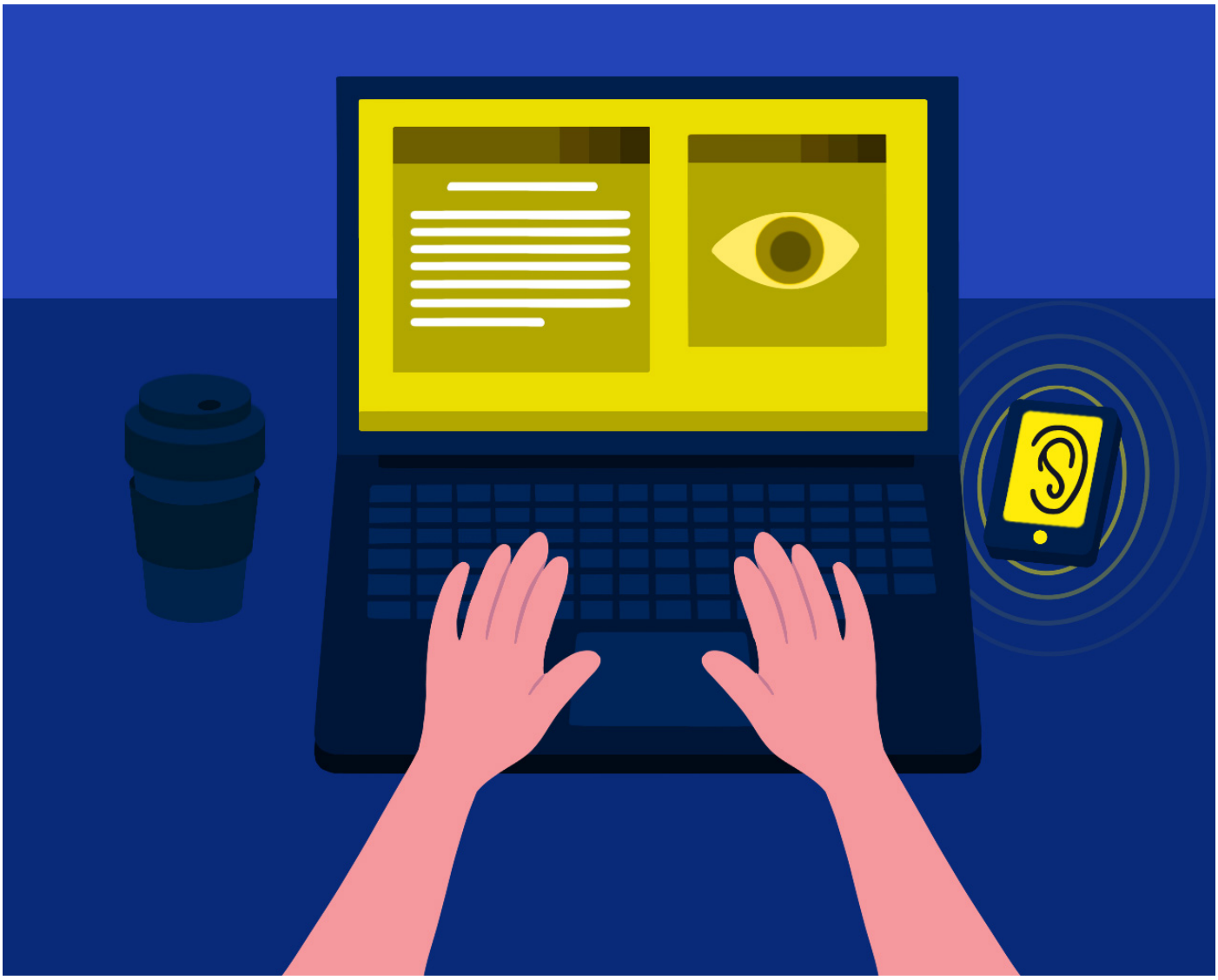


Stalkerware: Entwicklungen im Jahr 2021

COALITION AGAINST STALKERWARE

kaspersky

Inhalt

Zentrale Erkenntnisse aus dem Jahr 2021

Kaspersky analysiert jedes Jahr die weltweiten Entwicklungen im Bereich Stalkerware. So kann ein umfassendes Bild von der aktuellen Bedrohungslage in diesem Bereich gezeichnet werden. Dazu arbeiten wir mit Vertretern des öffentlichen und privaten Sektors zusammen, um für dieses wichtige Thema zu sensibilisieren und Lösungen für den Umgang mit Stalkerware zu entwickeln.

Stalkerware ermöglicht, mittels intelligenter Geräte das Privatleben einer Person auszuspionieren und kommt oft zum Einsatz, um Lebenspartner psychischer und physischer Gewalt auszusetzen. Die dazu nötige Software kann man käuflich erwerben und so auf eine ganze Reihe persönlicher Daten zugreifen, wie Gerätestandort, Browserverlauf, Textnachrichten, Chats in sozialen Medien, Fotos und vieles andere mehr. Die Vermarktung von Stalkerware an sich ist nicht verboten, wohl aber ihr Einsatz ohne die Zustimmung des Opfers. Diesen immer noch ziemlich unklaren rechtlichen Rahmen, der nach wie vor in vielen Ländern Bestand hat, machen sich die Täter zunutze. Der Einsatz von Stalkerware stellt eine Verletzung der Privatsphäre und eine Form von technischem Missbrauch dar. Stalkerware ist eine komplexe Bedrohung, der man im Sinne eines bestmöglichen Schutzes nur mit innovativen Tools begegnen kann, die alle rechtlichen, sozialen und technologischen Aspekte gleichermaßen berücksichtigen.

Zentrale Daten für 2021

- **Laut Daten von Kaspersky waren 2021 weltweit 32.694 Nutzer von Stalkerware betroffen.** Damit ist die Zahl im Vergleich zu den 2020 von uns erfassten Daten weiter rückläufig und markiert den bisher niedrigsten Stand seit Beginn der Datenerfassung zu Stalkerware im Jahr 2018. Von diesem vermeintlich positiven Trend sollte man sich allerdings nicht täuschen lassen.
- Denn vor allem seit Beginn der Pandemie **nimmt die Cybergewalt stetig zu.** Kontaktbeschränkungen und die Tatsache, dass die Menschen immer mehr Zeit zu Hause verbringen, gibt den Tätern ein Gefühl der Kontrolle, ohne ihren Partnern mithilfe von Stalkerware nachzuspionieren. Abgesehen davon gibt es dank intelligenter Geräte leider unzählige andere Möglichkeiten, sein Opfer auszuspähen oder ihm nachzustellen. Aus ihrer Arbeit mit den Tätern und Opfern von Stalkerware berichten auch gemeinnützige Organisationen, mit denen Kaspersky eng zusammenarbeitet, von ganz ähnlichen Entwicklungen. Man darf außerdem nicht vergessen, dass sich diese Zahlen nur auf Kaspersky-Nutzer beziehen: Wer die IT-Sicherheitslösungen unserer Mitbewerber verwendet oder gar keine IT-Sicherheitslösungen auf seinem Mobilgerät installiert hat, taucht in dieser Statistik nicht auf. Was wir sehen, ist also nur die Spitze des Eisbergs. Aber auch wenn sich die exakte Zahl der Betroffenen weltweit kaum ermitteln lässt, gehen die Mitglieder der Koalition gegen Stalkerware davon aus, dass sie mindestens 30 Mal so hoch ist. Damit käme man pro Jahr weltweit auf nahezu eine Million Opfer.

