich immer weiter entwickelt und auch Menschen sich inspirieren lassen und etwas weiter entwickeln, ob Texte, Bilder, Kunst oder Musik. In einem gewissen Rahmen ist das auch bei KI in Ordnung. Doch Kopien 1:1 auf Knopfdruck zu erzeugen, das geht nicht in Ordnung. Deshalb kann man in der Suno App auch keinen Künstler angeben und imitieren, sondern immer nur Musikrichtungen.

37C3: Gehackter Tesla, Ransomware und Sicherheitslecks



Der Hackerkongress 37C3 ist zu Ende gegangen. Herausragend waren diesmal ein Tesla-Hack - und ein Vortrag von Linus Neumann, der gezeigt hat, wie professionell Ransomware-Banden heute organisiert sind.

Das neue Jahr ist gestartet – und das alte ist noch mit einem Hackerkongress zu Ende gegangen. Traditionell in den Tagen nach Weihnachten findet der „Chaos Communication Congress“ statt: Das größte Hackertreffen in Europa.

Das darf man sich aber nicht so vorstellen, dass sich Hacker gegenseitig die neuesten Tricks zustecken, sondern es handelt sich um einen ernsthaften Kongress, auf dem drängende aktuelle Sicherheitsthemen diskutiert und vorgestellt werden. Unter anderem wurde gezeigt, dass Tesla-Autos völlig unzureichend vor Hackangriffen geschützt sind.



Das Geheimnis hinter dem Namen 37C3

Der jährlich stattfindende Kongress hat ja immer einen kryptischen Namen. Der gerade zu Ende gegangene Kongress wurde 37C3 getauft. Was bedeutet das?

Der Name des Chaos Communication Congress (CCC) ändert sich jedes Jahr. Das „C3“ ist noch einfach. Das steht für „drei Mal C“, also „CCC“. Zum einen, weil der Kongress „Chaos Computer Kongress“ getauft wurde, zum anderen aber auch, weil der angesehene „Chaos Computer Club“ den Kongress veranstaltet.

Hier treffen sich wirklich alle, die sich mit IT-Sicherheit beschäftigen und tauschen sich aus. Der Termin ist zwar nicht sonderlich familienfreundlich – zwischen den Jahren –, aber das ist eben Tradition. Die Zahl vor dem „C3“ ändert sich jedes Jahr und gibt an, um den wievielten Kongress es sich handelt.

Gerade also der 37. – Ende dieses Jahres wird es der 38. sein, dann werden wir also über den 38C3 sprechen. Eine einfache und effektive Methode also, um die jährliche Veranstaltung zu kennzeichnen und gleichzeitig eine Kontinuität und Tradition zu betonen.



37C3: Der jährliche Hackerkongress bringt immer relevante Sicherheitslücken ans Tageslicht

Drei Doktoranden knacken Teslas Autopiloten

Auf dem Kongress wurde nicht nur berichtet, sondern auch konkret gezeigt, wie sich ein Tesla hacken lässt.

Drei Doktoranden der TU Berlin haben das zentrale Teil eines jeden Teslas geknackt, den Autopiloten. Das haben sie nicht etwa hollywoodreif aus der Ferne gemacht, sondern mit den eigenen Händen: Sie mussten schon Zugriff auf das Auto haben.

Sie haben sich aber durch einige Tricks Zugang zur eigentlich geschützten Platine verschafft, auf der der Autopilot des Fahrzeugs steckt. Sie konnten die Software herunterladen, verstehen, wie der Autopilot funktioniert und sogar ein gelöscht Video aus dem Fahrzeug herunterladen.

Alles, was es dazu brauchte, war das Know-how der drei – und allgemein zugängliches Werkzeug für rund 600 EUR. Dass jemand den Autopiloten so einfach knackt, ist schon erstaunlich. Experten schätzen den Wert des Know-hows des Autopiloten auf mehrere Mio. EUR.

Keine unmittelbare Gefahr

Eine direkte und unmittelbare Gefahr ergibt sich daraus allerdings nicht.

Es bedeutet nicht, dass Fremde das Auto einfach fernsteuern können. Aber es lassen sich Daten auslesen, etwa zum Fahrverhalten. Oder sogar eigentlich gelöschte Videos – Tesla-Autos nehmen mit ihren mehreren Kameras eine Menge auf – werden nicht wirklich gelöscht.

