La situazione dello **stalkerware** nel 2019

COALITION AGAINST STALKERWARE

kaspersky

COALITION AGAINST
STALKERWARE

La coalizione contro gli stalkerware

Un nuovo gruppo di lavoro mondiale, che combina competenze in materia di assistenza alle vittime e cybersicurezza, per aiutare gli utenti colpiti

Dieci organizzazioni: 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 e WEISSER RING hanno lanciato nel novembre 2019 un'iniziativa mondiale chiamata Coalition Against Stalkerware (Coalizione contro gli stalkerware), volta a proteggere gli utenti dai cosiddetti stalkerware.

La Coalizione è stata realizzata per facilitare la comunicazione fra il mondo della sicurezza e le organizzazioni che combattono contro la violenza domestica. Con il suo portale online www.stopstalkerware.org, la Coalizione intende aiutare le vittime, facilitare il trasferimento di conoscenze fra i membri, sviluppare best practice per uno sviluppo etico dei software e sensibilizzare il pubblico sui pericoli degli stalkerware.

Il progetto nasce come un'iniziativa senza scopo di lucro, per coinvolgere attori provenienti da vari settori, come organizzazioni no-profit, imprese e altri settori come le forze dell'ordine. Visto l'alto impatto sociale per utenti in tutto il mondo e considerate le nuove varianti di stalkerware che vengono costantemente realizzate, la Coalition Against Stalkerware è aperta a nuovi partner o richieste di cooperazione.

Per ulteriori informazioni, visitare www.stopstalkerware.org

I fondatori descrivono l'importanza di **lavorare assieme contro gli stalkerware**:

COALITION AGAINST STALKERWARE

Alexander Vukcevic,
Direttore di Protection Labs,
Avira

"I software di monitoraggio si sono evoluti rapidamente nel corso degli ultimi anni, delle potenti funzioni di sorveglianza sono state aggiunte e lo scopo stesso di tali attività è radicalmente cambiato. Il continuo aumento nell'utilizzo di dispositivi mobili, unito alle falle legislative in materia, fornisce ai malintenzionati strumenti di spionaggio sui propri partner, familiari o amici. Avira considera tutto questo come una nuova categoria di minacce e invita le aziende impegnate nel campo della sicurezza informatica e le organizzazioni che operano contro la violenza domestica a unire le proprie forze, condividere informazioni e lavorare assieme per fermare queste violazioni della privacy."

Eva Galperin,
Direttrice della sicurezza informatica, **Electronic Frontier Foundation**

"Gli stalkerware, usati per spiare telefoni e computer nel quadro di abusi domestici o molestie, sono un problema molto serio, che spesso va di pari passo con altre forme di abuso, inclusa la violenza fisica. L'ubiquità degli stalkerware è un problema complesso, che va combattuto con più attori, provenienti da diversi campi."

Anna McKenzie, Manager delle comunicazioni, **European Network for the Work with Perpetrators of Domestic Violence (WWP EN)**

"Gli studi dimostrano che il 70% delle donne vittime di cyberstalking sperimenta anche una o più forme di violenza fisica e/o sessuale da parte di un partner intimo. Dobbiamo impedire ai responsabili di sfruttare i telefoni delle partner, mettendoli dinanzi alle proprie responsabilità. La Coalition Against Stalkerware ci permette mettere le nostre conoscenze relative a violenza di genere e perpetratori al servizio delle aziende di sicurezza informatica, per lavorare assieme contro lo sfruttamento di nuove tecnologie nella violenza contro le donne."

Hauke Gierow,
Portavoce,
G DATA CyberDefense

"L'installazione di stalkerware sul telefono del proprio partner costituisce una violazione dei diritti umani fondamentali. Siamo determinati a combattere questo tipo di comportamento e a proteggere i sopravvissuti agli abusi, che sono prevalentemente donne. G DATA Cyber Defense si impegna a sensibilizzare maggiormente gli utenti riguardo ai rischi potenziali, e a lavorare con le organizzazioni in difesa delle vittime per affrontare anche i risvolti meno tecnici associati agli stalkerware."

Vyacheslav Zakorzhevsky,
Capo ricerca anti-malware,
Kaspersky

"Per contrastare questo problema, è importante che i vendor di cybersicurezza e le organizzazioni no-profit lavorino assieme. L'industria della sicurezza informatica dà il suo contributo migliorando il rilevamento degli stalkerware e notificando più adeguatamente gli utenti su queste minacce alla loro privacy. Le organizzazioni di assistenza e sensibilizzazione lavorano direttamente a contatto con le vittime di violenza domestica, conoscendo le loro criticità e necessità, e possono per questo guidare il nostro lavoro. Agendo assieme, fianco a fianco, saremo in grado di assistere i sopravvissuti con competenze tecniche e creazione di capacità."