- **Auf der Grundlage von Daten aus dem Kaspersky Security Network gehören Russland, Brasilien und die Vereinigten Staaten nach wie vor zu den am stärksten betroffenen Ländern.** Das zeigten auch die Zahlen der letzten beiden Jahre. Nach Region findet man die höchsten Opferzahlen in:
  - Deutschland, Italien und Großbritannien (Europa)
  - der Türkei, Ägypten und Saudi-Arabien (Naher Osten und Afrika)
  - Indien, Indonesien und Vietnam (asiatisch-pazifischer Raum)
  - Brasilien, Mexiko und Kolumbien (Lateinamerika)
  - den Vereinigten Staaten (Nordamerika)
  - Die Russische Föderation, Ukraine und Kasachstan (Osteuropa (ohne EU-Länder), Russland und Zentralasien)
- **Cerberus und Reptilicus gehörten weltweit zu den am häufigsten eingesetzten Stalkerware-Programmen,** mit jeweils 5.575 bzw. 4.417 betroffenen Nutzern.

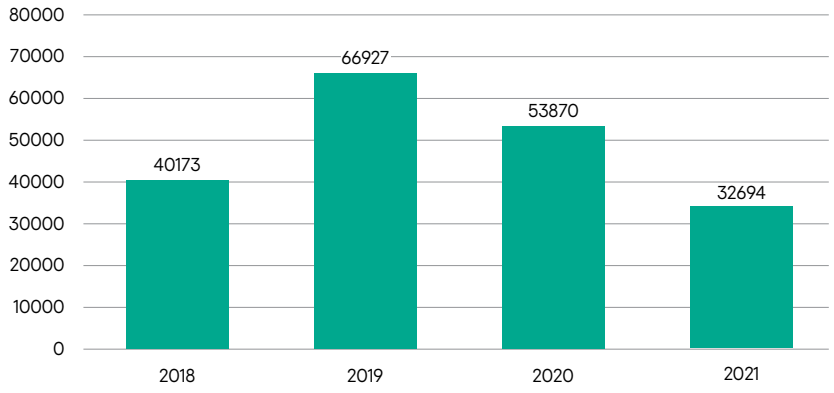
Von Kaspersky beobachtete Trends

Erkennungen in Zahlen: betroffene Nutzer weltweit

In diesem Abschnitt werden die von Kaspersky für 2021 ermittelten globalen und regionalen Zahlen vorgestellt und mit den Werten der Vorjahre verglichen.

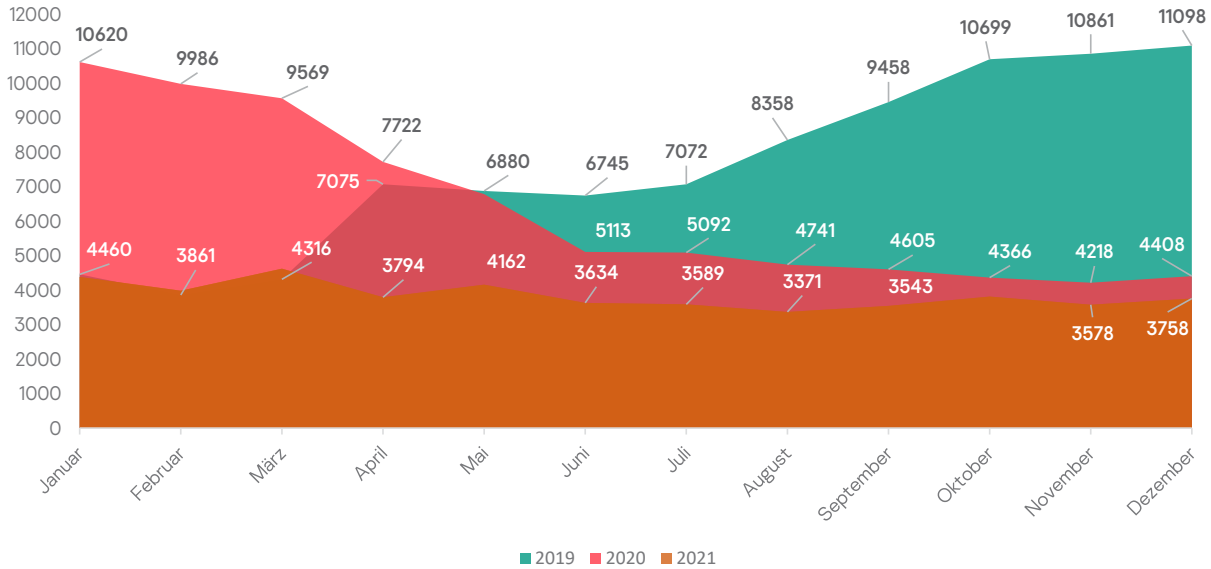
Im Jahr 2021 waren insgesamt 32.694 Nutzer von Stalkerware betroffen

Im Jahr 2021 waren insgesamt 32.694 Nutzer von Stalkerware betroffen. Die folgende Grafik zeigt die zahlenmäßige Entwicklung der betroffenen Nutzer seit 2018.