Auch zeigt sich, dass die Fahrzeuge Daten in die Firmenzentrale funken. Tesla selbst äußert sich dazu mal wieder nicht. Tesla äußert sich nie zu Datenschutzverstößen oder Sicherheitsrisiken. Das ist das eigentliche Problem.



Linus Neumann hat gezeigt, wie professionell Cyberkriminelle heute vorgehen

Ransomware und Lösegeldzahlungen

Apropos Sicherheit: Das ist immer ein wichtiges Thema auf solchen IT-Kongressen - auch in diesem Jahr.

Linus Neumann, Sprecher des CCC, hat in einem Vortrag Beispiele dafür gebracht, wie nach einem erfolgreichen Hackangriff per Ransomware mit den Cyberbetrügern verhandelt wird. Es ist tatsächlich so, dass Ransomware ein straff organisiertes Geschäft ist.

Zuerst wird angegriffen, dann hat man es mit einer Art „Support“ zu tun, dann wird ein Preis ausgehandelt – und womöglich werden alle verschlüsselten Daten wieder entschlüsselt. Wichtig ist, richtig mit solchen Angriffen umzugehen. Noch wichtiger aber ist: Updates einspielen, Mitarbeiter schulen und vor allem: Backups machen.

Backups, also Sicherheitskopien, die nicht in der normalen IT-Infrastruktur direkt zugänglich sind, damit sie nicht auch bei solchen Angriffen verschlüsselt werden. Wir müssen uns alle besser auf solche Angriffe vorbereiten: Schützen, Schulen und Sicherheitskopien anfertigen – rechtzeitig.

Was ist eigentlich der Chaos Communication Congress (CCC)



Jedes Jahr in den Tagen nach Weihnachten findet der "Chaos Communication Congress" (CCC) statt, eine Veranstaltung des Chaos Computer Club. Was genau findet da statt?

Der Chaos Communication Congress (CCC) ist ein jährliches, mehrtägiges Treffen der internationalen Hackerszene, das vom Chaos Computer Club (CCC) organisiert wird. Der Kongress ist die größte europäische Zusammenkunft der Hackerszene und eine der traditionsreichsten deutschen IT-Sicherheits- und Technikkompetenzkonferenzen.

Der Kongress bietet eine Vielzahl von Vorträgen und Workshops zu technischen und gesellschaftlichen Themen. Die Themen reichen von Überwachung, Datenschutz, Informationsfreiheit, Hacktivismus, Datensicherheit und vielen anderen interessanten Aspekten rund um Technologie und Hacking.

Ein großer Teil der Referenten kommt aus der Szene selbst, und die organisatorische Arbeit vor Ort wird von freiwilligen Helfern geleistet, die im CCC-Jargon als **Engel** bezeichnet werden.



Der CCC ist das weltweit größte Hackertreffen - immer in der letzten Woche des Jahres

