Der **Stalkerware** Report 2019

COALITION AGAINST STALKERWARE

kaspersky

COALITION AGAINST STALKERWARE

Über die Coalition Against Stalkerware

Eine neue, globale Arbeitsgruppe bündelt Wissen über Opferhilfe und Cybersicherheit, um Betroffenen zu helfen.

Zehn Organisationen – Avira, Electronic Frontier Foundation, European Network for the Work with Perpetrators of Domestic Violence, G DATA CyberDefense, Kaspersky, Malwarebytes, National Network to End Domestic Violence, NortonLifeLock, Operation Safe Escape und WEISSER RING – haben im November 2019 eine globale Initiative namens „Coalition Against Stalkerware" (Koalition gegen Stalkerware) gestartet, um Nutzer besser gegen Stalkerware zu schützen.

Die Koalition wurde gegründet, um den Austausch zwischen der IT Sicherheitsgemeinschaft und den Organisationen, die gegen häusliche Gewalt kämpfen, zu erleichtern. Mit dem Onlineportal www.stopstalkerware.org will die Koalition Opfern helfen, Wissenstransfer zwischen Mitgliedern ermöglichen, Best Practices zur Entwicklung ethischer Softwareentwicklung teilen und die Öffentlichkeit über die Gefahren von Stalkerware aufklären.

Das Projekt strebt als nicht-kommerzielle Initiative an, Stakeholder aus gemeinnützigen Einrichtungen, aus der Industrie und aus anderen Bereichen wie Polizeibehörden unter einem Dach zu vereinigen. Aufgrund der hohen gesellschaftlichen Relevanz des Themas für Nutzer auf der ganzen Welt und der beständigen Fortentwicklung weiterer Varianten von Stalkerware, steht die Coalition Against Stalkerware neuen Partnern offen und ruft zur Kooperation auf.

Für mehr Informationen www.stopstalkerware.org

Gründungsmitglieder über die Wichtigkeit der Zusammenarbeit gegen Stalkerware :

COALITION AGAINST STALKERWARE

Alexander Vukcevic
Director Protection Labs
Avira

Monitoring Software hat sich in den letzten Jahren rapide weiterentwickelt, tiefgreifende Überwachungsfunktionen wurden hinzugefügt und der Sinn der Ortungsfunktionen hat sich grundlegend geändert. Der ständige Anstieg der Nutzung mobiler Geräte kombiniert mit einem Mangel an gesetzlicher Einschränkung gibt Leuten Zugang zu Tools zur Überwachung des Ehepartners, Familienmitglieds oder Freundes. Avira stellt fest, dass dies eine neue Bedrohungskategorie ist und lädt IT Sicherheitsfirmen sowie Organisationen zur Bekämpfung häuslicher Gewalt ein, sich zusammenzuschließen, um Informationen auszutauschen und zusammen zu arbeiten, um diese Verletzungen der Privatsphäre zu beenden.

Eva Galperin
Director of Cybersecurity
Electronic Frontier Foundation

Stalkerware, die zum Ausspionieren von Handys und PCs im Bereich der häuslichen Gewalt oder der Belästigung eingesetzt wird, ist ein sehr großes Problem. Oft geht sie Hand in Hand mit anderen Formen von Missbrauch, bis hin zu und inklusive körperlicher Gewalt. Die Allgegenwart von Stalkerware ist ein komplexes Problem, und wir brauchen Unterstützer aus der ganzen Gesellschaft, um sie effektiv zu bekämpfen

Anna McKenzie
Communications Manager
European Network for the Work with Perpetrators of Domestic Violence

Studien haben gezeigt, dass 70% aller von Cyberstalking betroffenen Frauen auch mindestens eine Form physischer und/ oder sexualisierter Gewalt durch ihre Intimpartner/Partner erfahren haben. Wir müssen Täter für ihre Gewalt zur Rechenschaft ziehen und sie davon abhalten die Handys ihrer Partnerinnen zu deren Überwachung zu nutzen. Die Coalition Against Stalkerware gibt uns die Chance unser Wissen über gender-basierte Gewalt und Täterarbeit an IT Sicherheitsfirmen heranzutragen, damit wir gemeinsam an einer Lösung gegen digitale Gewalt an Frauen und Mädchen arbeiten können.

Hauke Gierow
Pressesprecher
G DATA CyberDefense

Das Aufspielen von Spyware auf das Smartphone des Partners ist eine eklatante Verletzung von Menschenrechten. Wir sind entschlossen, unsere Nutzer vor solchen Gefahren zu schützen. G DATA Cyber Defense verpflichtet sich dazu, Nutzer besser über potenzielle Risiken aufzuklären und mit Opferhilfen zusammenzuarbeiten, um auch nicht-technische Probleme, die mit Stalkerware zusammenhängen, anzugehen.

Vyacheslav Zakorzhevsky
Head of Anti-Malware Research
Kaspersky

Um dieses Problem wirkungsvoll zu bekämpfen, ist es wichtig, dass Cybersicherheitsunternehmen, Hilfsorganisationen sowie Interessensgruppen zusammenzuarbeiten. Als IT Sicherheitsindustrie leisten wir dazu einen Beitrag, indem wir kontinuierlich unsere Erkennung von Stalkerware verbessern und Nutzer über diese Gefahr für ihre Privatsphäre aufklären. Die Hilfs- und Interessensgruppen arbeiten ihrerseits direkt mit Opfern häuslicher Gewalt, kennen die sensiblen Punkte und können uns dadurch in unserer Arbeit beraten. Durch dieses Zusammenspiel mittels technischer Expertise und Wissenstransfer, Seite an Seite, unterstützen wir Opfer und Überlebende.