Entwicklung der betroffenen Benutzer von Jahr zu Jahr seit 2018

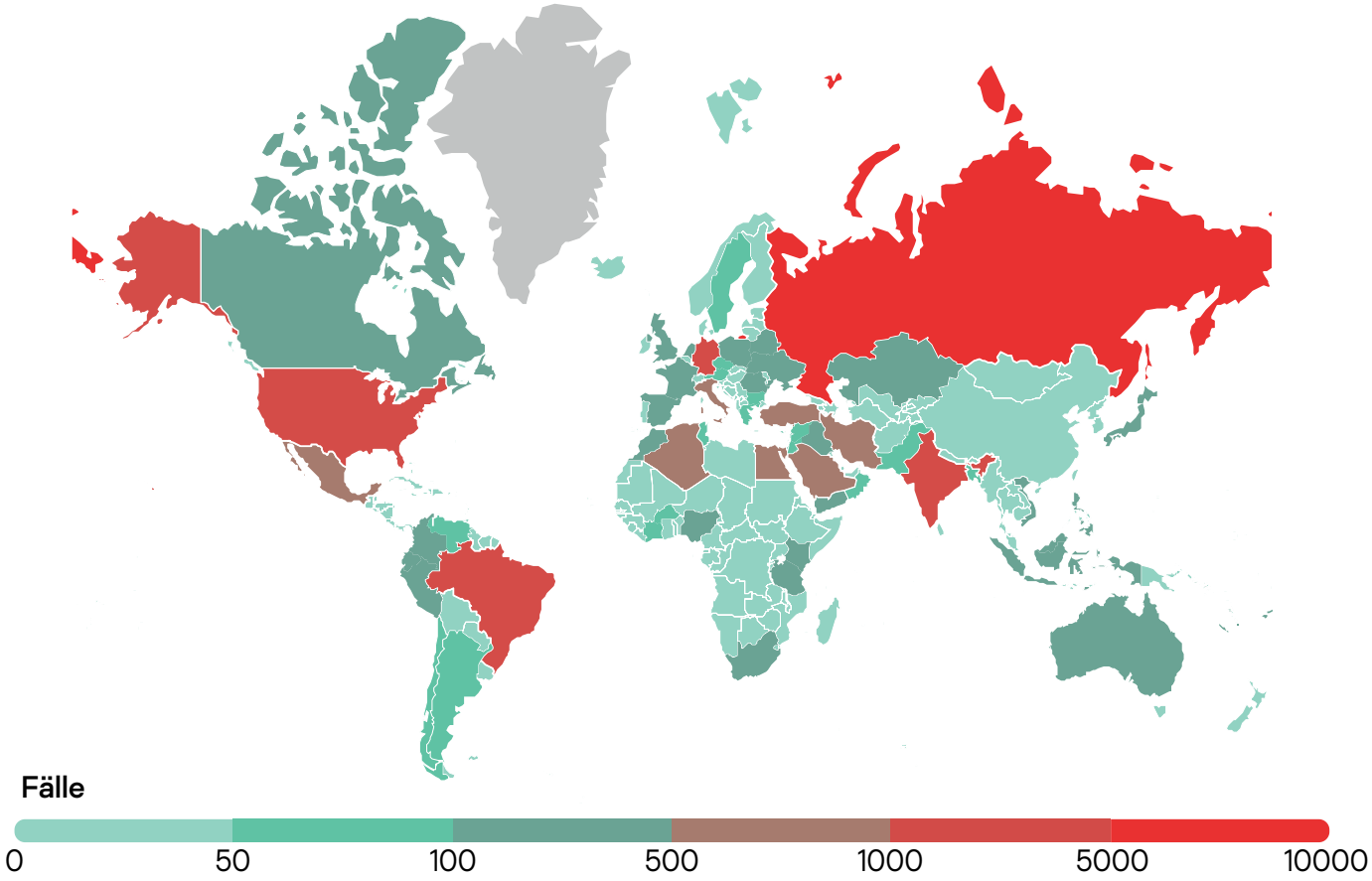
In der nachstehenden Grafik ist die Anzahl der betroffenen Nutzer pro Monat für die Jahre 2019 bis 2021 dargestellt. Wie zu erkennen ist, war der Trend 2021 stabiler als im Jahr 2020. In den Monaten, die am meisten von den Schließungen und Quarantänemaßnahmen geprägt waren, wurde ein deutlicher Rückgang verzeichnet.



Einmalige betroffene Benutzer pro Monat im Zeitraum 2019-2021

Globale und regionale Verteilung der Erkennungen: am stärksten betroffene Regionen

Nutzer sind weltweit auch weiterhin von Stalkerware betroffen: Im Jahr 2021 hat Kaspersky betroffene Nutzer in 185 Ländern oder Regionen verzeichnet.



Methodik

Die Bedrohungsstatistiken des Kaspersky Security Network bilden die Datengrundlage für diesen Bericht. In das Kaspersky Security Network fließen die sicherheitsrelevanten Datenströme von Millionen freiwilliger Teilnehmer weltweit ein. Alle diese Daten werden anonymisiert verarbeitet. Für die Erstellung unserer Statistiken haben wir unsere Produktpalette der mobilen Sicherheitslösungen für Privatkunden nur anhand der Erkennungskriterien der Koalition gegen Stalkerware überprüft. Das bedeutet, dass die betroffenen Nutzer ausschließlich das Ziel von Stalkerware waren. Andere Arten von Überwachungs- oder Spyware-Anwendungen, die nicht unter die Definition der Koalition fallen, sind nicht in die Statistik mit eingeflossen.

Somit spiegeln die Statistiken die Anzahl der von Stalkerware betroffenen Handynutzer wider, nicht die Anzahl der Erkennungen. Die Zahl der Erkennungen kann höher liegen, da wir eine Stalkerware möglicherweise mehrmals auf demselben Gerät desselben Nutzers erkennen, wenn dieser Nutzer nach Erhalt unserer Benachrichtigung die App nicht entfernt.

Zudem werden nur Handynutzer in der Statistik berücksichtigt, die IT-Sicherheitslösungen von Kaspersky nutzen. Manche Nutzer könnten eine andere Cybersicherheitslösung auf ihren Geräten nutzen, andere wiederum gar keine.

Wie schon 2020 sind Russland, Brasilien, die Vereinigten Staaten und Indien erneut die vier Länder mit der höchsten Zahl an betroffenen Einzelnutzern. Interessanterweise ist Mexiko vom fünften auf den neunten Platz gefallen und Algerien, die Türkei und Ägypten sind mittlerweile unter den Top 10 zu finden. Stattdessen gehören Italien, Großbritannien und Saudi-Arabien nicht mehr zu den 10 Ländern mit den höchsten Fallzahlen.

	Land	Betroffene Nutzer
1	Russische Föderation	7541
2	Brasilien	4807
3	USA	2319
4	Indien	2105
5	Deutschland	1012
6	Iran (Islamische Republik)	891
7	Algerien	665
8	Türkei	660
9	Mexiko	657
10	Ägypten	640

Tabelle 1: Die 10 Länder mit den höchsten Stalkerware-Fallzahlen des Jahres 2021 – weltweit

Der diesjährige Bericht enthält ausführlichere regionale Statistiken für Europa, den asiatisch-pazifischen Raum, Lateinamerika, Nordamerika, Osteuropa (ohne EU-Länder), Russland und Zentralasien sowie den Nahen Osten und Afrika.

In Europa lag die Gesamtzahl der betroffenen Einzelnutzer im Jahr 2021 bei 4.236. Deutschland, Italien und Großbritannien stehen wie bereits im letzten Jahr auf der Liste ganz weit oben. Österreich wurde in den Top 10 von der Tschechischen Republik abgelöst.

	Land	Betroffene Nutzer
1	Deutschland	1012
2	Italien	611
3	Großbritannien und Nordirland	430
4	Frankreich	410
5	Polen	321
6	Spanien	321
7	Niederlande	165
8	Rumänien	125
9	Belgien	94
10	Tschechische Republik	82

Tabelle 2: Die 10 Länder mit den höchsten Stalkerware-Fallzahlen des Jahres 2021 – Europa

In Osteuropa (ohne EU-Länder), Russland und Zentralasien lag die Gesamtzahl der betroffenen Einzelnutzer bei 9.207. Auf den drei Spitzenplätzen lagen Russland, die Ukraine und Kasachstan.

