Stalkerware
im Jahr 2022

Coalition Against Stalkerware

kaspersky

Inhalt

Zentrale Erkenntnisse aus dem Jahr 2022

Für den jährlichen Stalkerware-Report analysiert Kaspersky, wie viele Menschen weltweit von digitalem Stalking betroffen sind. Die hierfür verwendete Software, sogenannte Stalkerware, ist kommerziell erhältlich. Sie wird heimlich auf Smartphones installiert und ermöglicht es dem Täter, das Privatleben einer Person ohne deren Wissen auszuspionieren.

Stalkerware kann von jedem, der über eine Internetverbindung verfügt und physischen Zugriff auf ein Smartphone hat, heruntergeladen und relativ einfach installiert werden. Der Täter verletzt damit die Privatsphäre der Betroffenen; denn sie können deren persönliche Daten mithilfe der Software überwachen. Je nach Art der Software ist es in der Regel möglich, den Standort des Geräts, Textnachrichten, Chats in sozialen Medien, Fotos, den Browserverlauf und vieles andere mehr zu überwachen. Die meisten Betroffenen bemerken nicht, dass jeder ihrer Schritte überwacht wird, da die Software völlig unbemerkt im Hintergrund läuft.

In den meisten Ländern der Welt ist die Verwendung von Stalker-Software grundsätzlich nicht verboten; bislang ist es nur illegal und strafbar, diese auf dem Smartphone einer anderen Person ohne deren Einwilligung zu installieren. Allerdings wird lediglich der Täter zur Verantwortung gezogen, nicht die Entwickler des Programms selbst.

Neben weiteren ähnlichen Technologien zählt Stalkerware zum Technologie-gestützten Missbrauch und findet häufig Anwendung in Beziehungen, die auch in anderer Hinsicht von Missbrauch geprägt sind. Da sich das Problem nicht nur auf einen Aspekt reduzieren lässt, arbeitet Kaspersky mit Experten und Organisationen auf dem Gebiet der häuslichen Gewalt von Betroffenenhilfsdiensten und Täterprogrammen bis hin zu staatlichen Einrichtungen und Forschungsstätten zusammen, um Wissen auszutauschen sowie professionelle Helfer und Betroffene gleichermaßen zu unterstützen.

Zentrale Daten für 2022

- **Laut Kaspersky-Daten waren im Jahr 2022 weltweit 29.312 Einzelpersonen von Stalkerware betroffen.** Diese Zahl ist mit der Gesamtzahl der Betroffenen im Jahr 2021 vergleichbar. Unter Berücksichtigung der Weiterentwicklung digitaler Stalker-Programme in den vergangenen Jahren scheinen sich die Zahlen auf diesem Niveau einzupendeln. Generell muss aber darauf hingewiesen werden, dass sich die Daten nur auf betroffene Kaspersky-Nutzer beziehen, die Dunkelziffer der weltweit Betroffenen dürfte sehr viel höher liegen. Denn manche Betroffene nutzen eventuell eine andere Cybersicherheitslösung auf ihren Geräten, andere vielleicht auch gar keine.
- **Darüber hinaus zeigen die Daten eine stetige Verbreitung von Stalkerware über das Jahr 2022 hinweg.** Durchschnittlich waren jeden Monat 3.333 neue Nutzer von Stalkerware betroffen. Diese stabile Erkennungsrate deutet darauf hin, dass sich digitales Stalking zu einem anhaltenden Problem entwickelt hat, dem die Gesellschaft mehr Aufmerksamkeit widmen sollte. Die Mitglieder der Koalition gegen Stalkerware gehen davon aus, dass jedes Jahr weltweit fast eine Million Menschen von Stalkerware betroffen sind.
- Nach Angaben des Kaspersky Security Network **kommt Stalkerware am häufigsten in Russland, Brasilien und Indien zum Einsatz,** ist aber nach wie vor ein globales Phänomen. Die meisten Betroffenen sind in den folgenden Ländern zu finden:
  - Deutschland, Italien und Frankreich (Europa);
  - Iran, Türkei, Ägypten und Saudi-Arabien (Naher Osten und Afrika);
  - Indien, Indonesien und Australien (asiatisch-pazifischer Raum)
  - Brasilien, Mexiko und Ecuador (Lateinamerika);
  - Vereinigte Staaten (Nordamerika);
  - Russische Föderation, Kasachstan und Belarus (Osteuropa (ohne EU-Staaten), Russland und Zentralasien).
- Die weltweit am häufigsten verwendete Stalkerware-App ist Reptilicus mit 4.065 betroffenen Nutzern.

Entwicklungen, die Kaspersky im Jahr 2022 beobachtet hat

Im Jahr 2022 waren insgesamt 29.312 Einzelnutzer von Stalkerware betroffen

Erkennung in Zahlen: Betroffene Nutzer weltweit

In diesem Abschnitt werden die von Kaspersky für das Jahr 2022 ermittelten globalen und regionalen statistischen Erhebungen mit denen der Vorjahre verglichen. Im Jahr 2022 waren insgesamt 29.312 individuelle Nutzer von Stalkerware betroffen. In Abbildung 1 unten wird aufgezeigt, wie sich diese Zahl seit dem Jahr 2018 verändert hat.