David Ruiz,
Autore, esperto di privacy online,
Malwarebytes Labs

"Per anni, Malwarebytes ha rilevato e avvisato gli utenti delle abilità potenzialmente dannose degli stalkerware, una minaccia invasiva che può privare gli individui del proprio diritto alla privacy e le aspettative a esso correlate. Proprio come gli abusi che consentono, gli stalkerware proliferano lontano dagli occhi del pubblico, lasciando le proprie vittime nel più totale isolamento, bisognose di essere ascoltate e aiutate. Una Coalition Against Stalkerware che combatta assieme è il prossimo passo necessario per fermare questa minaccia digitale: si tratta di un approccio collaborativo guidato dal desiderio di offrire un utilizzo sicuro delle tecnologie per tutti, dappertutto."

Erica Olsen,
Direttrice del Safety Net Project,
National Network to End Domestic Violence

"Quando progettati per operare in modalità totalmente nascosta, senza notifiche al proprietario del dispositivo, gli stalkerware possono fornire agli stalker e altri criminali un solido strumento per mettere in atto molestie, sorveglianza, stalking, frodi e abusi. Questo tipo di crimini può essere terrificante, traumatizzante e solleva importanti questioni relative a sicurezza e privacy. La creazione di questa Coalizione è un importante passo avanti nella gestione di questo problema."

Kevin Roundy,
Direttore della ricerca,
NortonLifeLock

"A NortonLifeLock, i nostri esperti ricercatori si impegnano da 12 anni per impedire agli stalker di utilizzare questo tipo di software, fornendo a vittime reali e potenziali degli strumenti con cui proteggersi e liberarsi dalle molestie, dalle violenze e dagli attacchi. Siamo orgogliosi di fare parte della Coalition Against Stalkerware, di poter condividere le nostre competenze e lottare assieme per fermare gli abusi."

Wilson "Chilly" Hightower,
Capo Intake,
Operation Safe Escape

"Gli stalkerware non hanno altro scopo se non quello di violare, ferire e instillare un costante senso di paura e ansia in molti dei nostri clienti. Si tratta di una minaccia attiva alla sicurezza e alla privacy delle persone. Via via che le nostre vite diventano più radicate nella tecnologia e dipendenti da essa, la minaccia degli stalkerware si fa sempre più grande. Oggi è più importante che mai prevedere queste minacce e privare i perpetratori del loro potere, che siano stalker o altre entità malevole. Operation Safe Escape non potrebbe essere più orgogliosa di far parte di questo gruppo dedicato a restituire la privacy e il senso di sicurezza ai nostri clienti e a chiunque altro, ovunque si trovi."

Horst Hinger,
Vice direttore generale,
WEISSER RING

"Come associazione no-profit, siamo consapevoli di come la tecnologia possa facilitare l'accesso degli stalker ai dati privati delle proprie vittime. Queste ultime, raramente cercano aiuto, frenate dalla vergogna. WEISSER RING rileva come lo stalking sia un elemento sempre più presente nei contesti di abuso presi in carico. Nel 2018 abbiamo assistito 1019 casi di stalking, un incremento di circa il 3% rispetto all'anno precedente. Secondo le statistiche pubblicate dalla polizia tedesca, nel 2018 si sono verificati quasi 19.000 casi di stalking totali, 500 in più rispetto all'anno precedente, un altro numero chiaramente in ascesa. Per questo abbiamo creato l'app NO STALK assieme alla WEISSER RING Foundation, per fornire alle vittime uno strumento efficace per documentare l'abuso con prove evidenti."

Principali constatazioni, aggiornato ad aprile 2020

A livello mondiale, il numero di utenti con stalkerware installato sui propri dispositivi è salito del 67% in un solo anno.

Questa sezione fornisce un confronto in cifre dell'intero anno 2019 rispetto al 2018. A causa della data di pubblicazione, la parte restante del rapporto contiene dati da gennaio ad agosto 2019.

- Nel 2018, 40.386 singoli utenti di dispositivi mobili erano stati attaccati da stalkerware. Alla fine del 2019 questo numero è aumentato del 67%, con ben 67.500 dei nostri utenti colpiti.

- Si è verificato un duplice aumento degli attacchi durante la seconda metà del 2019, rispetto alla prima metà dello stesso anno. A gennaio 2019, 4483 utenti Kaspersky avevano subito un attacco su dispositivo mobile. Nel settembre 2019 il numero era salito a 9546 e a dicembre il numero raggiungeva gli 11.052 utenti attaccati.