	Land	Betroffene Nutzer
1	Russische Föderation	7541
2	Ukraine	490
3	Kasachstan	461
4	Weißrussland	250
5	Usbekistan	223
6	Aserbaidschan	92
7	Republik Moldau	51
8	Tadschikistan	49
9	Kirgisistan	40
10	Turkmenistan	19

Tabelle 3: Die 10 Länder mit den höchsten Stalkerware-Fallzahlen des Jahres 2021 – Osteuropa (ohne EU-Länder), Russland und Zentralasien

Im Nahen Osten und in Afrika lag die Gesamtzahl der betroffenen Einzelnutzer in der gesamten Region bei 6.270. Die höchsten Fallzahlen wurden in der Türkei, Ägypten und Saudi-Arabien verzeichnet.

	Land	Betroffene Nutzer
1	Türkei	660
2	Ägypten	640
3	Saudi Arabien	575
4	Kenia	271
5	Südafrika	240
6	Vereinigte Arabische Emirate	143
7	Nigeria	123
8	Kuwait	68
9	Oman	58
10	Äthiopien	46

Tabelle 4: Die 10 Länder mit den höchsten Stalkerware-Fallzahlen des Jahres 2021 – Nahen Osten und in Afrika

Im APAC-Raum lag die Gesamtzahl der betroffenen Einzelnutzer bei 4.243. Mit 2.105 betroffenen Einzelnutzern lag Indien deutlich vor den anderen Ländern. Dahinter folgen Indonesien und Vietnam.

	Land	Betroffene Nutzer
1	Indien	2105
2	Indonesien	353
3	Vietnam	258
4	Philippinen	240
5	Malaysia	229
6	Australien	205
7	Bangladesch	169
8	Japan	167
9	Pakistan	98
10	Sri Lanka	83

Tabelle 5: Die 10 Länder mit den höchsten Stalkerware-Fallzahlen des Jahres 2021 – asiatisch-pazifischer Raum

Die Rangliste für Lateinamerika und die Karibik führte vor allem ein Land an: Brasilien, auf das 72,5 % der Gesamtzahl der betroffenen Nutzer (und etwa 32 % der Bevölkerung) in der Region entfielen. Hinter Brasilien folgten Mexiko und Kolumbien. In der gesamten Region waren 6.609 Nutzer betroffen.

	Land	Betroffene Nutzer
1	Brasilien	4807
2	Mexiko	657
3	Kolumbien	202
4	Ecuador	192
5	Peru	179
6	Argentinien	90
7	Chile	73
8	Venezuela	58
9	Bolivien	46
10	Haiti	36

Tabelle 6: Die 10 Länder mit den höchsten Stalkerware-Fallzahlen des Jahres 2021 – Lateinamerika

In Nordamerika entfielen 87 % der betroffenen Nutzer auf die USA, was angesichts der hohen Einwohnerzahl (zehn Mal höher als in Kanada) nicht sonderlich überrascht. Die Gesamtzahl der Betroffenen in Nordamerika (ohne Mexiko, das in den Daten für Lateinamerika enthalten ist) liegt bei 2.666.

	Land	Betroffene Nutzer
1	USA	2319
2	Kanada	347

Tabelle 7: Von Stalkerware betroffene Benutzer im Jahr 2021 – Nordamerika

Gängige Funktionen von Stalkerware-Programmen

In diesem Abschnitt werden die Stalkerware-Programme aufgelistet, die global gesehen am häufigsten eingesetzt werden, um mobile Geräte zu kontrollieren. Dabei sind Cerberus und Reptilicus die weltweit führenden Stalkerware-Programme mit jeweils 5.575 bzw. 4.417 betroffenen Nutzern.

	Name des Programms	Betroffene Nutzer
1	Cerberus	5,575
2	Reptilicus (alias Vkurse)	4,417
3	Track My Phones	1,919
4	AndroidLost	1,731
5	MobileTracker Free	1670
6	Hoverwatch	1,094
7	wSpy	1,050

Tabelle 8: Liste der am häufigsten verwendeten Stalkerware-Programme 2021

Abhängig vom Programm und davon, ob dieses in der kostenlosen oder in der jeweiligen Bezahlversion eingesetzt wird, kann Stalkerware ihrem Nutzer ein sehr hohes Maß an Eingriffsmöglichkeiten verschaffen. Angepriesen als Diebstahl- oder Kindersicherung gehen einige dieser Programme weit darüber hinaus, angefangen beim so genannten verborgenen Modus, in dem die Software ohne die Zustimmung und das Wissen des Opfers läuft.

Die meisten der gängigen Anwendungen bieten typische Stalkerware-Funktionen, wie z. B.:

- Verbergen des App-Symbols
- Lesen von SMS, MMS und Anrufprotokollen
- Abruf von Kontaktlisten

Sind Android OS und iOS gleichermaßen von Stalkerware betroffen?

Stalkerware-Tools sind auf iPhones seltener anzutreffen als auf Android-Geräten, da iOS sich für ein geschlossenes System entschieden hat. Auch dieses System kann zwar durch Jailbreaking überwunden werden, die Täter benötigen dafür aber direkten physischen Zugriff auf das Smartphone. iPhone-Benutzer, die eine Überwachung befürchten, sollten daher ihr Gerät nicht aus der Hand geben.

Alternativ dazu kann ein Täter seinem Opfer ein iPhone – oder ein anderes Gerät – geben, auf dem die Stalkersoftware 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 dem künftigen Opfer überreicht werden kann.

- Verfolgung des GPS-Standorts
- Einsicht in Kalendereinträge
- 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, Weico, Reddit usw.
- Anzeige von Fotos und Bildern aus der Handy-Bildergalerie
- Aufnahme von Screenshots
- Fotoaufnahmen mit der Frontkamera (Selfie-Modus)

Der Einsatz von Stalkerware mag rückläufig sein, nicht aber die Gewalt

Neben den Opferzahlen sind auch einige Verhaltensweisen sowie die grundlegende Einstellung gegenüber Stalkerware nach wie vor besorgniserregend

Auch wenn wir bei den Betroffenen einen Rückgang um 39 % gegenüber unseren Daten für 2020 feststellen, ist der Kampf gegen Stalkerware und Cybergewalt noch lange nicht vorbei. Neben den Opferzahlen sind auch einige Verhaltensweisen sowie die grundlegende Einstellung gegenüber Stalkerware nach wie vor besorgniserregend. Im November 2021 gab Kaspersky eine weltweite Umfrage in Auftrag, bei der mehr als 21.000 Teilnehmer in 21 Ländern zu ihrer Einstellung zu Privatsphäre und digitalem Stalking in intimen Beziehungen befragt wurden. Während die Mehrheit der Befragten (70 %) es nicht für akzeptabel hält, den Partner ohne seine Zustimmung zu überwachen, sieht ein erheblicher Anteil der Befragten (30 %) kein Problem darin und findet es unter bestimmten Umständen akzeptabel. Von denjenigen, die der Meinung sind, dass es gute Gründe für eine heimliche Überwachung gibt, würden es fast zwei Drittel tun, wenn es darum ginge, sich Gewissheit über eine vermeintliche Untreue des Partners (64 %) oder dessen Sicherheit (63 %) zu verschaffen. Die Hälfte würde sich darauf einlassen, wenn es um eine mögliche Verwicklung des Partners in kriminelle Aktivitäten (50 %) ginge.