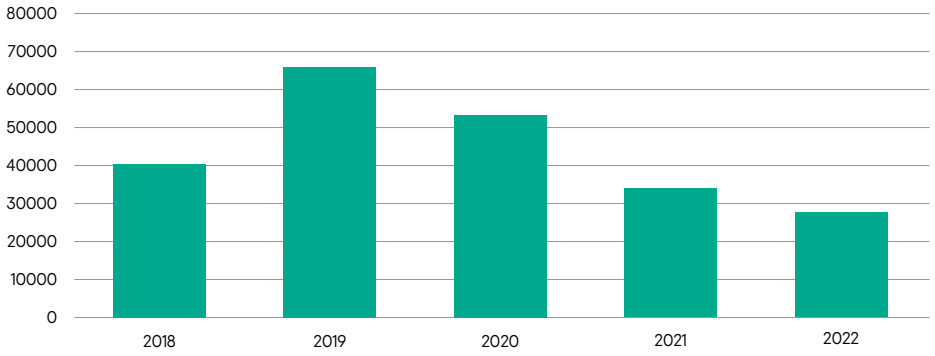


Abbildung 1: Jährliche Entwicklung der Anzahl der Betroffenen seit 2018

In Abbildung 2 unten ist die monatliche Entwicklung der Zahl der betroffenen Einzelbenutzer für die Jahre 2021 und 2022 visualisiert. In diesem Zeitraum gab es kaum Veränderungen, was darauf hindeutet, dass sich die Verbreitungsrate von Stalkerware auf diesem Niveau eingependelt hat. Durchschnittlich kamen jeden Monat 3.333 neue betroffene Nutzer hinzu.

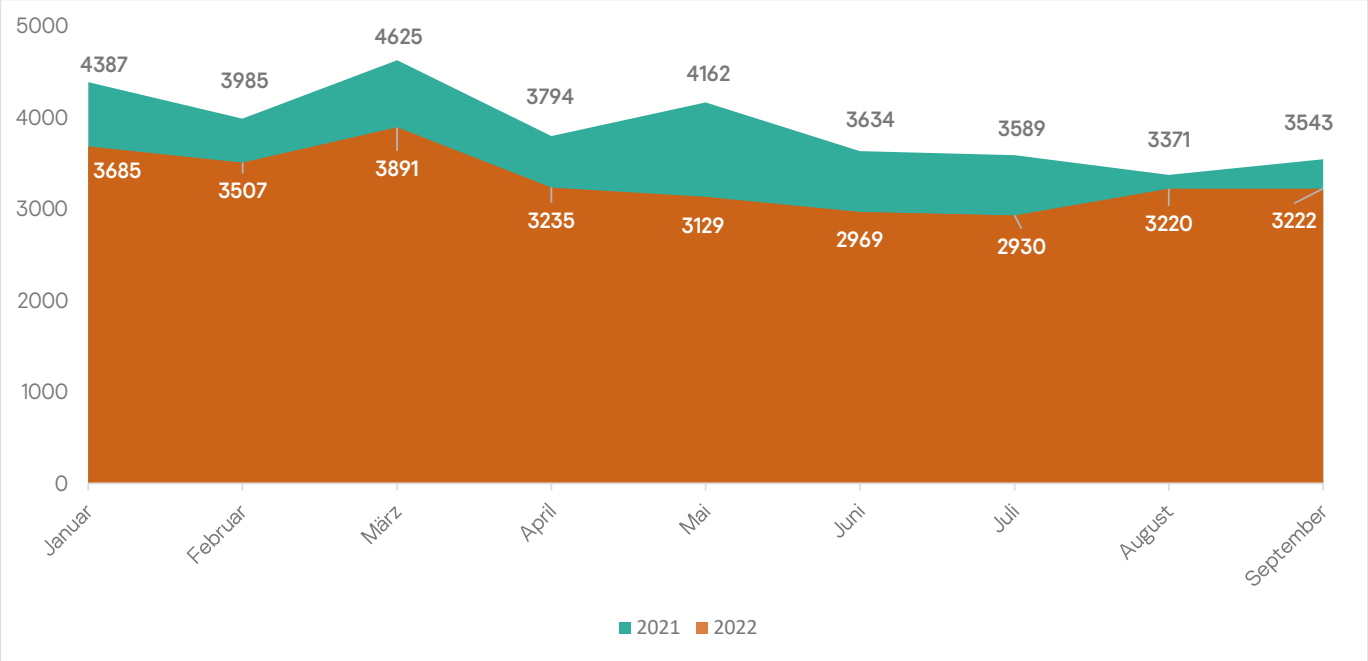
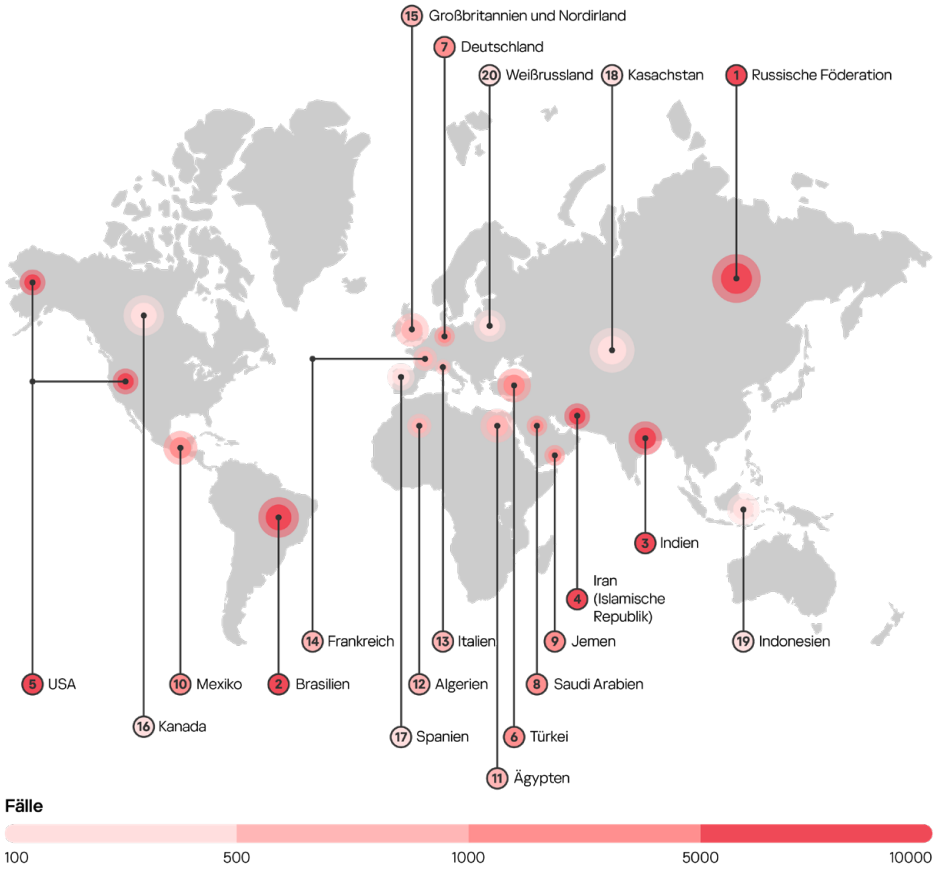