David Ruiz
Online Privacy Writer
Malwarebytes Labs

Seit Jahren erkennt und warnt Malwarebytes Internetnutzer vor potenziell gefährlichen Funktionen von Stalkerware. Stalkerware stellt eine invasive Bedrohung dar, die Menschen ihrer Erwartung und ihrer Rechte in Bezug auf Privatsphäre berauben kann. Genau wie den Missbrauch, dem sie die Türen öffnen kann, vermehrt sich Stalkerware unbeobachtet von der Öffentlichkeit und lässt ihre Opfer isoliert, ungehört und hilflos zurück. Die Gründung der Koalition gegen Stalkerware und der gemeinsame Kampf ist der nächste erforderliche Schritt dafür, diese digitale Bedrohung zu stoppen – ein gemeinsamer Ansatz, der durch das Versprechen gesteuert wird, Technologien für jeden und überall sicher zu ermöglichen

Erica Olsen
Director of the Safety Net Project
National Network to End Domestic Violence

Wenn diese Software für den Einsatz im vollständigen Stealth-Modus, also im unsichtbaren Modus, ohne ständige Benachrichtigung des Gerätebesitzers entwickelt wurde, gibt sie Menschen mit böswilligen Absichten und Stalkern ein mächtiges Werkzeug für Belästigungen, Überwachung, Stalking und Missbrauch an die Hand. Diese Art von Missbrauch kann bedrohlich sowie traumatisierend sein und wirft erhebliche Sorge um Sicherheit und Schutz der Privatsphäre auf. Die Gründung dieser Koalition ist daher ein großartiger Schritt in die richtige Richtung, um dieses Problem anzugehen.

Kevin Roundy
Research Director
NortonLifeLock

Bei NortonLifeLock arbeiten unsere Forschungsexperten seit über zwölf Jahren daran, Stalkerware aus den Händen der Tätern zu nehmen und potentiellen sowie realen Opfern Tools für den Selbstschutz zu geben, damit sich diese selber vor Belästigung, Gewalt und Angriffen schützen können. Wir sind stolz, ein Gründungsmitglied der Koalition gegen Stalkerware zu sein, um unsere Expertise zu teilen und Kräfte im Kampf gegen Missbrauch zu bündeln

Wilson "Chilly" Hightower
Head of Intake
Operation Safe Escape

Das heimtückische Vorgehen von Stalkerware dient einzig dem Zweck, zu verletzen, zu schaden und eine konstantes Gefühl von Angst und Schrecken bei vielen unserer Mandanten einzuflößen. Es ist eine aktive und existenzielle Bedrohung der Sicherheit und Privatsphäre aller Menschen. Da unser Leben immer mehr mit Technologie verflochten und von ihr abhängig ist, wächst die Gefahr beständig, die Stalkerware bereits darstellt. Mehr denn je ist es wichtig, dass wir dieser Gefahr zuvorkommen und die Macht den potenziellen Tätern und Stalkern entziehen. Operation Safe Escape ist sehr stolz, Teil dieser gemeinsamen Anstrengung zu sein, um unseren Mandanten und Menschen überall wieder ein Gefühl von Sicherheit und Privatsphäre zurückzugeben.

Horst Hinger
Stv. Bundesgeschäftsführer
WEISSER RING

Wir als gemeinnützige Organisationen wissen, dass die technischen Möglichkeiten Tätern den Zugang zu privaten Daten ihrer Opfer erleichtern. Die Betroffenen suchen selten Hilfe, weil sie sich schämen. Für den WEISSEN RING stellt Stalking ein zunehmend wichtigeres Thema in der Opferarbeit dar. 2018 etwa haben wir 1019 Fälle von Stalking betreut, das waren rund drei Prozent mehr als im Vorjahr. Laut Polizeilicher Kriminalstatistik sind 2018 insgesamt fast 19.000 Fälle von Stalking bei den Polizeibehörden registriert worden. Im Vorjahr waren es noch 500 weniger – eine deutliche Steigerung. Daher haben wir gemeinsam mit der WEISSER RING Stiftung die NO STALK App entwickelt, mit der wir Betroffenen ein wirksames digitales Instrument an die Hand geben, mit dem sie Stalkinghandlungen beweissicher dokumentieren können. Wir wünschen uns, dass die Zahl der Stalking-Fälle mit diesem Hilfsmittel auf Dauer signifikant gesenkt werden kann. Aufgrund der Verbesserung der Beweislage soll die Anzeigenhäufigkeit gesteigert werden. Außerdem sollen Menschen dafür sensibilisiert werden, dass Stalking eine Straftat ist und für die Betroffenen eine nachhaltige Belastung darstellt. Die App steht seit Mai kostenlos in den Stores von Apple und Android zum Download zur Verfügung.