IKT-Technologien sind mächtige Werkzeuge für Täter, um ihre Opfer zu kontrollieren, insbesondere in Beziehungen, in denen physische Gewalt bereits an der Tagesordnung ist

Schnelles Internet in Verbindung mit der raschen Verbreitung der Informations- und Kommunikationstechnologien (IKT) hat die Cybergewalt begünstigt, indem es den Tätern ein weiteres Instrument an die Hand gibt, um gewaltverherrlichendes und gefährliches Material zu verbreiten oder durch ihr Verhalten emotionalen, psychischen oder physischen Schaden zu verursachen. Während diese Technologien den Menschen einerseits die Möglichkeit geben, soziale Kontakte über räumliche Distanzen hinweg zu pflegen, haben IKT auch der Cybergewalt den Weg geebnet – mit verheerenden Auswirkungen auf die reale Welt und negativen Folgen für das tägliche Leben der Opfer.

Die Ergebnisse unserer Umfrage bestätigen das: 15 % der Befragten weltweit wurden von ihrem Partner gezwungen, eine Überwachungs-App zu installieren, 34 % erlebten außerdem körperliche und/oder verbale Gewalt durch den Intimpartner.

Auch wenn es für endgültige Schlüsse aus dem zahlenmäßigen Rückgang der Betroffenen im Jahr 2021 noch zu früh ist, gibt es zwei Theorien, die diesen Trend erklären könnten.

Zum einen sind wir der Meinung, dass die Pandemie unser aller Leben immer noch stark prägt. Jüngste Studien zeigen, dass sich unser Verhalten in allen Lebensbereichen wandelt, sei es beim Arbeiten, Lernen, Wohnen, Konsumieren, beim Reisen oder der Mobilität, der Kommunikation oder Information. Kurz gesagt, die Menschen verbringen mehr Zeit zu Hause (49 % vermeiden es, das Haus zu verlassen, 50 % arbeiten ganz oder teilweise im Homeoffice), reduzieren ihre privaten Kontakte (57 % geben an, Distanz zu Freunden und Bekannten zu halten) und nutzen für Reisen, Einkäufe, Fortbildung und Unterhaltung vermehrt das Internet. Aus Sicht eines Missbrauchstäters bedeutet das, dass er seinem Partner nicht mehr nachspionieren muss, weil er ihn sowieso die meiste Zeit im Blick hat.

Zum zweiten sind das Internet der Dinge (IoT) und die Digitalisierung mittlerweile zu einem festen Bestandteil unseres Lebens geworden. Technische Geräte sind allgegenwärtig – im Alltag, zu Hause, im Auto und im Büro. Aber neben den vielen Chancen und Vorteilen ermöglichen sie auch die ständige Überwachung durch Dritte. Unsere Forschung legt nahe, dass die Täter neben Stalkersoftware auch andere Mittel nutzen, um ihre Partner auszuspähen. 50 % der Befragten gaben an, dass ihnen über Telefon-Apps nachgestellt wurde, weitere 29 % wurden über Ortungsgeräte, 22 % über Webcams und 18 % über Smart-Home-Geräte ausspioniert.

Die jüngste Veröffentlichung eines Sicherheitshandbuchs von Apple für sein AirTag-Produkt im Januar 2022 zeigt, dass ein Umdenken in der Wahrnehmung der Situation eingesetzt hat.

NNEDV, das Nationale Netzwerk zur Beendigung häuslicher Gewalt, und WWP EN, das Europäische Netzwerk für die Arbeit mit Tätern häuslicher Gewalt, geben uns einen Einblick in ihre Erfahrungen und Ansichten zu diesen beiden Theorien und zum technischen Missbrauch im Allgemeinen.

WWP EN

Das Europäische Netzwerk für die Arbeit mit Tätern häuslicher Gewalt (WWP EN) ist ein Zusammenschluss von Organisationen, die direkt oder indirekt mit Menschen arbeiten, die in engen Beziehungen gewalttätig werden. Das Hauptaugenmerk von WWP EN liegt auf der Gewalt von Männern gegenüber Frauen und Kindern. Um Frauen, Kinder und andere von Gewalt in der Beziehung bedrohte Personen zu schützen, versucht die Organisation, mit ihrer Arbeit bei denen anzusetzen, von denen diese Gewalt ausgeht, hauptsächlich Männer.

www.work-with-perpetrators.eu/experiencing-violence

Wie die während der Pandemie auferlegten staatlichen Maßnahmen den Kontrollzwang und die Kontrollmöglichkeiten der Täter verstärkt haben — **Berta Vall Castelló, Leiterin der Forschungs- und Entwicklungsabteilung und Anna McKenzie, Sprecherin von WWP DE**

Kontrollzwang wird definiert als „ein missbräuchliche Verhaltensmuster, das darauf abzielt, den Beziehungspartner zu dominieren und zu kontrollieren. Dazu gehört eine ganze Reihe von missbräuchlichen Verhaltensweisen – physische, psychische, emotionale oder finanzielle Machtausübung – die den Opfern im Laufe der Zeit ihre individuelle Selbständigkeit und Unabhängigkeit rauben." (McGorrery and McMahon, 2020) Wie wir in unserem Handbuch „Same Violence, New Tools – How to work with violent men who use cyberviolence" schreiben, isolieren die Täter ihre Partner und machen sie emotional abhängig. Mit Schlägen, Drohungen, Einschüchterung, Demütigung, Isolation und anderen Methoden schaffen sie ein Klima der Angst und das Gefühl des Eingesperrtseins. IKT-Technologien sind mächtige Werkzeuge für Täter, um ihre Opfer zu kontrollieren, insbesondere in Beziehungen, in denen physische Gewalt bereits an der Tagesordnung ist.

Eine erst kürzlich durchgeführte Studie zur häuslichen Gewalt während der Corona-Pandemie ergab, dass die verhängten Lockdown-Maßnahmen den Kontrollzwang und die Kontrollmöglichkeiten der Täter noch verstärkt haben. Die Autoren vermuten, dass die staatlich verhängte Isolation und die Kontaktbeschränkungen den Kontrollmaßnahmen der Täter gegenüber ihren Partnern Vorschub leisten (Pentaraki und Speake, 2020). Vor diesem Hintergrund ist davon auszugehen, dass die Täter weniger die Notwendigkeit sehen, ihre Partner mithilfe von Stalkerware zu kontrollieren. Jüngste Studien haben zudem ergeben, dass der Missbrauch mithilfe von Technik meist in der Trennungsphase seinen Höhepunkt erreicht (George und Harris 2014; Woodlock 2016). Paare, die während eines Lockdowns sowieso gezwungen sind, gemeinsam zu Hause zu bleiben, werden sich so gesehen eher nicht mit technischen Mitteln bespitzeln.