- Russia, Brasile, India e Stati Uniti sono le regioni globali più colpite dallo stalkerware, corrispondendo rispettivamente al 23,4%, 9,4%, 9% e 5,6% degli utenti coinvolti nel 2019.

- Il podio europeo dei paesi più colpiti è occupato da Germania (3,1%), Italia (2,4%) e Francia (1,8%).

Resumen

Lo stalkerware permette a chi abusa di spiare la propria vittima senza il suo consenso

Introduzione e metodologia

Sei mesi fa, abbiamo creato uno speciale avviso che informa gli utenti nel caso vi siano prodotti di spyware commerciale (stalkerware) installati sui loro telefoni. Questo rapporto prende in esame l'utilizzo dello stalkerware e il numero di utenti coinvolti da questo software durante i primi otto mesi del 2019.

Le tecnologie di sorveglianza dei consumatori si sono evolute rapidamente negli ultimi anni e lo scopo stesso di tale attività è drasticamente cambiato. L'avvento di Internet e la conseguente esplosione nell'uso di dispositivi mobili ha portato a un fiorente sviluppo di un certo tipo di software di sorveglianza, noto come stalkerware. Questo software permette agli utenti di spiare altre persone, ad esempio monitorandone i messaggi, le informazioni sulle chiamate e le posizioni GPS; il tutto nella più completa segretezza. Può spesso venire sfruttato per abusare della privacy di attuali o precedenti partner, ma anche di perfetti sconosciuti, semplicemente installando manualmente un'applicazione sullo smartphone o il tablet della vittima designata. A questo punto, lo stalker avrà accesso a una serie di dati personali senza la necessità di trovarsi in prossimità della vittima. Questo software è molto diverso da quello relativo al controllo genitoriale: mentre quest'ultimo utilizza app volte a restringere l'accesso a contenuti rischiosi o inadeguati, notificando costantemente un utente in base alle sue richieste, lo stalkerware permette a chi abusa di spiare la propria vittima senza il suo consenso.

La stragrande maggioranza delle app di stalkerware non sono disponibili nei negozi di applicazioni ufficiali come Google Play, e la loro installazione richiede accesso a un sito dedicato oltre che al dispositivo della vittima. I malintenzionati possono sfruttarle per monitorare le e-mail dei dipendenti, tener traccia di movimenti di bambini e perfino spiare i propri partner. Un simile utilizzo può sfociare in molestie, sorveglianza non autorizzata, stalking e perfino violenza domestica. Tuttavia, le attuali leggi che regolano l'utilizzo dello stalkerware non sono sufficientemente rigide da dissuadere i responsabili dall'abuso e lo sfruttamento di altre persone.

I dati presenti in questo rapporto sono estrapolati da statistiche di minaccia aggregate, ottenute dalla rete Kaspersky Security Network, per misurare la frequenza e il numero di utenti colpiti da minacce di stalkerware durante i primi otto mesi del 2019, rispetto ai dati rilevati l'anno precedente. Kaspersky Security Network è l'infrastruttura dedicata all'elaborazione dei dati di sicurezza informatica inviati da milioni di partecipanti volontari in tutto il mondo. In questo blog abbiamo discusso del perché lo stalkerware venga utilizzato e di dove venga più efficientemente implementato.

Principali constatazioni

In tutto il mondo, il numero di utenti che ha installato uno stalkerware sui proprio dispositivi è aumentato del 35% in un solo anno

- Da gennaio ad agosto 2019, in tutto il mondo, si sono verificati oltre 518.223 casi nei quali le nostre tecnologie di protezione hanno registrato la presenza di stalkerware sui dispositivi degli utenti, oppure ne hanno rilevato un tentativo di installazione; un aumento del 373% rispetto allo stesso periodo nel 2018.
- Durante i primi otto mesi del 2019, 37.532 utenti sono entrati in contatto almeno una volta con stalkerware. Si tratta di un aumento del 35% rispetto allo stesso periodo nel 2018, quando 27.798 utenti erano stati vittima di questa minaccia.
- Il numero di utenti presi di mira da uno spyware aggressivo rilevato come Trojan-Spy ha raggiunto i 26.620 durante i primi otto mesi del 2019, ovvero una minoranza rispetto al numero totale di utenti infettati da stalkerware.
- La Federazione russa rimane la regione più prominente per quanto riguarda il problema dello stalkerware a livello globale, riportando il 25,6% degli utenti potenzialmente infettati durante i primi otto mesi del 2019. L'India si piazza al secondo posto con il 10,6% degli utenti coinvolti e il Brasile al terzo (10,4%). Gli Stati Uniti si classificano al quarto posto con il 7,1%.
- Per quanto riguarda l'Europa, Germania, Italia e Gran Bretagna si classificano rispettivamente ai primi tre posti.