Hauptergebnisse, aktualisiert April 2020

Weltweit stieg die Zahl der Benutzer mit auf ihren Geräten installierter Stalkerware innerhalb nur eines Jahres um 67%

Dieser Abschnitt enthält eine Aktualisierung mit Zahlen für das gesamte Jahr 2019 im Vergleich zu 2018. Aufgrund des Veröffentlichungsdatums enthält der verbleibende Teil des Berichts Daten von Januar bis August 2019.

- Ende 2019 stieg die Zahl unserer Mobilfunknutzer, die mit Stalkerware konfrontiert waren, um 67%: Im Jahr 2018 wurden 40.386 Einzelbenutzer angegriffen, im Jahr 2019 stieg diese Zahl auf 67.500
- Die Zahl der Angriffe in der zweiten Hälfte des Jahres 2019 hat sich im Vergleich zur ersten Hälfte verdoppelt. Im Januar 2019 wurden 4483 Kaspersky-Mobilfunknutzer angegriffen; im September 2019 stieg diese Zahl auf 9546 und im Dezember 2019 erreichte diese Zahl 11.052 angegriffene Nutzer
- Russland, Brasilien, Indien und die USA sind mit 23,4 %, 9,4 %, 9 % und 5,6 % der betroffenen Nutzer im Jahr 2019 die weltweit bedeutendsten Regionen für Stalkerware
- Wenn es um Europa geht, sind Deutschland (3,1%), Italien (2,4%) und Frankreich (1,8%) die drei am stärksten betroffenen Länder

Stalkerware dient dazu, dem Täter die Überwachung des Opfers ohne dessen Zustimmung zu ermöglichen

Einleitung und Methodik

Vor sechs Monaten haben wir einen speziellen Alarm entwickelt, der Nutzer vor kommerziellen Spyware-Produkten (Stalkerware) warnt, die auf ihren Handys installiert sind. Dieser Bericht analysiert den Einsatz von Stalkerware und die Anzahl der Nutzer, die in den ersten acht Monaten des Jahres 2019 von dieser Art Software betroffen waren.

Die Technologie zur Überwachung von Verbrauchern hat sich in den letzten Jahren rapide entwickelt und der zentrale Fokus von Überwachungsaktivitäten hat einen dramatischen Wandel erlebt. Die schnelle Entwicklung des Internets und die darauffolgende rasante Verbreitung mobiler Geräte hat einer Art von Überwachungssoftware, der sogenannten Stalkerware, großen Aufschwung gebracht. Diese Software ermöglicht es Nutzern, andere Personen auszuspionieren und Daten wie deren Nachrichten, Anrufinformationen und GPS-Positionen ohne deren Wissen zu überwachen. Ihr Einsatz dient häufig dazu, die Privatsphäre von aktuellen oder ehemaligen Partnern und sogar von Fremden zu verletzen. Dabei genügt es, auf dem Smartphone oder Tablet des Opfers manuell eine App zu installieren. Nach der Installation erhält der Stalker Zugriff auf eine Vielzahl persönlicher Daten, selbst wenn er sich nicht in der Nähe des Opfers befindet. Diese Art der Software unterscheidet sich wesentlich von Kinderschutzsoftware. Während Apps zur Kindersicherung darauf abzielen, den Zugriff auf gefährliche und ungeeignete Inhalte einzuschränken, und Nutzer stets über Anfragen in Kenntnis setzt, dient Stalkerware dazu, dem Täter die Überwachung des Opfers ohne dessen Zustimmung zu ermöglichen.

Der Großteil von Stalkerware-Apps ist nicht in den offiziellen App Stores wie Google Play erhältlich, und ihre Installation erfordert Zugriff auf eine spezielle Website sowie den Zugang zum Gerät des Opfers. Ein Individuum mit schlechten Absichten kann eine solche App dazu verwenden, um die E-Mails von Angestellten zu überwachen, den Standort von Kindern nachzuverfolgen oder einen Partner auszuspionieren. Eine solche Nutzung führt häufig zu Belästigung, Überwachung ohne Zustimmung, Stalking und sogar häuslicher Gewalt. Tatsache ist, dass die aktuellen Rechtsvorschriften zum Einsatz von Stalkerware noch nicht stark genug sind, um Täter vom Missbrauch und von der Ausnutzung anderer Personen abzuhalten.

Die Daten in diesem Bericht stammen von Bedrohungsstatistiken, die von Kaspersky Security Network gesammelt wurden, um festzustellen, wie häufig Benutzer in den ersten acht Monaten von 2019 im Vergleich zum Vorjahr von Stalkerware bedroht waren und wie viele Nutzer betroffen waren. Kaspersky Security Network (KSN) ist eine Infrastruktur, die der Verarbeitung von Datenströmen dient, die für die Cybersicherheit relevant sind. Diese Datenströme werden von Millionen von freiwilligen Teilnehmenden auf der ganzen Welt an KSN übermittelt. In diesem Bericht haben wir analysiert, warum Stalkerware verwendet wird und wo sie am häufigsten zum Einsatz kommt.