Man darf nicht den Fehler begehen, den rückläufigen Einsatz von Stalkerware während der Pandemie mit einer Abnahme der Gewalt in Paarbeziehungen gleichzusetzen. Ganz im Gegenteil: Boxall, Morgan und Brown (2020) weisen darauf hin, dass die Ausübung von Gewalt in der Beziehung während der Corona-Pandemie zugenommen hat. Nach den Ergebnissen dieses Berichts scheint eher eine Verlagerung von Stalkerware zu anderen Tools stattgefunden zu haben. Wie Elena Gajotto von der italienischen NRO Una

Die verhängten Lockdown-Maßnahmen den Kontrollzwang und die Kontrollmöglichkeiten der Täter noch verstärkt haben

Casa per l'Uomo ausführt: „Es ist so einfach, jemanden zu bespitzeln und auszuspionieren, zum Beispiel über sein Google-Konto, dass man eigentlich keine Stalkerware mehr braucht." Vor diesem Hintergrund könnte der Rückgang beim Einsatz von Stalkerware auf die breite Palette an alternativen technischen Möglichkeiten zurückzuführen sein. Letizia Baroncelli von Centro Ascolto Uomini Malttratanti (CAM), einer gemeinnützigen Organisation aus Italien, kann das nur bestätigen und ergänzt: „Ich glaube, wir sehen weniger Stalkerware, weil es so viele andere Formen des digitalen Missbrauchs gibt."

Seit Beginn der Pandemie berichten Nichtregierungsorganisationen, Regierungen und Forscher von einer erheblichen Zunahme bei der sexuellen Erpressung mit Bildern, Sextortion genannt (Boniello, 2020; CCRI, in einem persönlichen Schreiben, 2. Juni 2020; FBI, 2020, 2021). Diese Art des Technik-gestützten Missbrauchs scheint enormen Aufwind bekommen zu haben, insbesondere bei Jugendlichen und getrennt lebenden Paaren. Wie Letizia Baroncelli bemerkt: „Der Austausch von privaten Bildern hat in Pandemiezeiten stark zugenommen, vor allem bei jungen Tätern. Denen ist oft nicht einmal klar, dass das eine Straftat ist." Und Elena Gajotto fügt hinzu: „Die Weitergabe sehr privater Bilder fügt den betroffenen Frauen erhebliches Leid zu, während die Männer gar nichts dabei finden."

Mehrere WWP EN-Mitglieder berichten, dass die häufigste Form der digitalen Gewalt darin besteht, dass Männer die digitalen Aktivitäten ihrer Partnerinnen überwachen, indem sie z. B. E-Mails, Telefone und soziale Konten kontrollieren. Diese Annahme deckt sich mit den Beobachtungen von Daniel Antunovic von der kroatischen Nichtregierungsorganisation UZOR, dass meist diese „primitiven" Formen des digitalen Stalkings zum Einsatz kommen.

Wir von WWP EN sind der Ansicht, dass man sich auf den mit technischen Mitteln durchgeführten Missbrauch konzentrieren sollte, um die Sicherheit der Opfer zu gewährleisten. Und Elena Gajotto ergänzt: „Etwa die Hälfte der Männer lassen andere an ihrer digitalen Gewalt teilhaben, ohne sich klar zu machen, dass dies eine Form des Missbrauchs ist. Wenn wir in unserer Arbeit mit den Tätern nicht explizit darauf eingehen, werden sie es nie verstehen." Daher braucht es mehr Aufklärung für alle, die mit Tätern und Opfern häuslicher Gewalt arbeiten, damit sie Fälle von digitaler Gewalt erkennen und dagegen einschreiten können. Wie Daniel Antunovic hinzufügt: „Wir haben seit Corona weniger Fälle von digitaler Gewalt gesehen als erwartet. Der mit technischen Mitteln durchgeführte Missbrauch ist jedoch in gewisser Weise mit sexualisierter Gewalt vergleichbar. Beides kommt häufig vor, bleibt aber unsichtbar."

NNEDV

Beim Safety Net Project von NNEDV geht es um die Schnittstellen zwischen Technologie, Datenschutz, Vertraulichkeit und Innovation in Bezug auf Sicherheit und Missbrauch. Im Rahmen des Projekts werden politische Maßnahmen gefördert, Befürworter und Fachleute im Justizsystem geschult. Zusammen mit Gemeinden, Behörden und Technologieunternehmen wird daran gearbeitet, wirksame Maßnahmen gegen technischen Missbrauch zu ergreifen, Überlebende bei der Nutzung moderner Technik zu unterstützen und Technologien im Sinne besserer Services zu beschränken.

https://nnedv.org/content/mission-vision/

Die Zahl der „smarten Geräte", die bei Gewalt in der Partnerschaft eingesetzt werden, nimmt zu — Toby Shulruff, Projektleiter für technische Sicherheit bei NNEDV

Stalkerware ist zwar ein weit verbreitetes Problem, es gibt aber auch viele andere missbräuchlich eingesetzte Tools, die oft nur wie Stalkerware aussehen, ohne es zu sein. So können beispielsweise ganz legal im Internet verfügbare persönliche Informationen und die alltäglichen Funktionen von Geräten und Konten genutzt werden, um den Standort einer Person zu ermitteln oder ihre Aktivitäten zu verfolgen. Die Komplexität und Abhängigkeit zwischen Geräten, Konten und Informationen im Internet machen es den Opfern und ihren Unterstützern oft schwer, das Geschehene nachzuvollziehen und wirksame Antworten zu finden. Für Überlebende ist es häufig geradezu beängstigend und überwältigend zu sehen, wie viele Details der Täter aus ihrem täglichen Leben kennt.

Leider werden immer mehr „smarte" Geräte, d. h. vernetzte Geräte und Sicherheitssysteme, die mit WLAN-Netzwerken und Smartphones verbunden sind, als Mittel zur Gewalt in der Partnerschaft missbraucht.

Eine Erhebung der NNEDV im Dezember 2020 und Januar 2021 zeigt, dass es während der Pandemie zu einer erheblichen Zunahme aller Arten von Technik-basiertem Missbrauch gekommen ist. Während Telefone die am häufigsten missbrauchte Technologie sind – laut Analyse der NNEDV in 87 % der Fälle – rücken auch so genannte smarte oder vernetzte Geräte im Zusammenhang mit technischem Missbrauch immer stärker in den Vordergrund, was auch von etwa einem Drittel der in Opferorganisationen tätigen Fachleute bestätigt wird.

Weil immer mehr Menschen IoT-Geräte nutzen, ist davon auszugehen, dass diese Zahl noch weiter steigen wird. Der ursprüngliche Zweck dieser Produkte bestand darin, das Leben einfacher und bequemer zu gestalten. Die Herstellung von IoT-Geräten ist ein schnell wachsender globaler Markt, auf dem es sowohl größere, gut etablierte Akteure als auch viele kleinere und neuere Unternehmen[1] gibt. Das Internet der Dinge wird durch mehrere sich gegenseitig stärkende Technologietrends befördert: immer schneller und kleiner werdende Prozessoren, größere Datenspeicher, sinkende Herstellungskosten und Konnektivität.