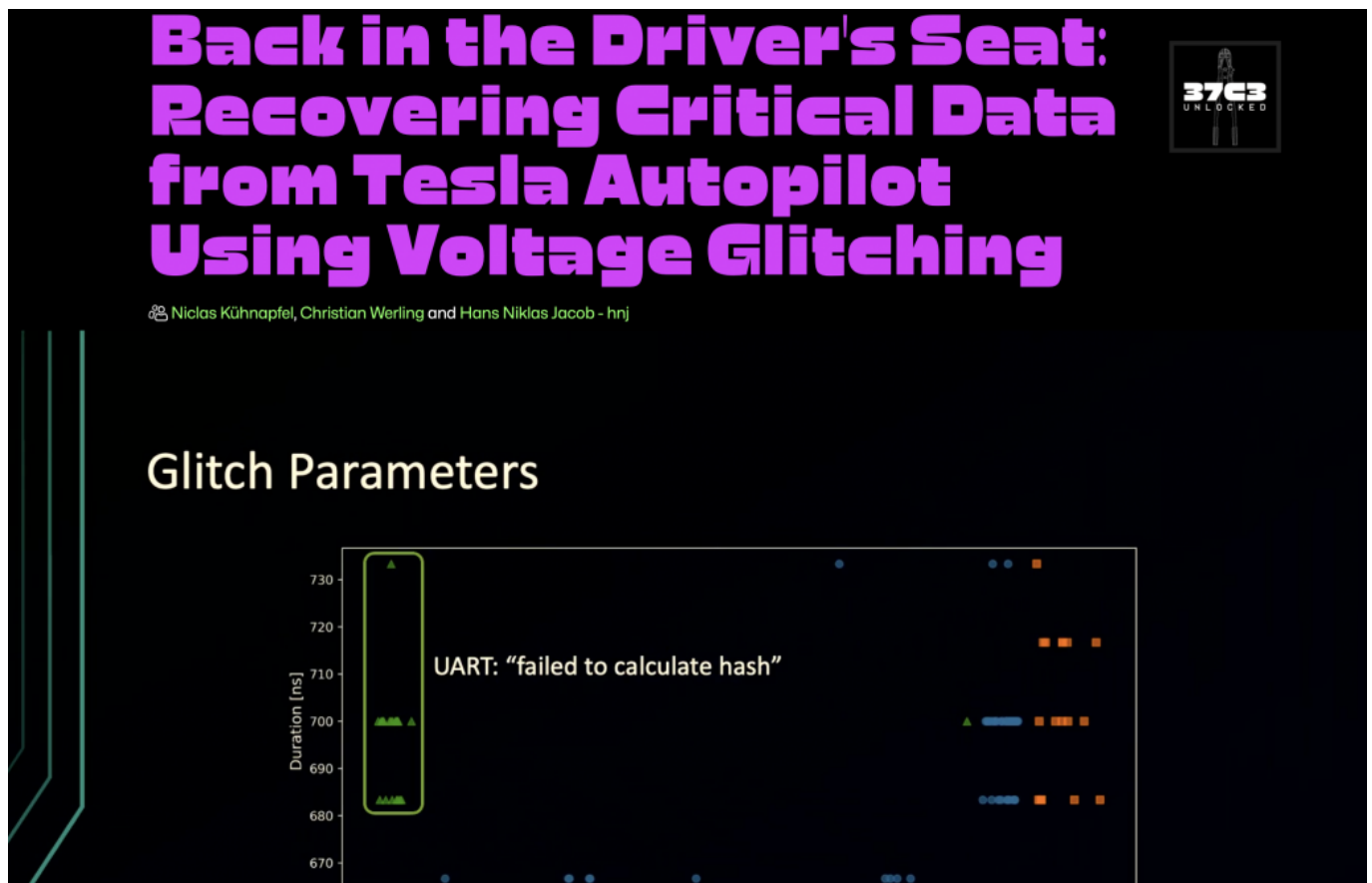
Warum eigentlich 37C3 als Name?

Der Name des Chaos Communication Congress (CCC) ändert sich jedes Jahr, um die jeweilige Iteration des Kongresses zu kennzeichnen. Die Nummer im Namen repräsentiert die Anzahl der Kongresse, die bis zu diesem Zeitpunkt stattgefunden haben. Zum Beispiel wurde der 37. Kongress als "37C3" bezeichnet, wobei "37" die Anzahl der Kongresse und "C3" eine Abkürzung für "Chaos Communication Congress" ist.

Diese Namensgebung ist eine einfache und effektive Methode, um die jährliche Veranstaltung zu kennzeichnen und gleichzeitig eine Kontinuität und Tradition zu betonen. Es ermöglicht den Teilnehmern und der breiteren Öffentlichkeit, sich auf einen spezifischen Kongress zu beziehen und diesen in der Geschichte des CCC zu verorten.

Es ist wichtig zu beachten, dass trotz der jährlichen Namensänderung der grundlegende Charakter und die Ziele des Kongresses konstant bleiben: ein Treffen der internationalen Hackerszene, das technische und gesellschaftliche Themen diskutiert und ein offenes und inklusives Umfeld für Wissensaustausch

und Vernetzung bietet.



Dieses Jahr wurden Sicherheitslecks im autonomen Fahrsystem von Tesla dokumentiert

Die Tradition des CCC

Die Tradition des Kongresses ist es, ein offenes und inklusives Umfeld zu schaffen, in dem Wissen ausgetauscht, Kontakte geknüpft und gefeiert werden kann. Es ist auch ein Ort, an dem komplexe Dinge durchdrungen werden können, nicht nur Technologie, sondern auch Gesellschaft, Medien und Politik.

Der Kongress ist auch für seine Hackcenter bekannt, ein großes Areal, in dem die verschiedenen regionalen Gruppierungen des Clubs mit ihrer Technik auf dem Kongress präsent sind. Es ist kein LAN-Party, sondern ein "Hands-On"-Labor zum gemeinsamen Erforschen und Testen von Netzwerktechnologie.

Es ist wichtig zu beachten, dass der Begriff "Hacker" im Kontext des CCC positiv besetzt ist und Menschen bezeichnet, die Technik verstehen wollen, indem sie sie auseinandernehmen.