Incremento della minaccia stalkerware

Quest'anno ha visto un netto aumento del numero di rilevamenti di stalkerware su dispositivi Android protetti da prodotti Kaspersky. Un motivo per questo incremento potrebbe essere il miglior rilevamento di software di questo tipo, grazie a nuove soluzioni di cybersicurezza. In aprile, Kaspersky ha lanciato una funzionalità nella sua app di sicurezza Android, Privacy Alert, che informa specificamente gli utenti nel caso in cui un software utilizzabile a scopo di stalking venga rilevato nel dispositivo. Da allora, il numero di rilevamenti è aumentato costantemente. Ad esempio, 4.315 utenti hanno incontrato dello stalkerware a marzo 2019, rispetto ai 7.075 di aprile, un aumento del 64% in un solo mese. Il dato passa a 9.251 nel mese di agosto, un aumento del 94% rispetto al mese in cui la funzionalità è stata lanciata.

Questi programmi di sorveglianza apertamente in commercio vengono spesso usati per spiare colleghi, familiari o partner e ve ne è una forte richiesta. Per cifre relativamente contenute, a volte addirittura soltanto 6 € al mese, queste app restano nascoste pur continuando a informare chi le ha installate dell'attività del dispositivo: posizione del proprietario, cronologia del browser, messaggi di testo, chat provenienti da social media e molto altro. Alcuni di essi sono addirittura in grado di effettuare registrazioni video e vocali.

Per esaminare più a fondo la portata del problema dello stalkerware, Kaspersky ha analizzato gli ultimi otto mesi di attività. Fra gennaio e agosto del 2019, 37.533 utenti sono entrati in contatto con stalkerware sui loro dispositivi almeno una volta. Si tratta di un aumento del 35% rispetto allo stesso periodo nel 2018, quando 27.798 utenti erano stati vittima dello stesso. In generale, si sono verificati 518.223 casi in cui i prodotti Kaspersky hanno registrato la presenza di stalkerware sul dispositivo dell'utente, oppure ne hanno rilevato un tentativo di installazione durante il periodo fra gennaio e agosto del 2019, un impressionante aumento del 373% rispetto allo stesso periodo nel 2018.

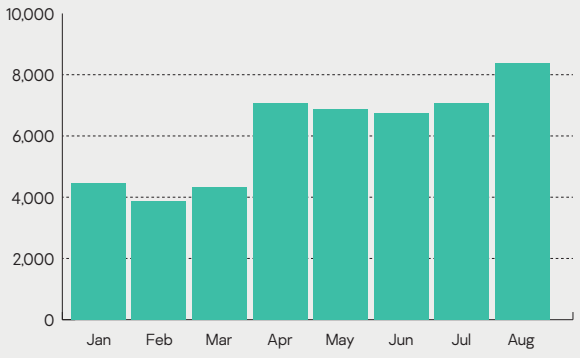


Fig. 1 Numero di utenti che hanno avuto contatti con stalkerware nei mesi di gen-ago 2019

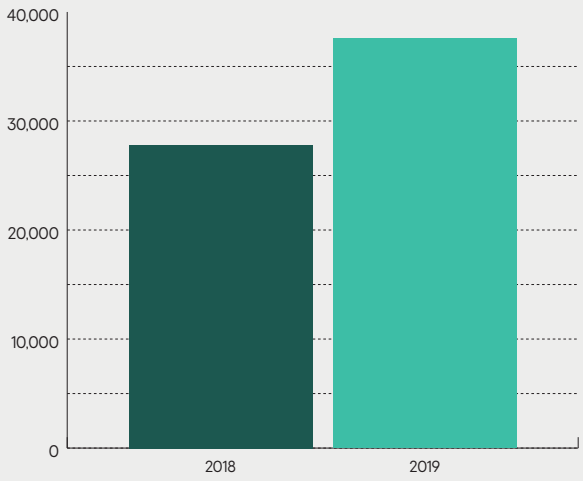
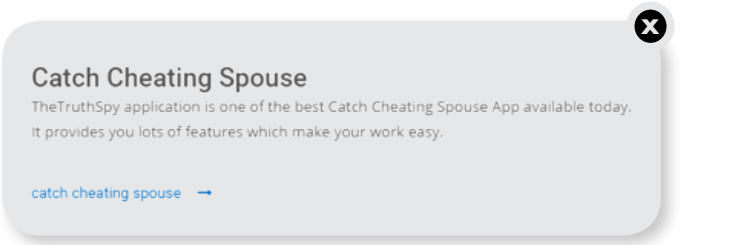