1 Internet Society. (2015). The Internet of Things: An Overview. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf or https://www.internetsociety.org/iot/

Werden immer mehr „smarte“ Geräte, d. h. vernetzte Geräte und Sicherheitssysteme, die mit WLAN-Netzwerken und Smartphones verbunden sind, als Mittel zur Gewalt in der Partnerschaft missbraucht

Aufgrund verschiedener Faktoren wie steigender Wettbewerb, rasante technische Entwicklungen und Komplexität des IoT werden weitreichende Risiken für die Sicherheit und den Datenschutz dabei zunehmend vernachlässigt[2]. Vor allem Smart Home-Geräte werden im Zusammenhang mit Gewalt in Paarbeziehungen missbraucht, um die Opfer zu kontrollieren, zu drangsalieren und zu schädigen. [Forscher des Projekts Gender + IoT am University College London[3] haben diese Schäden untersucht] [und in Zusammenarbeit mit Fachleuten vor Ort Abhilfemaßnahmen vorgeschlagen].

Die jüngste Bedarfsanalyse von NNEDV hat gezeigt, dass sich vor allem während der Pandemie ganz neue Taktiken zur Umsetzung Technik-basierten Missbrauchs entwickelt haben. Wir sehen mit Sorge, dass es auch nach Beendigung dieser Krise im Gesundheitswesen für die Täter, die diese Taktiken anwenden oder den missbräuchlichen Einsatz von Technologien in dieser Zeit ausgebaut haben, keinen Grund gibt, davon wieder abzusehen. Jüngste Untersuchungen[4] raten, dass die Mitarbeiter in Hilfsorganisationen nach allen Arten von technischem Missbrauch fragen sollten, einschließlich Stalkerware und Smart Home-Geräten. Es ist sehr wahrscheinlich, dass der Trend zum Technik-basierten Missbrauch, den die Mitarbeiter derzeit beobachten, anhalten wird. Um so wichtiger ist es, die Opfer weiterhin zu unterstützen und den missbräuchlichen Einsatz von Technologien zu verhindern.

2 Internet Society. (2015). The Internet of Things: An Overview. https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf or https://www.internetsociety.org/iot/

3 Tanczer, L., Neira, I. L., Parkin, S., Patel, T., & Danezis, G. (2018). The rise of the Internet of Things and implications for technology-facilitated abuse. University College London.

4 Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. Proceedings of the ACM on human-computer interaction, 1(CSCW), p.1-22.

Zusammenarbeit zwischen Kaspersky und seinen Partnern im Kampf gegen Stalkerware

Stalkerware ist nicht nur ein technisches, sondern ein gesamtgesellschaftliches Problem. In den vergangenen Jahren hat sich Kaspersky intensiv in die Debatte um Stalkerware eingebracht. Zusammen mit Akteuren aus dem öffentlichen und privaten Sektor arbeiten wir das Problem auf und entwickeln Lösungen. Wir beteiligen uns an der Zusammenstellung von Aufklärungsmaterialien und praktischen Hilfsmitteln, um gemeinnützige Organisationen, Unternehmen, Institutionen und Einzelpersonen im Kampf gegen Stalkerware zu unterstützen. Wir organisieren eigene Veranstaltungen und nehmen an Webinaren und Rundtischgesprächen mit Institutionen teil, um unsere Stimme zu erheben und zu Diskussionen beizutragen, die die Gesetzgebung von morgen prägen werden.

Kaspersky gehört zu den Mitbegründern und treibenden Kräften der Coalition Against Stalkerware (CAS), einer internationalen Arbeitsgruppe, die sich der Bekämpfung von Stalkerware und häuslicher Gewalt verschrieben hat. Die Koalition bringt unterschiedliche Organisationen zusammen, die mit Opfern und Tätern, digitalen Aktivisten und Anbietern von Cybersicherheitslösungen arbeiten. Diese einzigartige Plattform ermöglicht allen Beteiligten, Best Practices auszutauschen und Seite an Seite gegen Stalkerware vorzugehen.

Kaspersky ist auch einer der Partner des DeStalk-Projekts. Dieses von der Europäischen Kommission finanzierte Forschungsprojekt zielt darauf ab, eine Strategie zur Schulung und Unterstützung von Fachleuten zu entwickeln, die in Opferorganisationen und Täterprogrammen, Institutionen und Kommunalverwaltungen bzw. anderen relevanten Gruppen arbeiten. Das Konsortium plant die Verbesserung und Erprobung bestehender Instrumente für Menschen, die in diesem Bereich praktisch tätig sind, und arbeitet im Rahmen eines Pilotprojekts derzeit an einer regionalen Aufklärungskampagne in Italien.

Seit 2021 arbeiten wir mit INTERPOL und zwei renommierten gemeinnützigen Organisationen in den USA und Australien an einem Projekt, um jedem Mitarbeiter der Strafverfolgungsbehörden die Teilnahmen an zwei Online-Schulungen zu ermöglichen. Diese Kurse wurden bislang von mehr als 210 Teilnehmern aus der ganzen Welt besucht.

Ende 2021 nahm Kaspersky auch an einer vom Europarat organisierten Veranstaltung zum Thema „Bekämpfung von Gewalt gegen Frauen im digitalen Zeitalter – Umsetzung der Istanbul-Konvention" teil. Diese Veranstaltung bot Gelegenheit, die Empfehlungen der Expertengruppe zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (GREVIO) zu diskutieren.

TinyCheck: Unterstützungstool für Opfer häuslicher Gewalt

Eine weitere wichtige Initiative, an der Kaspersky beteiligt ist, betrifft das Tool TinyCheck. Dabei handelt es sich um ein kostenloses Open-Source-Tool, das von Kaspersky entwickelt und supported wird. TinyCheck wurde ursprünglich entwickelt, um gemeinnützige Organisationen beim Schutz der Opfern häuslicher Gewalt und ihrer Privatsphäre zu unterstützen. Ohne Installation ermöglicht es die einfache und schnelle Erkennung von Stalkerware auf den Geräten der Opfer und auf jedem Betriebssystem, ohne dass der Täter etwas davon mitbekommt. Sicherheitslösungen können zwar auch auf Stalkerware prüfen und davor warnen, müssen aber auf dem Gerät installiert werden, was dazu führen kann, dass auch der Täter gewarnt wird. Mit Entwicklungen wie dem TinyCheck-Tool soll sichergestellt werden, dass Überlebende ihre Geräte ohne Angst vor Bespitzelung nutzen können.