Zentrale Erkenntnisse

Weltweit ist die Anzahl der Nutzer, die von Stalkerware betroffen sind, um 35% innerhalb nur eines Jahres gestiegen

- Zwischen Januar und August 2019 gab es weltweit mehr als 518.223 Fälle, in denen unsere Schutztechnologien entweder Stalkerware auf einem Benutzergerät feststellten oder den Versuch der Installation einer solchen Software registrierten: Das ist ein Anstieg von 373 % im Vergleich zum gleichen Zeitraum in 2018.
- In den ersten acht Monaten des Jahres 2019 stießen 37.532 Nutzer mindestens einmal auf Stalkerware. Das ist ein Anstieg von 35 % im Vergleich zum gleichen Zeitraum in 2018, in dem 27.798 Nutzer betroffen waren.
- Die Anzahl der Nutzer, die zum Ziel eines Spyware-Direktangriffs wurden, der als "Trojan-Spy" identifiziert wurde, erreichte 26.620 in den ersten acht Monaten von 2019, was unter der Anzahl der Nutzer liegt, die auf Stalkerware stießen.
- Die Russische Föderation ist mit 25,6 % aller potenziell betroffenen Benutzer in den ersten acht Monaten von 2019 global nach wie vor die Region mit dem häufigsten Auftreten von Stalkerware. An zweiter Stelle steht Indien mit 10,6 % der betroffenen Benutzer, gefolgt von Brasilien an dritter Stelle (10,4 %). Die USA stehen mit 7,1 % auf Platz vier.
- In Europa belegen Deutschland, Italien und UK jeweils die drei obersten Plätze.

Anstieg des Stalkerware-Problems

In diesem Jahr wurde ein starker Anstieg der Anzahl der Funde von Stalkerware auf Android-Geräten verzeichnet, die von Kaspersky-Produkten geschützt sind. Ein möglicher Grund für den Anstieg ist die Optimierung der Erkennung von Stalkerware-Software in Cybersicherheitslösungen. Im April veröffentlichte Kaspersky eine Funktion in der Android-Sicherheitsapp – Privacy Alert –, die Nutzer alarmiert, wenn eine Software auf ihrem Gerät für Stalking verwendet werden kann. Seitdem hat die Anzahl der Erkennungen konstant zugenommen. So waren zum Beispiel 4.315 Benutzer im März 2019 von Stalkerware betroffen, verglichen mit 7.075 im April – ein Anstieg von 64 % in nur einem Monat. Diese Zahl stieg im August auf 9.251, das sind 94 % mehr als im Monat der Veröffentlichung der Funktionalität.

Diese frei verkäuflichen Programme zur Überwachung von Verbrauchern sind sehr gefragt und werden häufig dazu verwendet, um Mitarbeiter, Familienmitglieder und Partner auszuspionieren. Für eine geringe Gebühr, manchmal wenig mehr als 6 € im Monat, bleiben diese Apps verborgen auf dem Gerät und informieren die Betreiber über Aktivitäten wie Standort des Besitzers, Browser-Verlauf, Textnachrichten, Chats in sozialen Netzwerken und mehr. Einige sind sogar in der Lage, Video- und Sprachaufnahmen zu machen.

Um das Ausmaß des Stalkerware-Problems besser zu verstehen, hat Kaspersky die Aktivitäten der letzten acht Monate analysiert. Zwischen Januar und August 2019 stießen 37.533 Benutzer auf ihren Geräten mindestens einmal auf Stalkerware. Das ist ein Anstieg von 35 % im Vergleich zum gleichen Zeitraum in 2018, in dem 27.798 Benutzer betroffen waren. Insgesamt gab es zwischen Januar und August 2019 mehr als 518.223 Fälle, in denen Kaspersky-Produkte entweder Stalkerware auf einem Benutzergerät feststellten oder den Versuch der Installation einer solchen Software registrierten: Das ist ein dramatischer Anstieg von 373 % im Vergleich zum gleichen Zeitraum in 2018.