Fig. 2 Confronto fra utenti presi di mira da stalkerware, 2018 e 2019



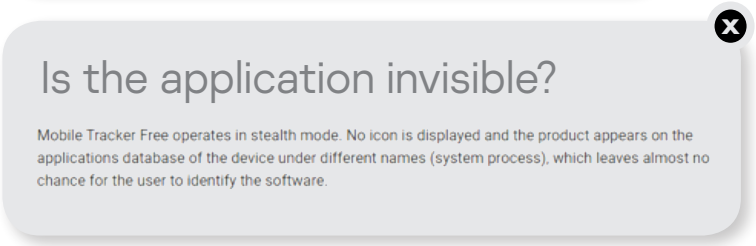


Fig. 3 Screenshot dal sito ufficiale Mobile Tracker Free

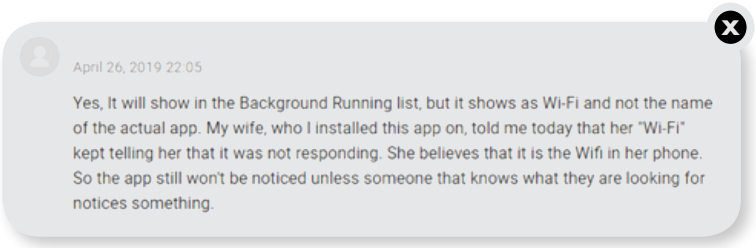


Fig. 4 Screenshot dal sito ufficiale di TheTruthSpy

L'installatore potrebbe anche accedere alle foto della vittima contenute sul telefono e alla fotocamera stessa, in tempo reale, oltre a poter consultare cronologia del browser, file presenti sul dispositivo, calendario e rubrica. Inoltre, l'applicazione permette di controllare il dispositivo in remoto

Esempi di software utilizzati a scopo di stalking

La famiglia di stalkerware più prolifica del 2019 è sicuramente Monitor.AndroidOS.MobileTracker.a, che ha colpito 6.559 utenti singoli. Al secondo posto vediamo Monitor.AndroidOS.Cerberus.a, rilevato sui dispositivi di 4.370 utenti, immediatamente seguito da Monitor.AndroidOS.Nidb.a al terzo posto con 4.047 utenti.

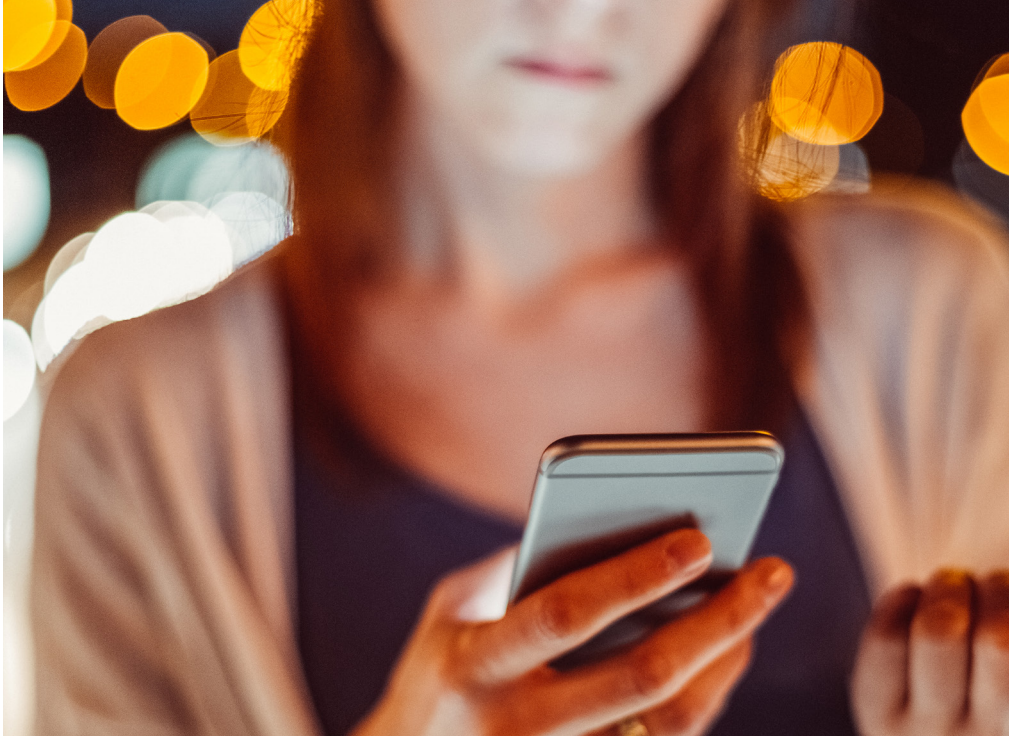
Facendo un confronto con i dati del 2018 notiamo un cambiamento ai primi due posti. Monitor.AndroidOS.Nidb.a e Monitor.AndroidOS.PhoneSpy.b erano i software maggiormente rilevati nel 2018, con un risultato rispettivo di 4.427 e 2.819 utenti infettati. Monitor.AndroidOS.XoloSale.era il terzo software di stalkerware più comune, con 1.946 vittime.