Abbildung 2: Anzahl der betroffenen Nutzer pro Monat für die Jahre 2021 bis 2022

Globale und regionale Verteilung der Erkennungen: Am stärksten betroffene Regionen

Stalkerware ist nach wie vor ein weltweites Problem. Im Jahr 2022 identifizierte Kaspersky betroffene Nutzer in insgesamt 176 Ländern.



Karte 1: Die am stärksten von Stalkerware betroffenen Länder im Jahr 2022

Methodik

Die Statistiken des Kaspersky Security Network bilden die Datengrundlage für diesen Bericht. In das Kaspersky Security Network fließen sicherheitsrelevante Datenströme von Millionen freiwilliger Teilnehmer weltweit ein,die Daten werden anonymisiert verarbeitet. Zur Erstellung der Statistiken wurde die Kaspersky-Produktpalette mobiler Sicherheitslösungen für Verbraucher entsprechend der Erkennungskriterien für Stalkerware der Koalition gegen Stalkerware überprüft. Das bedeutet, dass die betroffenen Nutzer ausschließlich das Ziel von Stalkerware waren. Andere Arten von Überwachungs- oder Spyware-Apps, die nicht unter die Definition der Koalition gegen Stalkerware fallen, sind nicht in die Statistik dieses Berichts eingeflossen.

Die Statistiken spiegeln die Anzahl der von Stalkerware betroffenen Handynutzer wider, nicht die Gesamtzahl der Erkennungen. Die Anzahl der Erkennungen kann höher liegen, da Stalkerware möglicherweise mehrmals auf demselben Gerät desselben Nutzers erkannt wurde, falls sich dieser nach Erhalt der entsprechenden Benachrichtigung dennoch dazu entschieden hat, die App nicht zu entfernen.

Schlussendlich gehen nur solche Handynutzer in die Statistik ein, die IT-Sicherheitslösungen von Kaspersky nutzen. Manche Nutzer könnten eine andere Cybersicherheitslösung auf ihren Geräten nutzen, andere wiederum gar keine.

Nutzer in Russland (8.281), Brasilien (4.969) und Indien (1.807) waren im Jahr 2022 am häufigsten von Stalkerware betroffen. Wie die Zahlen von Kaspersky zeigen, führen diese drei Länder die Statistik seit dem Jahr 2019 an. Im Vergleich zum Vorjahr ist die Anzahl der betroffenen Nutzer in den USA gesunken; mit 1.295 Betroffenen liegt das Land nun auf Platz fünf. Dagegen ist im Iran ein Anstieg zu verzeichnen, mit 1.754 Betroffenen ist das Land auf den vierten Platz vorgerückt.

Verglichen mit dem Jahr 2021 ist der Iran der einzige Neueinsteiger in die Liste der fünf am häufigsten betroffenen Länder. Die anderen vier – Russland, Brasilien, Indien und die USA – gehörten von jeher zu den traurigen Spitzenreitern im Bereich Stalkerware. Des Weiteren gehören die Türkei, Deutschland und Mexiko nach wie vor zu den am häufigsten betroffenen Ländern. Neu in den Top 10 der am stärksten betroffenen Länder sind im Jahr 2022 Saudi-Arabien und der Jemen.

	Land	Anzahl betroffener Nutzer
1	Russische Föderation	8.281
2	Brasilien	4.969
3	Indien	1.807
4	Iran	1.754
5	USA	1.295
6	Türkei	755
7	Deutschland	736
8	Saudi-Arabien	612
9	Jemen	527
10	Mexiko	474

Tabelle 1: Top 10 der am stärksten von Stalkerware betroffenen Länder weltweit in 2022

In Europa waren insgesamt 3.158 Einzelnutzer im Jahr 2022 betroffen. Die drei am stärksten betroffenen Länder in Europa waren Deutschland (737), Italien (405) und Frankreich (365). Im Vergleich zum Vorjahr 2021 hat sich die Liste der am häufigsten betroffenen Länder Europas bis Platz sieben (die Niederlande) nicht verändert. Neuzugänge in der Liste sind die Schweiz, Österreich und Griechenland.

	Land	Anzahl betroffener Nutzer
1	Deutschland	736
2	Italien	405
3	Frankreich	365
4	Vereinigtes Königreich	313
5	Spanien	296
6	Polen	220
7	Niederlande	154
8	Schweiz	123
9	Österreich	71
10	Griechenland	70

Tabelle 2: Top 10 der am stärksten von Stalkerware betroffenen Länder in Europa (2022)

In Osteuropa (ohne die Länder der Europäischen Union), Russland sowie Zentralasien waren im Jahr 2022 9.406 Nutzer betroffen. Am häufigsten traf es Nutzer in Russland, Kasachstan und Belarus.

	Land	Anzahl betroffener Nutzer
1	Russische Föderation	8.281
2	Kasachstan	296
3	Belarus	267
4	Ukraine	258
5	Aserbaidschan	130
6	Usbekistan	76
7	Moldawien	34
8	Tadschikistan	32
9	Kirgisistan	31
10	Armenien	27

Tabelle 3: Top 10 der am stärksten von Stalkerware betroffenen Länder in Osteuropa (ohne EU-Länder), Russland sowie Zentralasien im Jahr 2022

Im Nahen Osten und in Afrika betrug die Gesamtzahl der betroffenen Nutzer 6.330, die Anzahl liegt etwas höher als im Jahr 2021. Während der Iran mit 1.754 Betroffenen die Liste im Jahr 2022 anführt, belegt die Türkei mit 755 betroffenen Nutzern in dieser Region nun Platz zwei, gefolgt von Saudi-Arabien mit 612 Betroffenen.