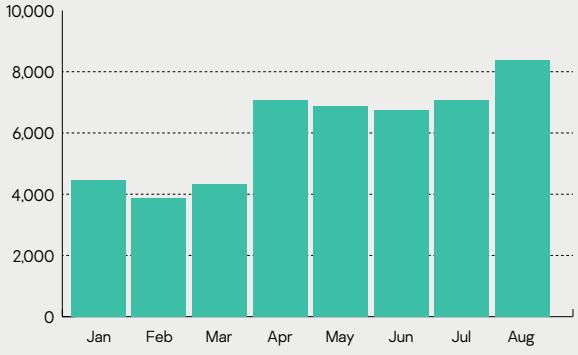


Abb.1 Anzahl der Nutzer, die Jan-Aug 2019 auf Stalkerware stießen

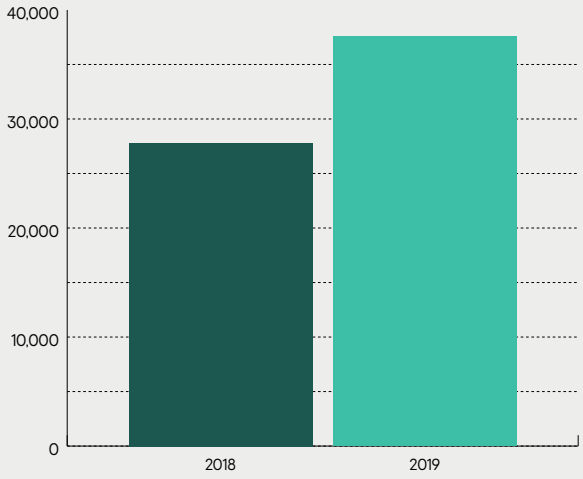


Abb.2 Von Stalkerware betroffene Nutzer, 2018 vgl. mit 2019

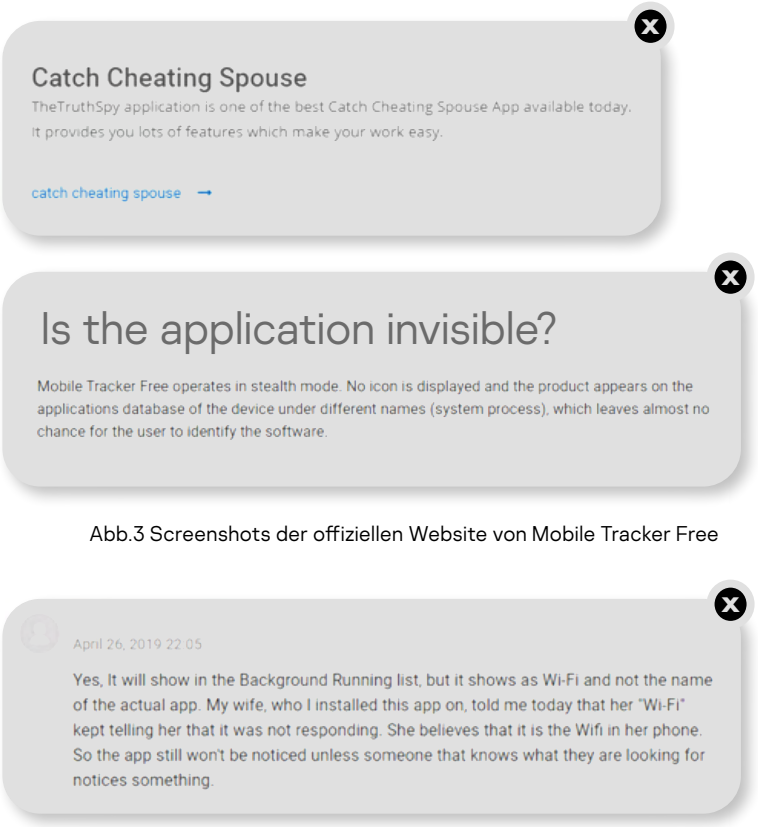


Abb.3 Screenshots der offiziellen Website von Mobile Tracker Free

Abb.4 Screenshot der offiziellen Website von TheTruthSpy

Dritte können auf die Fotos auf dem Handy des Opfers und auf die Kamera in Echtzeit zugreifen und den Browser-Verlauf, die Dateien auf dem Gerät, den Kalender und die Kontaktliste abrufen

Beispiele für Software, die für Stalking verwendet wird

Die am weitesten verbreitete Stalkerware-Software-Reihe von 2019 wurde als Monitor.AndroidOS.MobileTracker.a identifiziert. 6.559 individuelle Benutzer waren davon betroffen. An zweiter Stelle steht Monitor.AndroidOS.Cerberus.a – diese Software wurde auf den Geräten von 4.370 Benutzern gefunden, dicht gefolgt von Monitor.AndroidOS.Nidb.a (4.047) auf Platz drei.

Im Vergleich zu den Ergebnissen aus 2018 gibt es eine Abweichung bei den obersten zwei Plätzen. Im Jahr 2018 wurden auf den meisten Geräten Monitor.AndroidOS.Nidb.a und Monitor.AndroidOS.PhoneSpy.b gefunden – mit jeweils 4.427 und 2.819 Benutzern. Monitor.AndroidOS.XoloSale.a war mit 1.946 Benutzern die dritthäufigste Stalkerware.

In unserem internen Klassifizierungssystem wird ein Eintrag von Monitor.AndroidOS.MobileTracker.a verwendet, um "Mobile Tracker Free"-Apps zu identifizieren, die als Tool positioniert sind, mit dem sich die Aktivitäten von Kindern oder Angestellten überwachen lassen.