TinyCheck wurde ursprünglich entwickelt, um gemeinnützige Organisationen beim Schutz der Opfern häuslicher Gewalt und ihrer Privatsphäre zu unterstützen

Bei TinyCheck muss kein Programm auf dem Gerät installiert werden und die Ergebnisse der Prüfung werden weder auf dem potenziell infizierten Gerät angezeigt noch an dieses übertragen. Außerdem können Opfer mit TinyCheck jedes beliebige Gerät überprüfen, ganz gleich, ob es unter IOS, Android oder einem anderen Betriebssystem läuft. Damit werden gleich zwei der Hauptprobleme im Zusammenhang mit der Bekämpfung von Stalkerware gelöst. Das Tool läuft auf einem Raspberry Pi mit einer ganz normalen WLAN-Verbindung. TinyCheck analysiert schnell den ausgehenden Datenverkehr eines mobilen Geräts und sucht nach so genannten Gefährdungsindikatoren (Indicators of Compromise, IOCs), z. B. Interaktionen mit bekannten schädlichen Quellen wie Stalkerware-Servern. Aktuell arbeitet das Tool mit IoCs, die nicht nur von Kaspersky-Mitarbeitern, sondern auch aus den Repositorys unabhängiger Sicherheitsforscher stammen (besonderer Dank gebührt hierbei Etienne Maynier, auch bekannt als Tek, von Echap und Cian Heasley). Wir hoffen, diese Zusammenarbeit noch lange fortsetzen zu können, damit die IoCs auf dem neuesten Stand bleiben.

Allerdings hat auch TinyCheck seine Grenzen. Folgendes sollte man daher bei der Nutzung des Tools im Hinterkopf behalten: IoCs bieten nicht den umfassenden Echtzeit-Schutz gegen Stalkerware-Apps wie eine IT-Sicherheitslösung. Auch wenn TinyCheck keine Stalkerware findet, ist das noch keine Garantie, dass auch keine installiert wurde.

Eine Reihe von gemeinnützigen Organisationen aus dem Bereich der häuslichen Gewalt hat TinyCheck 2021 getestet und entsprechendes Feedback gegeben, um den Service zu verbessern. In einigen Ländern haben auch Polizei- und Justizbehörden ihr Interesse an dem Tool bekundet.

Positive Entwicklungen 2021 in der Gesetzgebung und bei zentralen Institutionen

Weltweit waren 2021 einige positive Entwicklungen im Kampf gegen Stalkerware vonseiten der Gesetzgeber und Institutionen zu verzeichnen. Im Mai 2021 verabschiedete das japanische Parlament eine überarbeitete Version seines bis dahin geltenden Anti-Stalker-Gesetzes. Die neue Fassung verbietet unter anderem die Beschaffung von Standortinformationen von Smartphones durch Apps ohne die ausdrückliche Zustimmung der Besitzer.

Im August 2021 untersagte die Federal Trade Commission in den USA einem App-Hersteller die Verbreitung von Stalkerware. Es war das erste Verbot dieser Art.

Am 17. August 2021 hat der Deutsche Bundestag das „Gesetz zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings“ verabschiedet. Das neue Gesetz trat am 1. Oktober 2021 in Kraft und nimmt nun auch Cyberstalking in den Katalog der Straftaten auf. Grund für diesen Wandel ist der fortschreitende technologische Fortschritt und die damit verbundene Zunahme von Cyberstalking, insbesondere über Stalking-Apps oder Stalkerware. Eine wesentliche Neuerung des Gesetzes besteht darin, dass ein Fall dann als schwerwiegend eingestuft wird, wenn der Täter „bei der Tathandlung ein Computerprogramm einsetzt, dessen Zweck das digitale Ausspähen anderer Personen ist“.

Der Europarat hat sich 2021 sehr intensiv mit diesem Thema befasst. In ihrem ersten Bewertungsbericht zur „digitalen Dimension“ der Gewalt gegen Frauen umreißt die Expertengruppe des Europarats zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (GREVIO) die Probleme sowohl der geschlechtsspezifischen Gewalt gegen Frauen, die im Internet stattfinde, als auch der Technologie-gestützten Angriffe auf Frauen, wie z. B. durch ganz legal erworbene Ortungsgeräte, die es den Tätern ermöglichen, ihren Opfern nachzustellen. Kurze Zeit später, im Dezember 2021, folgte ein Initiativbericht zur geschlechtsspezifischen Cybergewalt, der vom Europäischen Parlament angenommen wurde. Im Bericht wird (i) eine gemeinsame Definition von geschlechtsspezifischer Cybergewalt und (ii) der Aufbau von Kapazitäten für die Beteiligten gefordert. Stalkerware wird weiterhin als eines der wichtigsten Mittel zur Ausübung von Cybergewalt hervorgehoben und „die Vorstellung zurückgewiesen, dass Stalkerware-Programme als Anwendungen zur Kindersicherung durch ihre Eltern angesehen werden können“. In Anlehnung an die allgemeinen Empfehlungen des Europarats ist dieser Bericht, wenn nicht bindend, so doch ein

weiteres positives offizielles Dokument, das ein Schlaglicht auf das Problem der Stalkerware wirft und die europäischen Staaten drängt, ihre Gesetzgebung und Maßnahmen zur Bekämpfung des Problems anzupassen. Schließlich hat die Europäische Kommission am 8. März 2022 einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt veröffentlicht. In diesem Dokument wird die Cybergewalt thematisiert, wobei zwei Artikel dem Cyberstalking (Artikel 8) und der Cyberbelästigung (Artikel 9) gewidmet sind, die unter Strafe gestellt werden sollen.

Möchten Sie Gewissheit, ob auch Sie Opfer von Stalkerware sind? Hier einige Tipps

Wenn Sie Hilfe brauchen, wenden Sie sich an eine örtliche Hilfsorganisation. Eine in Ihrer Nähe finden Sie auf der Website der Koalition gegen Stalkerware.

Auch wenn Sie kein Opfer von Stalkerware sind, finden Sie hier eine Reihe von nützlichen Tipps, wie Sie sich besser schützen können:

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

Opfer von Stalkerware befinden sich häufig schon in einer Spirale der Gewalt, auch physischer. Der Täter könnte eine Benachrichtigung erhalten, wenn sein Opfer einen Gerätescan durchführt oder die Stalkerware-App entfernt. Das wiederum kann zu einer Eskalation der Situation und zu weiterem aggressivem Verhalten führen. Deshalb sollten Sie unbedingt vorsichtig vorgehen, wenn Sie vermuten, dass Sie ins Visier einer Stalkerware geraten sind.

- 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 die **folgenden 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. Bei all dem ist zu bedenken, dass die oben genannten Anzeichen nur mögliche Symptome einer installierten Stalkerware darstellen und noch kein Beweis sind.
- **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 aus dem Ruder laufen. Außerdem riskieren Sie, dass wichtige Daten oder Beweise gelöscht werden, die bei der Strafverfolgung hilfreich sein könnten.

Für weitere Informationen über unsere Aktivitäten im Bereich Stalkerware oder andere Anfragen, schreiben Sie uns bitte 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/

COALITION AGAINST STALKERWARE

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

kaspersky