	Land	Anzahl betroffener Nutzer
1	Iran	1.754
2	Türkei	755
3	Saudi-Arabien	612
4	Jemen	527
5	Ägypten	469
6	Algerien	407
7	Marokko	168
8	Vereinigte Arabische Emirate	155
9	Südafrika	145
10	Kenia	123

Tabelle 4: Top 10 der am stärksten von Stalkerware betroffenen Länder im Nahen Osten und Afrika (2022)

Im asiatisch-pazifischen Raum waren 3.187 Nutzer betroffen. Noch immer liegt Indien mit 1.807 Betroffenen weit vor allen anderen Ländern dieser Region; gefolgt von Indonesien mit 269 betroffenen Nutzern und Australien mit 190 Betroffenen.

	Land	Anzahl betroffener Nutzer
1	Indien	1.807
2	Indonesien	269
3	Australien	190
4	Philippinen	134
5	Malaysia	129
6	Vietnam	109
7	Bangladesch	105
8	Japan	95
9	Thailand	52
10	Pakistan	48

Tabelle 5: Top 10 der am stärksten von Stalkerware betroffenen Länder im asiatisch-pazifischen Raum (2022)

In der Region Lateinamerika und Karibik stammte ein Drittel (32 Prozent; 4.969 Nutzer) der Betroffenen aus Brasilien. Weitere Betroffene finden sich in Mexiko, Ecuador und Kolumbien. Insgesamt waren in dieser Region 6.170 Personen betroffen.

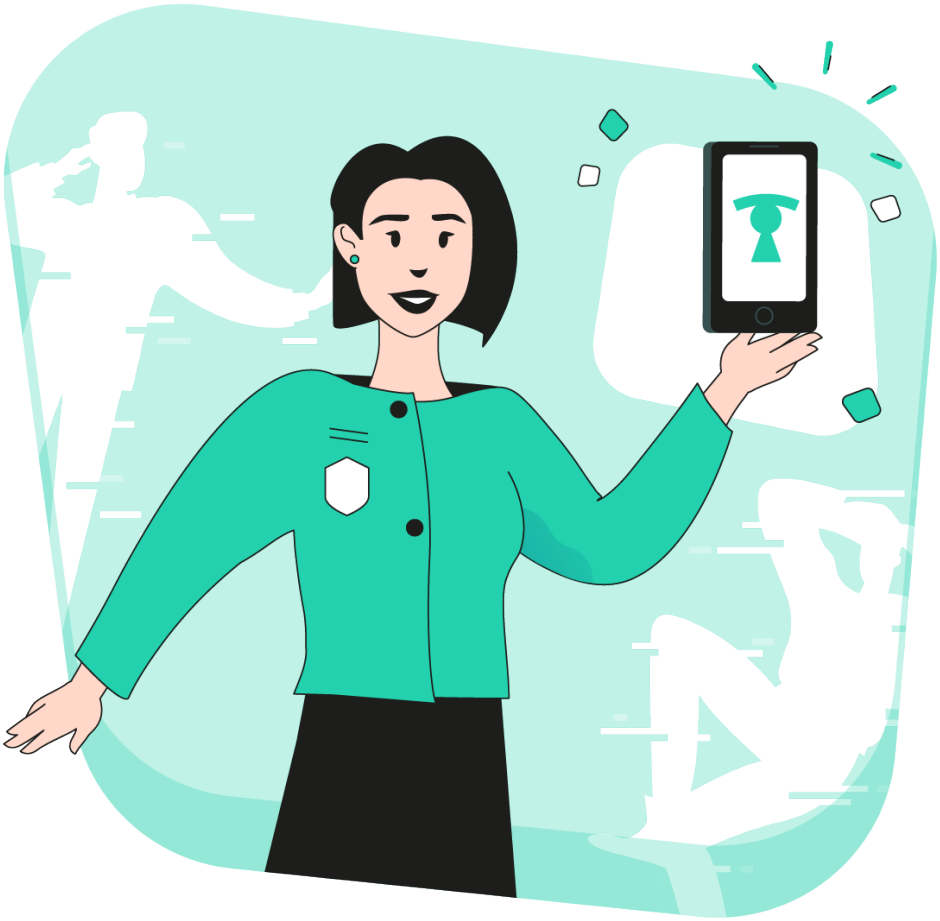
	Land	Anzahl betroffener Nutzer
1	Brasilien	4.969
2	Mexiko	474
3	Ecuador	146
4	Kolumbien	120
5	Peru	111
6	Argentinien	85
7	Chile	49
8	Bolivien	32
9	Venezuela	30
10	Dominikanische Republik	24

Tabelle 6: Top 10 der am stärksten von Stalkerware betroffenen Länder in Lateinamerika (2022)

Weiterhin stammten 87 Prozent aller betroffenen, nordamerikanischen Nutzer aus den Vereinigten Staaten. Angesichts der relativen Bevölkerungsgröße der Vereinigten Staaten im Vergleich zu Kanada ist diese Relation nicht überraschend. Insgesamt waren in der Region Nordamerika 1.585 Nutzer betroffen.

	Land	Anzahl betroffener Nutzer
1	USA	1.295
2	Kanada	299

Tabelle 7: Gesamtzahl der von Stalkerware betroffenen Nutzer in Nordamerika (2022)



Weltweite Erkennung in Zahlen – Stalkerware-Programme

Dieser Abschnitt enthält eine Liste der Stalkerware-Programme, die weltweit am häufigsten verwendet wurden, um Smartphones auszuspionieren. Im Jahr 2022 Reptilicus (4.065 betroffene Nutzer) am häufigsten zum Einsatz. Insgesamt identifizierte Kaspersky im Jahr 2022 182 unterschiedliche Stalkerware-Apps.