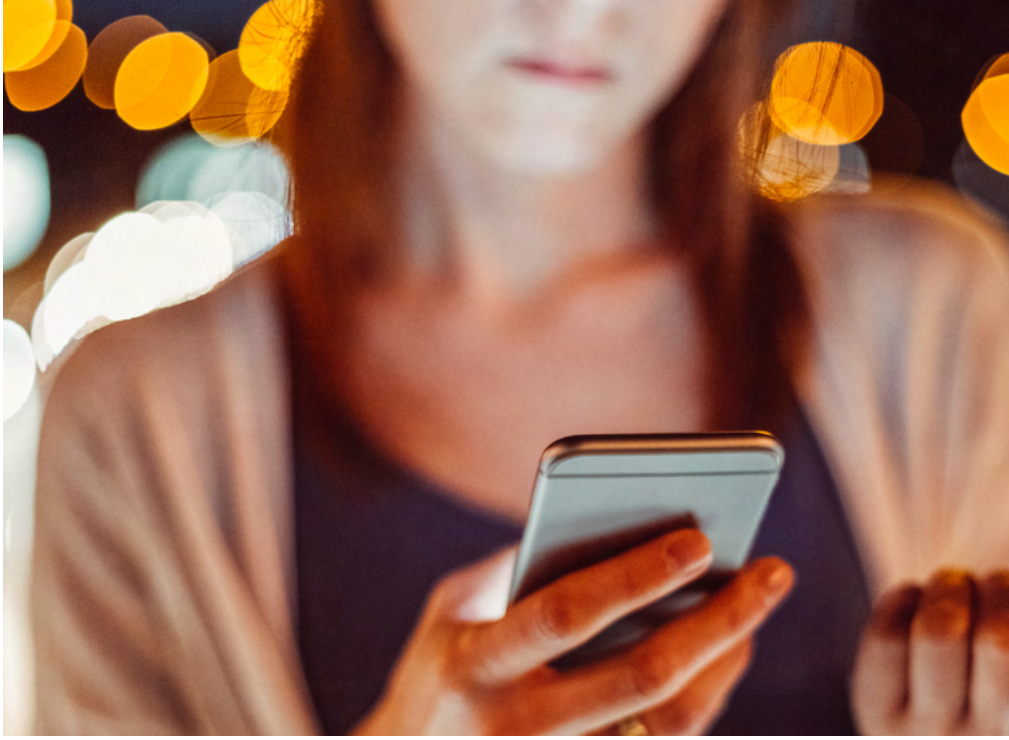
Genau genommen erlaubt die App die Überwachung der Standorte von Nutzern, ihrer Unterhaltungen über

SMS und Messenger-Apps (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram usw.) sowie ihrer Anrufe. Außerdem können Dritte auf die Fotos auf dem Handy des Opfers und auf die Kamera in Echtzeit zugreifen und den Browser-Verlauf, die Dateien auf dem Gerät, den Kalender und die Kontaktliste abrufen. Darüber hinaus ermöglicht die App die Steuerung des Geräts per Fernsteuerung. Hinzu kommt die Möglichkeit, die App als Systemanwendung zu tarnen und verborgen im Hintergrund auszuführen.

Die nächste App, Cerberus (Monitor.AndroidOS.Cerberus.a), ist als App für den Diebstahlschutz positioniert. Allerdings erlaubt sie einem Stalker, verborgen im Hintergrund zu agieren und ihre eigene Deinstallation zu verhindern. Sie macht es unter anderem möglich, den Standort des Gerätes zu verfolgen, Bilder mit der Kamera sowie Screenshots aufzunehmen und Tonaufnahmen über das Mikrofon zu machen.

Auf Platz drei steht mit Monitor.AndroidOS.Nidb.a eine Gruppe ähnlicher Apps: iSpyoo/TheTruthSpy/Copy9. Anders als die bereits besprochenen zwei Apps werben einige Vertreter dieser Gruppe öffentlich mit ihren Möglichkeiten zum Ausspionieren eines Partners und verfassen sogar Artikel zu diesem Thema.

Das Angebot an Funktionen ist für solche Programme recht standardmäßig, aber dennoch erschreckend: Website-Tracing, Abfangen von Unterhaltungen über SMS und Messenger-Apps, Anrufverfolgung und Browser-Verlauf. Wie bei vielen ähnlichen Apps werden hier zur Ausführung bestimmter Funktionen Superuser-Rechte (Administratorrechte) benötigt. Die Apps können verborgen im Hintergrund ausgeführt werden und tarnen sich in der Liste installierter Apps hinter Namen, die Systemprozesse imitieren.



Wo findet man Stalkerware?

Die breite Palette an Regionen, in denen die meisten Angriffe erfolgen, weist darauf hin, dass ein globaler Markt für legale Spyware und Stalkerware-Software existiert. Die 10 Länder mit dem größten Anteil an Nutzern, die von Stalkerware betroffen sind, unterscheiden sich geopolitisch und liegen nicht nahe beieinander.

1. Russian Federation – **25.61%**
2. India – **10.56%**
3. Brazil – **10.39%**
4. United States – **7.11%**
5. Germany – **3.55%**
6. Italy – **2.65%**
7. Mexico – **2.10%**
8. United Kingdom – **1.95%**
9. France – **1.76%**
10. Iran – **1.68%**