Nel nostro sistema di classificazione interno, l'indicazione Monitor.AndroidOS.MobileTracker.a fa riferimento a un'applicazione Mobile Tracker Free, installata per tener traccia dell'attività di bambini o dipendenti. Questa applicazione permette di registrare la posizione dell'utente, la sua corrispondenza via SMS e applicazioni di messaggistica (WhatsApp, Hangouts, Skype, Facebook Messenger, Viber, Telegram, ecc.), oltre alle normali chiamate. L'installatore potrebbe anche accedere alle foto della vittima contenute sul telefono e alla fotocamera stessa, in tempo reale, oltre a poter consultare cronologia del browser, file presenti sul dispositivo, calendario e rubrica. Inoltre, l'applicazione permette di controllare il dispositivo in remoto. Ma non è tutto: vi è anche la possibilità di lavorare in modalità segreta, celandosi dietro l'aspetto di un'applicazione di sistema.

La prossima applicazione, Cerberus (Monitor.AndroidOS.Cerberus.a), viene pubblicizzata come app antifurto. Tuttavia, questa permette anche a uno stalker di lavorare in modalità 'nascosta', impedendone il rilevamento. Fra le altre cose, dà la possibilità di registrare la posizione del dispositivo, scattare foto con la fotocamera o ottenere catture di schermata, oltre a poter registrare audio dal microfono.

Lo stalkerware terzo classificato, Monitor.AndroidOS.Nidb.a, è in realtà un gruppo di applicazioni simili: iSpyoo/TheTruthSpy/Copy9. A differenza delle due precedenti applicazioni, alcuni rappresentanti di questo gruppo si presentano apertamente come strumenti per spiare i propri partner, scrivendo addirittura articoli su questo tema.

Il set di funzioni di questi programmi è relativamente standard, ma comunque impressionante: tracciamento dei siti Web, intercettamento della corrispondenza via SMS e applicazioni di messaggistica, rilevamento delle chiamate e della cronologia del browser. Come molte altre applicazioni simili, richiedono diritti di amministratore per poter eseguire alcune funzioni sul dispositivo. Possono funzionare in modalità 'nascosta' e il loro nome nell'elenco di applicazioni installate mima quello dei processi di sistema.



Dove viene rilevato lo stalkerware?

Esiste un mercato globale per software di spyware e stalkerware legali, come dimostra la vasta gamma di regioni in cui gli attacchi si verificano. I primi 10 paesi con la maggior fetta di utenti attaccati da stalkerware non presentano somiglianze geopolitiche e non sono geograficamente vicini.