	Name des Stalkerware-Programmes:	Anzahl betroffener Nutzer
1	Reptilicus (alias Vkurse)	4.065
2	Cerberus	2.407
3	KeyLog	1.721
4	MobileTracker	1.633
5	wSpy	1.342
6	SpyPhone	1.211
7	Anlost	1.189
8	Track My Phones	1.137
9	MonitorMinor	864
10	Hovermon	827

Tabelle 8: Liste der 10 am häufigsten verwendeten Stalkerware-Programme 2022

Stalkerware gibt dem Täter die Möglichkeit, die Kontrolle über das Leben einer anderen Person zu erlangen. Der Funktionsumfang variiert je nach Programmtyp und ob es sich um eine bezahlte oder eine kostenlose Version handelt. Stalkerware tarnt sich häufig unter dem Deckmantel einer legitimen Diebstahlschutz- oder Kindersicherungs-App. Tatsächlich wird sie ohne Zustimmung oder Hinweis an die überwachte Person installiert und läuft unbemerkt im Hintergrund,

Sind Android- und iOS-Geräte gleichermaßen von Stalkerware betroffen?

Stalkerware ist auf iPhones seltener zu finden als auf Android-Geräten, da es sich bei iOS um ein geschlossenes System handelt. Zwar könnte ein Täter durch Jailbreaking diese Barriere überwinden, dafür benötigt er jedoch direkten physischen Zugriff auf das Smartphone. iPhone-Nutzer, die eine Überwachung befürchten, sollten daher ihr Gerät nicht aus der Hand geben.

Alternativ dazu wäre es auch möglich, dass ein Täter seinem Opfer ein iPhone – oder ein anderes Gerät – gibt, auf dem die Stalkerware bereits vorinstalliert ist. Es gibt viele Online-Firmen, die als speziellen Dienst derartige Tools auf einem neuen Telefon installieren, damit es unter dem Deckmantel eines Geschenks original verpackt der betroffenen Person überreicht werden kann.

Zu den gängigsten Funktionen von Stalkerware-Programmen zählen:

- Nichtanzeige des App-Symbols
- Lesemöglichkeit von SMS, MMS und Anrufprotokollen
- Zugriff auf Kontaktlisten
- Verfolgung des GPS-Standorts
- Einsicht in den Kalender
- Lesen von Nachrichten aus beliebten Messenger-Diensten und sozialen Netzwerken wie Facebook, WhatsApp, Signal, Telegram, Viber, Instagram, Skype, Hangouts, Line, Kik, WeChat, Tinder, IMO, Gmail, Tango, SnapChat, Hike, TikTok, Kwai, Badoo, BBM, TextMe, Tumblr oder Weico, Reddit.
- Anzeige von Fotos und Bildern aus der Handy-Bildergalerie
- Aufnahme von Screenshots
- Fotoaufnahmen mit der Frontkamera (Selfie-Modus)

Digitales Stalking und geschlechtsspezifische Gewalt

Stalkerware ist eine Form des Stalkings und zählt damit zu digitaler Gewalt

Obwohl sowohl Männer als auch Frauen von Stalkerware betroffen sein können, zeigen Studien, dass überwältigend Frauen zum Ziel digitaler Gewalt werden. Dabei darf nicht vergessen werden, dass digitale Gewalt eine weitere Form von Gewalt darstellt. Da sie sich spürbar negativ auf die Betroffenen auswirkt, muss sie als Fortführung der Gewalt im realen Leben gesehen werden. Weitere Informationen hierzu sind im Merkblatt Cybergewalt gegen Frauen und Mädchen: Schlüsselbegriffe und Konzepte (2022) vom Europäischen Institut für Gleichstellungsfragen zu finden.

Daten sind zum Verständnis des Ausmaßes von digitaler Gewalt von großer Bedeutung — Dr. Leonie Maria Tanczer, Associate Professor am University College London und Head der UCL's Gender and Tech Research Group

Die bisherige Forschung zu Technologie-gestütztem Stalking und geschlechtsspezifischer Gewalt fokussierte herkömmliche digitale Systeme, die eine Person oder eine Gruppe zu etwas nötigen, kontrollieren und schädigen können. Zudem beschränken sich aktuelle Berichte und die vorhandenen Daten derzeit auf mobile Geräte. Allerdings kann digitales Stalking auch mithilfe weiterer Geräte erfolgen – darunter GPS-Tracker oder das sogenannte „Internet of Things" (IoT). Letzteres umfasst internetfähige Produkte wie beispielsweise intelligente Türklingeln, Überwachungskameras oder Lautsprecher.

Die Beweislage rund um Technologie-gestützten Missbrauch ist noch sehr limitiert. Derzeit findet die Forschung dazu vor allem in Australien, dem Vereinigten Königreich und den USA statt. Die meisten Studien nutzen folglich Daten aus diesen Ländern, was zu blinden Flecken führt. Daten, wie sie in diesem Bericht jedoch zu finden sind, tragen zu einem größeren Verständnis des Technologie-gestützten Missbrauchs bei. Dies ist auch dringend notwendig.

Es hat sich zudem gezeigt, dass Hilfsdienste für Betroffene beispielsweise mit der stetig wachsenden Anzahl neuer technologischer Entwicklungen zu kämpfen haben. Deshalb forderen sie Add-Ons zu den bereits bestehenden Risikobewertungs- und Sicherheitspraktiken – zum Beispiel „Aktionspläne zum Schutz vor Cyberstalking" sowie spezielle Schulungen. Damit sollen die Fähigkeiten und die Reaktionsfähigkeit der Helfer verbessert werden. Derzeit gibt es spezialisierte Dienstleistungsangebote, wie beispielsweise Refuge's Tech Safety team, das Safety Net Project des National Network to End Domestic Violence (NNEDV) oder die to End Tech Abuse (CETA).