Other – **32.65%**

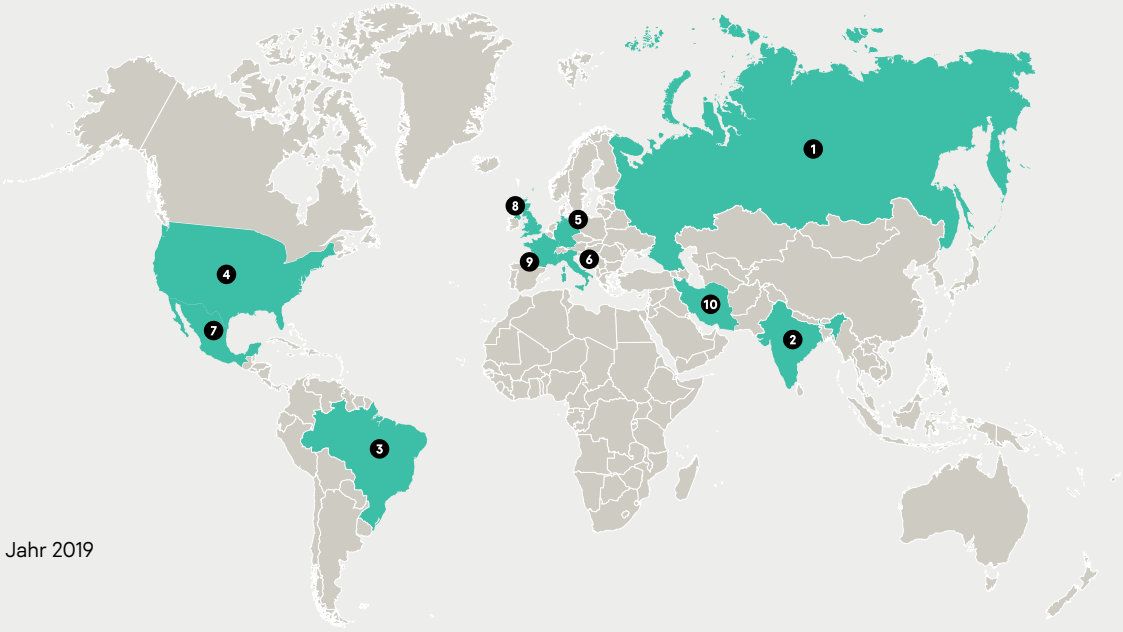


Abb. 5 Geografie der Benutzer, die im Jahr 2019 von Stalkerware betroffen sind

Eine Umfrage hat gezeigt, dass 85 % der Hilfsberatungsstellen angaben, Opfern geholfen zu haben, bei denen die Täter sie mittels GPS verfolgt hatten

Nach den Ergebnissen von Kaspersky ist Russland die Region mit der höchsten Stalkerware-Aktivität. Entsprechende Aktivitäten dauern auch in Indien hartnäckig an: Das Land steht mit 10,56 % der betroffenen Benutzer auf Platz zwei der Regionen mit den meisten Vorfällen in Bezug auf Stalkerware zwischen Januar und August.

Für Brasilien ergeben sich 10,39 % aller angegriffenen Benutzer in 2019, während die USA jetzt auf Platz vier stehen (7,11 %). Interessensgruppen in den USA klären über die Gefahren von Stalkerware auf und führen aufschlussreiche Erhebungen durch. Eine Befragung von 72 Unterkünften für Opfer häuslicher Gewalt durch den öffentlichen Hörfunksender "National Public Radio" ergab, dass 85 % des Personals angab, Opfern geholfen zu haben, bei denen die Täter sie mittels GPS verfolgt hatten. Fast drei Viertel (71 %) aller Täter häuslicher Gewalt verfolgen die Computeraktivitäten des Opfers, während 54 % deren Handys mittels Stalkerware überwachen. Deutschland belegt in der Statistik dabei den fünften Platz im Jahr 2019 mit 3,55 % an Nutzern, die von Stalkerware betroffen sind.

Stalkerware in der Landschaft der Cyberbedrohungen

Über 37.000 Nutzer wurden 2019 zur Zielscheibe von Stalkerware, während es das Jahr zuvor knapp 27.000 waren

Ein Vergleich von Stalkerware und Spyware mit anderen Angriffen auf mobile Nutzer (wie Adware, Riskware und Malware) ergibt, dass erstere einen großen Anteil an den weniger zielgerichteten "not-a-virus"-Programmen haben. In den ersten acht Monaten von 2019 konnte Kaspersky feststellen, dass 2.350.862 Benutzer mit möglicherweise unerwünschten Bedrohungen konfrontiert wurden, von denen nur 1,60 % mit Stalkerware in Zusammenhang standen. Allerdings muss beachtet werden, dass Stalkerware anders als die Mehrzahl der auf die Masse zugeschnittenen potenziellen Bedrohungen (wie Adware) einen einzelnen Stalker erfordert, der die Software betreibt. Jedes Ziel wird gestalkt und wurde bewusst ausgewählt. Während die Zahlen also niedriger sind, richtet sich Stalkerware gezielt gegen ein bestimmtes Opfer und ist mit einem bestürzenden Ausmaß an Missbrauch verbunden.

Um bei der Einschätzung der Entwicklungsdynamik von Stalkerware das Gesamtbild zu berücksichtigen, haben wir Stalkerware mit groß angelegter, illegaler Überwachungs-Malware für PC verglichen, die wir als "Trojan Spy" identifizieren. Die Ergebnisse haben gezeigt, dass die Verbreitung illegaler Spyware abnimmt, während bei Stalkerware die Tendenz stark nach oben zeigt.

Unsere Analyse der ersten acht Monate von 2019 zeigt, dass die Anzahl der Nutzer, die von Stalkerware betroffen waren, die Anzahl der Angriffe durch Trojan-Spy überstieg. Während in 2018 noch mehr als 43.000 Ziele von Spyware den etwa 28.000 Zielen von Stalkerware gegenüberstanden, zeigt sich in 2019 ein exakt umgekehrtes Bild. Die Anzahl der Benutzer, die von Stalkerware betroffen sind, stieg um 35 % und wuchs auf mehr als 37.000 an, während von Spyware-Tools lediglich 26.620 Ziele betroffen waren.