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%**

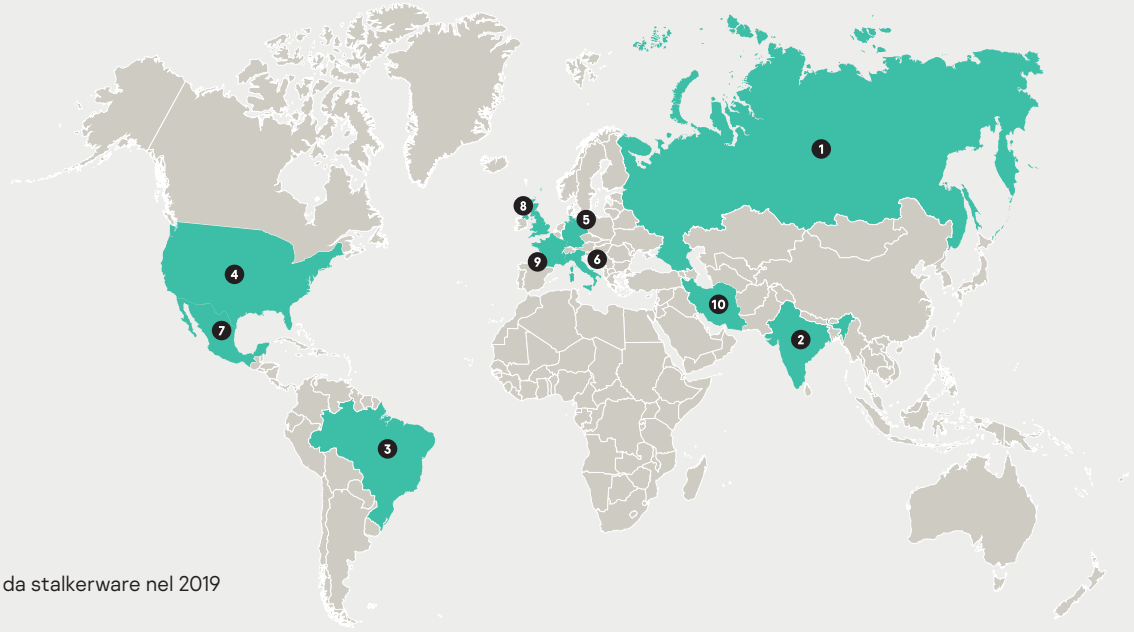


Fig. 5 Geografia degli utenti infettati da stalkerware nel 2019

Da un'indagine è emerso che, l'85% degli operatori sociali che supportano le vittime di violenza domestica, ha assistito delle vittime il cui molestatore le ha rintracciate utilizzando il GPS

I rilevamenti di Kaspersky mostrano che la Russia è la regione di punta per l'attività di stalkerware. La persistente attività in India ha portato il paese sul secondo gradino del podio, con il 10,56% di utenti coinvolti in incidenti di stalkerware da gennaio ad agosto.

Il Brasile contribuisce con il 10,39% di utenti attaccati nel 2019, mentre gli Stati Uniti sono ora quarti (7,11%). Nel paese vi sono gruppi di pressione che cercano di aumentare l'attenzione sui danni dello stalkerware e che stanno conducendo illuminanti ricerche sui consumatori. 72 rifugi per vittime di violenza domestica sono stati presi in esame da National Public Radio; i dati riportano che l'85% dei dipendenti di tali centri ha riferito di aver assistito vittime controllate via GPS dal proprio aguzzino. Quasi i tre quarti (71%) dei perpetratori di violenza domestica monitorano le attività informatiche delle proprie vittime, mentre il 54% ha tenuto traccia del telefono cellulare della propria vittima con stalkerware. Il quinto paese più colpito nel 2019 è stata la Germania con il 3,55% dei casi.

Lo stalkerware nel panorama delle minacce informatiche

Nel 2019 oltre 37.000 utenti sono stati attaccati attraverso uno stalkerware, contro i quasi 27.000 dell'anno precedente

Se confrontiamo lo stalkerware e lo spyware al resto degli attacchi subiti dagli utenti di dispositivi mobili, come adware, riskware e malware, noteremo che rappresentano una bella fetta dei programmi dannosi che non fanno parte della categoria dei virus. Durante i primi otto mesi del 2019, Kaspersky ha rilevato 2.350.862 utenti attaccati da minacce potenzialmente indesiderate e solo l'1,60% di queste erano relative allo stalkerware. Tuttavia, a differenza delle altre potenziali minacce di massa (come l'adware), lo stalkerware richiede una specifica azione da parte di uno stalker per portare a termine l'operazione. Ogni obiettivo viene scelto e abusato di proposito. Quindi, nonostante le cifre siano nettamente inferiori, lo stalkerware richiede uno sforzo ben più specifico per avere effetto e si inserisce in un inquietante contesto di abuso a ogni attacco.

Per inquadrare le dinamiche di sviluppo dello stalkerware in modo più generale, abbiamo confrontato questo tipo di software con l'intera gamma di malware illegali per PC che indichiamo come Trojan Spy. I risultati dimostrano che mentre lo spyware illegale è in declino, lo stalkerware fiorisce.

La nostra analisi dei primi otto mesi del 2019 dimostra che il numero di utenti che sono venuti in contatto con lo stalkerware ha, di fatto, sorpassato le cifre relative agli attacchi Trojan-Spy. Mentre il 2018 ha visto oltre 43.000 obiettivi di spyware e 28.000 obiettivi di stalkerware, nel 2019 abbiamo un quadro molto diverso. Il numero di utenti colpiti da stalkerware è cresciuto del 35%, raggiungendo i 37.000, mentre gli strumenti di spyware hanno interessato 26.620 obiettivi.