Die Gender and Tech Research Group des University College London (UCL) hat es sich zur Aufgabe gemacht, die Schnittpunkte von Technologie, Sicherheit und Geschlecht zu untersuchen, um digitale Systeme für alle sicher nutzbar zu machen. Erfahren Sie mehr:

https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech

Betroffenen von digitaler Gewalt mehr Aufmerksamkeit widmen — Elena Gajotto, Vice President bei Una Casa Per L'Uomo

Cyberstalking hat direkte Auswirkungen auf das Leben der Betroffenen. Es gibt mittel- bis langfristige psychologische, physische sowie soziale Folgen, die wir täglich in unseren Anti-Gewalt-Zentren beobachten. Wie der European Parliament Research Service in seiner Studie (2021) zeigte, können potenziell alle Frauen von Cyberstalking betroffen sein – egal ob sie in der Öffentlichkeit stehen, eine Ex-Freundin sind oder einfach nur Soziale Medien nutzen. Cyberstalking umfasst verschiedene Arten von Verhaltensweisen, wie beispielsweise das Verschicken unzähliger Nachrichten, Überwachung der Aktivitäten oder andere Formen der Online-Verfolgung. Laut Studie „kann Cyberstalking auch einfach ein zusätzliches Tool des Stalkers sein".

Folgendes muss hinsichtlich digitaler Gewalt berücksichtigt werden:

- Digitale Gewalt kann zusammen mit anderen Formen von Gewalt – zum Beispiel körperlicher, sexueller, psychologische oder wirtschaftlicher – erfolgen.
- Gewalt kann online beginnen und sich dann offline fortsetzen – oder umgekehrt.
- Es ist fast unmöglich, beleidigende, gewalttätige oder triggernde Inhalte, die online veröffentlicht werden, dauerhaft zu entfernen.
- Bei den Tätern kann es sich um Einzelpersonen oder Gruppen handeln; sie können den Betroffenen sowohl bekannt als auch unbekannt sein.
- Digitale Gewalt kann über unterschiedliche Geräte, beispielsweise über den PC, das Smartphone oder auch Smart-Home-Geräte, und auf vielen verschiedenen Plattformen, wie Websites, Instant-Messaging-Apps, Online-Chats und soziale Medien, erfolgen.

Die Formen dieser Gewalt können, obwohl sie in der digitalen Welt ausgeübt werden, spürbare Auswirkungen auf das reale Leben der Betroffenen haben. Studien zeigen, dass hauptsächlich Frauen von Cyberstalking und weiteren Formen digitaler Gewalt betroffen sind. Sie leiden unter den gleichen Symptomen wie Betroffene von Offline-Gewalt, darunter Angstzustände, Panikattacken, Posttraumatische Belastungsstörung (PTBS), Suizidgedanken, Wut, mangelndes Selbstvertrauen oder Konzentrationsschwierigkeiten. Weiterhin kann sie zu negativen wirtschaftlichen Auswirkungen (zum Beispiel Erpressung oder Einkommensverlust) sowie zu Beziehungsproblemen (zum Beispiel Verlust des Familien- und Freundeskreises) oder soziale Isolation führen. Darüber hinaus hat digitale Gewalt mit einem Anstieg der öffentlichen Rechts-, Verwaltungs- und Gesundheitskosten sowie einer geringeren Beteiligung von Frauen am öffentlichen Diskurs auch kollektive Auswirkungen auf wirtschaftlicher und politischer Ebene.

Una Casa Per L'Uomo ist eine italienische zivilgesellschaftliche Organisation, die Hilfsdienste für Betroffene anbietet. Una Casa Per L'Uomo war Konsortialpartner des Projekts DeStalk (2021-2023), das vom Programm für Rechte, Gleichstellung und Unionsbürgerschaft der Europäischen Union kofinanziert wird, und ist Mitglied der Koalition gegen Stalkerware.

Es ist daher wichtig, auf die Gefahr hinzuweisen und die Aufmerksamkeit der Gesellschaft auf das Leiden, das durch digitale Gewalt verursacht wird, zu lenken. Unsere Mitglieder, Kaspersky und alle weiteren Partner der Koalition gegen Stalkerware arbeiten deshalb zusammen, um Betroffene zu unterstützen und Fachleute, die im Bereich der häuslichen Gewalt arbeiten, besser zu schulen.

Gesellschaftlichen Ansichten entgegentreten, die Technologie-gestützten Missbrauch unterstützen — Anna McKenzie, Communications Manager bei WWP EN

Technologie-gestützter Missbrauch, wie mithilfe von Stalkerware, ist ein zunehmendes Problem für unsere Mitglieder, die sich mit den Verhaltensweisen bei Tätern häuslicher Gewalt auseinandersetzen.

Digitale Gewalt ist weiterhin auf dem Vormarsch: Digitale Geräte, geheime Überwachungssoftware und Online-Räume bieten die perfekte Grundlage für Täter, um das Leben ihrer Partner zu kontrollieren. Es ist heutzutage so normal, das Telefon eines anderen zu überprüfen, dessen E-Mails zu lesen und dessen Standort sowie Passwörter zu kennen, dass die Täter oft nicht merken, dass es sich eigentlich um missbräuchliche Verhaltensweisen handelt.

Aber warum werden diese offensichtlichen Verstöße gegen die Privatsphäre nicht als solche wahrgenommen?

Im Jahr 2021 veröffentlichte Kaspersky den „Digital Stalking in Relationships Report", der einige beunruhigende Entwicklungen aufzeigte. Den Daten zufolge wurden Verhaltensweisen wie die Überwachung der digitalen Aktivitäten eines Partners mit dessen Zustimmung, um die Transparenz innerhalb einer Beziehung zu gewährleisten, weitgehend als akzeptabel angesehen. Besorgniserregend ist jedoch, dass fast ein Drittel der Befragten die Überwachung der Aktivitäten eines Partners ohne dessen Zustimmung in Ordnung findet – insbesondere, wenn sie glauben, dass ihr Partner untreu ist.