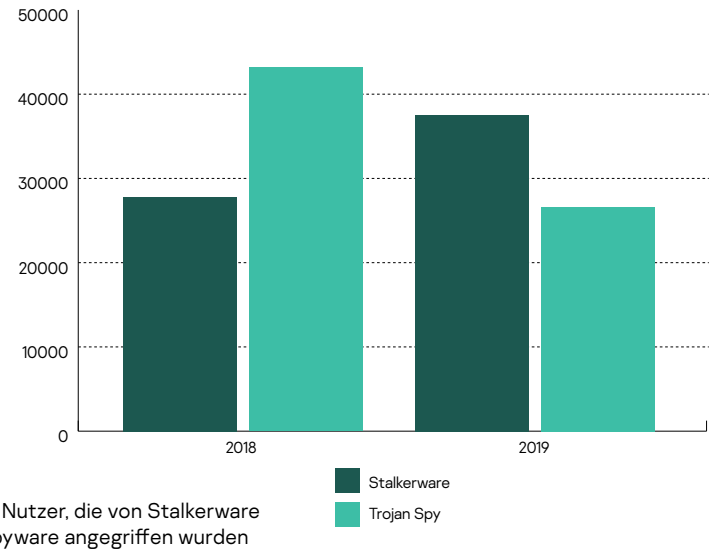


Abb. 6 Nutzer, die von Stalkerware und Spyware angegriffen wurden

Die Anzahl von Vorfällen, die mit Stalkerware im Zusammenhang stehen und von Kaspersky-Produkten registriert wurden, ist im Vergleich zu allen Bedrohungen im Jahr 2018 erheblich gestiegen. Zwischen Januar und August des letzten Jahres betrug die Anzahl der Benutzer, die mit solcher Software in Kontakt kamen, nur 1,01 % der Gesamtanzahl aller Benutzer, die mit potenziell gefährlicher Software (Adware und andere Tools der Kategorie "not-a-virus") konfrontiert wurden (2.740.023). Stalkerware scheint an Verwendung zuzunehmen, während traditionelle Malware-Angriffe jetzt weniger verbreitet sind, als sie es vor 12 Monaten waren.

Fazit und Empfehlungen

Es lässt sich eindeutig feststellen, dass Stalkerware auf dem Vormarsch ist und in der Landschaft der Cybersicherheit eine immer stärkere Position einnimmt. Unter Berücksichtigung der Schwankungen in der Gesamtzahl der festgestellten Riskware-, Adware- und Spyware-Angriffe im Jahresvergleich steigt der Anteil der Vorfälle mit Stalkerware-Bezug weiter an. Es wird vermutlich noch einige Zeit dauern, bis die Rolle von Stalkern in der Landschaft der Cyberbedrohungen herausgearbeitet ist, aber es sind jetzt auf jeden Fall schon mehr Vorfälle zu verzeichnen. Der starke Anstieg ist optimierter Cybersicherheitssoftware zu verdanken, da Kaspersky im April 2019 eine Lösung herausbrachte, die Nutzer vor Stalkerware warnt.

Es lässt sich außerdem eine gewisse Konstanz in Bezug auf Länder beobachten, in denen die meisten Stalkerware-Vorfälle registriert wurden – mit Russland, Indien, den USA und Deutschland als den am häufigsten betroffenen Regionen der letzten 2 Jahre.

Wir sind der Überzeugung, dass jede Person ein Recht auf den Schutz ihrer Privatsphäre hat. Aus diesem Grund stellen wir unsere Sicherheitskompetenz zur Verfügung, arbeiten im Kampf gegen Cyberkriminelle eng mit internationalen Organisationen und Vollzugsbehörden zusammen und entwickeln Technologien, Lösungen und Dienstleistungen, die vor Cyberbedrohungen schützen.

Doch es gibt auch eine gute Nachricht für Nutzer: Es werden Funktionen und effektive Lösungen entwickelt, um ihren Schutz zu gewährleisten. Praktische Methoden zur Behebung dieses Problems treten immer mehr in den Vordergrund. Unternehmen rund um IT-Sicherheit und Interessengruppen, die sich um Opfer häuslicher Gewalt kümmern, sollten ihre Kräfte bündeln und gemeinsam sicherstellen, dass Unternehmen der Cybersicherheit schneller auf Stalkerware reagieren. Von solchen Initiativen würden Opfern mithilfe von Technologie und Know-how profitieren. Aus diesem Grund hat Kaspersky das internationale Bündnis zur Bekämpfung von Stalkerware, der ‚Coalition Against Stalkerware', mit initiiert und unterstützt dieses tatkräftig.

Über Kaspersky

Kaspersky ist ein internationales Cybersicherheitsunternehmen, das im Jahr 1997 gegründet wurde. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky dient als Grundlage für innovative Sicherheitslösungen und -dienste, um Unternehmen, kritische Infrastrukturen, Regierungen und Privatanwender weltweit zu schützen. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung gegen komplexe und sich weiter entwickelnder Cyberbedrohungen. Über 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky geschützt. Die Unternehmenskultur von Kaspersky basiert auf den Werten von Transparenz, Vertrauen und einem globalen Mindset.

www.kaspersky.com

www.securelist.com

kaspersky