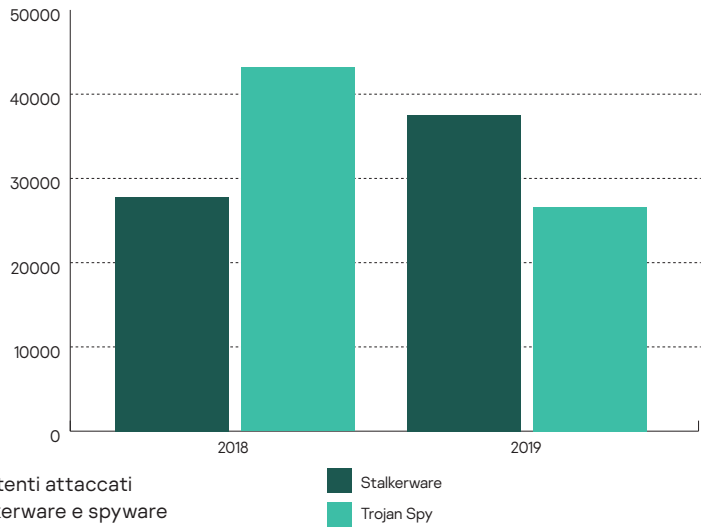


Fig. 6 Utenti attaccati da stalkerware e spyware

Si nota un evidente incremento nel numero di incidenti a sfondo di stalkerware registrati dai prodotti Kaspersky, rispetto a tutte le minacce rilevate nel 2018. Fra gennaio e agosto dello scorso anno, software simili rappresentavano un misero 1,01% del numero totale (2.740.023) di software potenzialmente pericolosi (adware e altri di categoria non virus) affrontati dagli utenti. Si direbbe che lo stalkerware stia crescendo a livello di popolarità, mentre gli attacchi malware di tipo più tradizionale sono meno prolifici rispetto a 12 mesi fa.

Conclusioni e consigli

Lo stalkerware è chiaramente in ascesa e sta assumendo una posizione sempre più di primo piano nel panorama della sicurezza informatica. Come dimostra il numero totale di riskware rilevati, gli attacchi di adware e spyware fluttuano di anno in anno, mentre la percentuale di incidenti collegati a stalkerware è costantemente in salita. Individuare il ruolo degli stalker nel panorama delle minacce informatiche potrebbe richiedere del tempo, ma sempre più incidenti vengono segnalati. Grazie a un miglioramento del software di sicurezza, da quando Kaspersky ha lanciato la sua soluzione d'avviso di stalkerware per gli utenti nell'aprile 2019 si nota un forte incremento di rilevamenti.

Si nota inoltre un certo livello di conformità fra i paesi in cui si segnalano più incidenti relativi a stalkerware, con Russia, India, Stati Uniti e Germania sempre in testa negli ultimi due anni.

La buona notizia per gli utenti è che sempre nuove funzionalità e soluzioni vengono messe sul mercato per proteggersi. Modalità pratiche per risolvere il problema continuano ad apparire. Le aziende dedicate alla sicurezza informatica e le organizzazioni impegnate nel sostegno di vittime della violenza domestica dovrebbero unire le loro forze per spingere le aziende di cybersicurezza a meglio rispondere agli stalkerware. Simili iniziative aiuterebbero le vittime con tecnologia ed esperienza.

Noi crediamo che ogni persona abbia diritto alla protezione della propria privacy. È per questo che portiamo sul mercato competenza nel campo della sicurezza, lavorando fianco a fianco con organizzazioni internazionali e forze di polizia per combattere i criminali informatici, oltre a sviluppare tecnologie, soluzioni e servizi che permettono agli utenti di mettersi al sicuro dalle cyberminacce.

Informazioni su Kaspersky

Con oltre 20 anni di esperienza nel campo della sicurezza informatica, le competenze di Kaspersky riguardo a conoscenze delle minacce e sicurezza sono sempre in evoluzione per trasformarsi in soluzioni e servizi innovativi, volti a proteggere aziende, infrastrutture critiche, governi e consumatori in tutto il mondo. Oltre 400 milioni di utenti vengono protetti dalle tecnologie Kaspersky e aiutiamo 270.000 clienti corporate a mettere al sicuro ciò che di più importante hanno. La cultura aziendale di Kaspersky si basa sulla trasparenza, sulla fiducia e su una mentalità globale con più di 3.900 specialisti che lavorano in 35 uffici collocati in 31 paesi.

www.kaspersky.com

www.securelist.com

kaspersky