Diese Einstellung steht in direktem Zusammenhang mit den Schwierigkeiten, auf die unsere Mitglieder bei ihrer Arbeit mit Tätern häuslicher Gewalt regelmäßig stoßen. Es ist höchst problematisch, davon auszugehen, dass eine Person, die der Kontrolle nicht zustimmt, untreu ist. In missbräuchlichen Beziehungen ist das Einverständnis zudem zweifelhaft: Denn ist es wirklich ein Ja, wenn sie nicht Nein sagen können? Ebenso sehen Täter den Verdacht auf Untreue als einen guten Vorwand, um den Partner auszuspionieren. Das spricht auch für ein besitzergreifendes Verhalten sowie einen Mangel an gesunder Kommunikation. Beides ist in missbrauchen Beziehungen ein zentrales Problem.

Es ist offensichtlich, dass eine gesetzliche Regelung notwendig ist, Kapazitäten geschaffen werden müssen und mehr Aufklärung für das Thema digitale Gewalt nötig ist. Weiterhin müssen problematische Ansichten in Bezug auf Technologie-gestützten Missbrauch auf breiter Ebene – und von Kindesalter an – angesprochen werden. Studien wie der State of Stalkerware Report sind eine wichtige Quelle, um den Status quo zu kennen, jedoch muss mehr getan werden, um diesen auch zu ändern. Mit der Kampagne #NoExcuse4Abuse, die in Zusammenarbeit mit Kaspersky entwickelt und umgesetzt wurde, haben wir einen ersten Schritt getan, um schädlichen gesellschaftlichen Ansichten gegenüber Technologie-gestütztem Missbrauch und Stalkerware entgegenzutreten.

WWP EN ist ein europäisches Netzwerk mit 69 Mitgliedern aus 34 Ländern. Jede Strategie zur Beendigung von Gewalt in Beziehungen ist unserer Meinung nach fehlgeschlagen, wenn es nicht gelingt, die Täter von häuslicher Gewalt ins Visier zu nehmen und zur Rechenschaft zu ziehen. Unsere Arbeit konzentriert sich darauf, die Gewalt von Männern zu stoppen, sie zur Verantwortung zu ziehen und die Istanbul Concention zu fördern. Mehr Infos unter:

https://www.work-with-perpetrators.eu

Gemeinsam gegen Stalkerware

Stalkerware ist in erster Linie kein technisches, sondern ein gesellschaftliches Problem, und erfordert daher Maßnahmen aus allen Bereichen der Gesellschaft. Kaspersky setzt sich nicht nur aktiv für den Schutz vor dieser Bedrohung ein, sondern steht auch auf allen Ebenen weltweit im Dialog und arbeitet gemeinsam mit gemeinnützigen Organisationen, staatlichen Stellen, der Industrie und Forschung an Lösungenen.

Kaspersky war im Jahr 2019 der erste Cybersicherheitsanbieter, der einen nicht zu übersehenden Warnhinweis zu Stalkerware in seine Software eingebaut hat. Während die Lösungen von Kaspersky bereits seit vielen Jahren potenziell schädliche Apps melden, auch wenn es sich um keine Malware handelt (was auch für Stalkerware gilt), werden Nutzer in der neuen Benachrichtigung nun darauf hingewiesen, dass sich eine App auf dem Gerät befindet, die Spionagezwecken dienen könnte.

Im Jahr 2022 wurde der Privacy Alert im Rahmen der Einführung eines neuen Produktportfolios von Kaspersky für Privatanwender erweitert. Neben der reinen Warnung vor Stalkerware auf dem Gerät gibt es jetzt einen Hinweis, wenn die Person, die die App installiert hat, bei Deinstallation der Stalkerware eine Benachrichtigung erhält. Dies ist von Bedeutung, weil eine solche Information an den Täter die Situation eskalieren lassen könnte. Außerdem riskiert der Betroffene, dass wichtige Daten oder Beweise gelöscht werden, die bei der Strafverfolgung hilfreich sein könnten. Die neue Warnung ist in Abbildung 2 unten dargestellt. Der Privacy Alert von Kaspersky zum Schutz vor Stalkerware ist in allen Sicherheitslösungen für Privatanwender enthalten.

Coalition Against Stalkerware

Kaspersky war einer der Mitbegründer der Koalition gegen Stalkerware im Jahr 2019.- Die internationale Arbeitsgruppe hat sich der Bekämpfung von Stalkerware und häuslicher Gewalt verschrieben und bringt private IT-Unternehmen, NGOs, Forschungseinrichtungen und Strafverfolgungsbehörden zusammen, um Stalkerware zu bekämpfen und Betroffene von Online-Missbrauch zu unterstützen. Derzeit sind mehr als 40 Organisationen beteiligt; sie stehen im Austausch, um gemeinsam Lösungen gegen Online-Gewalt zu erarbeiten. Darüber hinaus finden Betroffene auf der Website der Koalition gegen Stalkerware, die in sieben Sprachen verfügbar ist, Hilfe und Anleitung, was zu tun ist, wenn sie vermuten, dass Stalkerware auf ihrem Gerät installiert wurde.

DeStalk
detect and stop stalkerware and cyberviolence against women

Weiterhin beteiligte sich Kaspersky zwischen 2021 und 2023 an dem EU-Projekt DeStalk, das vom EU-Programm für Rechte, Gleichstellung und Unionsbürgerschaft mitfinanziert wurde. Zu den fünf Projektpartnern, die ihr gesammeltes Know-how in dieses Konsortium einbrachten, gehörten Vertreter aus den Bereichen Cybersicherheit und Forschung, aber auch aus der Zivilgesellschaft und von staatlichen Behörden an. Im Rahmen des DeStalk-Projekts wurden insgesamt 375 Mitarbeiter von Frauenberatungsstellen und Täterprogrammen sowie Beamte aus den zuständigen Behörden in der Bekämpfung von Stalkerware und anderen digitalen Formen geschlechtsspezifischer Gewalt geschult. Weiterhin wurde die Öffentlichkeit für das Thema digitale Gewalt und Stalkerware sensibilisiert.

Als Teil dieses Projekts entwickelte Kaspersky eine Online-Schulung zum Thema Cybergewalt und Stalkerware. Diese ist Teil der Kaspersky-Automated Security-Awareness-Plattform, einer frei zugänglichen Mikro-Lernplattform im Internet, die in fünf verschiedenen Sprachen verfügbar ist. Bislang haben mehr als 130 Fachleute den Online-Kurs absolviert, weitere 80 nehmen gerade teil. Auch nach dem Auslaufen des DeStalk-Projekts ist der Online-Kurs weiterhin auf der Projekt-Website von DeStalk abrufbar: https://www.work-with-perpetrators.eu/destalk.

TinyCheck®

Im Juni 2022 launchte Kaspersky eine Website zu TinyCheck, auf der weitere Informationen zum Tool zu finden sind. TinyCheck ist ein kostenloses und sicheres Open-Source-Tool, das von gemeinnützigen Organisationen und Mitarbeitern der Polizei bei der Unterstützung von Betroffenen digitalen Stalkings eingesetzt werden kann. Es wurde im Jahr 2020 entwickelt, um Geräte auf Stalkerware und Spionageprogramme zu überprüfen, ohne dass der Täter darüber informiert wird. TinyCheck arbeitet unabhängig, muss nicht auf dem Gerät der betroffenen Person installiert werden und bleibt daher auch für den Täter unsichtbar. Über eine WLAN-Verbindung scannt TinyCheck den ausgehenden Datenverkehr und erkennt, wenn Interaktionen mit bekannten Quellen, wie typischen Stalkerware-Servern, stattfinden. TinyCheck ist außerdem unabhängig von der verwendeten Plattform einsetzbar, sei es iOS, Android oder ein anderes Betriebssystem.

Möchten Sie Gewissheit darüber, ob Sie von Stalkerware betroffen sind? Hier einige Tipps

Auch wenn Sie nicht von Stalkerware betroffen sind, finden Sie hier eine Reihe nützlicher Tipps, wie Sie sich schützen können:

- Schützen Sie Ihr Telefon mit einem sicheren Passwort, das Sie niemals mit Ihrem Partner, Freunden oder Kollegenteilen.
- Ändern Sie die Passwörter für alle Ihre Konten regelmäßig und geben Sie sie nicht an Dritte weiter.
- Laden Sie Apps grundsätzlich nur aus offiziellen Quellen wie Google Play oder dem App Store herunter.
- Installieren Sie eine zuverlässige IT-Sicherheitslösung wie Kaspersky Premium und scannen Sie Ihre Geräte regelmäßig. Wenn eventuell bereitsStalkerware installiert wurde, sollte dieser Schritt allerdings nur nach Abwägung aller potenziellen Gefahren erfolgen, da der Täter die Cybersicherheitslösung bemerken könnte.

Betroffene befinden sich häufig schon in einer Spirale der Gewalt, auch physischer.

Der Täter könnte eine Benachrichtigung erhalten, wenn ein Gerätescan durchgeführt oder die Stalkerware-App entfernt wird. Das wiederum kann zu einer Eskalation der Situation und zu weiterem aggressivem Verhalten führen. Deshalb sollten Sie unbedingt vorsichtig vorgehen, wenn Sie vermuten, dass Stalkerware auf Ihrem Gerät installiert ist.

- Wenden Sie sich **an eine Hilfsorganisation vor Ort:** Entsprechende Kontakte in Ihrer Nähe finden Sie auf der Webseite der Koalition gegen Stalkerware.
- **Achten Sie auf Warnzeichen:** Dazu gehören ein ständig leerer Akku aufgrund unbekannter oder verdächtiger Apps, die viel Strom verbrauchen, sowie neu installierte Apps mit verdächtigem Zugriff zur Nutzung und Nachverfolgung Ihres Standorts, zum Senden oder Empfangen von Textnachrichten und anderen privaten Aktivitäten. Überprüfen Sie auch, ob die Einstellung „Unbekannte Quellen“ aktiviert ist. Dies kann ein Hinweis darauf sein, dass unerwünschte Software von einer externen Quelle installiert wurde. Die genannten Anzeichen sind noch kein eindeutiger Beweis für Stalkerware auf Ihrem Gerät.
- **Versuchen Sie nicht, die Stalkerware zu löschen, Einstellungen zu ändern oder an Ihrem Telefon herumzuspielen:** Der potentielle Täter könnte darauf aufmerksam werden und die Situation könnte eskalieren. Außerdem riskieren Sie, dass wichtige Daten oder Beweise gelöscht werden, die bei der Strafverfolgung hilfreich sein könnten.

Wenn Sie weitere Informationen über unsere Aktivitäten zur Bekämpfung von Stalkerware benötigen oder Fragen haben, schreiben Sie uns gerne eine Mail an: ExtR@kaspersky.com.

Die Koalition gegen Stalkerware wurde im November 2019 als Reaktion auf die wachsende Bedrohung durch Stalkerware gegründet. Ziel ist es, die vielfältige Expertise der Partner bei der Unterstützung von Opfern häuslicher Gewalt und bei der Täterarbeit sowie bei der Förderung der Rechtssicherheit im Internet und der Vertretung digitaler Rechte bei kriminellem Verhalten, wie es durch Stalkerware ausgeübt wird, zusammenzubringen. Alle Mitglieder verpflichten sich, häusliche Gewalt, Stalking und Belästigung zu bekämpfen, indem sie den Einsatz von Stalkerware zum Thema machen und einer breiten Öffentlichkeit ins Bewusstsein rufen.

Die Koalition gegen Stalkerware:
https://stopstalkerware.org

TinyCheck:
https://tiny-check.com

Neuigkeiten zuCyberbedrohungen: www.securelist.com
IT-Sicherheitsnachrichten: business.kaspersky.com
IT-Sicherheit für kleine und mittlere Unternehmen:
www.kaspersky.de/small-to-medium-business-security
IT-Sicherheit für Großunternehmen:
www.kaspersky.de/enterprise-security

www.kaspersky.de

Coalition Against Stalkerware

TinyCheck®

kaspersky