Inseguito in tempo reale: Intellexa, il predatore israeliano in tasca

thecradle.co/articles/stalked-in-real-time-intellexa-the-israeli-predator-in-your-pocket

Kit Klarenberg

Nuova ricerca Un rapporto pubblicato da Amnesty International denuncia le operazioni chiave di Intellexa, un consorzio di spyware legato a Israele responsabile di sorveglianza di massa e violazioni dei diritti umani in diversi continenti. Tra questi, "Predator", uno strumento altamente invasivo che dirotta gli smartphone per rubare qualsiasi cosa, dai feed delle telecamere alle chat crittografate, alle posizioni GPS e alle email. È solo l'ultimo esempio di uno specialista di spyware legato a Israele che agisce senza riguardo per la legge. Tuttavia, il rapporto di Amnesty non si è concentrato su questo aspetto e si è limitato ai dettagli tecnici, lasciando in gran parte oscurata la piena portata della violazione legale. Intellexa è tra gli " spyware mercenari" più noti al mondo. fornitori. Nel 2023, la società è stata multata dall'Autorità greca per la protezione dei dati personali per non aver ottemperato alle indagini sulla società.

Un caso giudiziario in corso Ad Atene, l'inchiesta coinvolge gli apparati di Intellexa e i servizi segreti locali nell'hacking dei telefoni di ministri del governo, alti ufficiali militari, giudici e giornalisti. Amnesty International denuncia le attività di spionaggio di Intellexa, ma non fornisce informazioni sul suo fondatore. Tal Dilian, un ex agente di spionaggio militare israeliano di alto rango, è composto da veterani dello spionaggio israeliano.

Nel marzo 2024. Dopo anni di rivelazioni dannose sulle attività criminali di Intellexa, il Tesoro degli Stati Uniti ha imposto sanzioni drastiche a Dilian, alle aziende a lui più vicine e a cinque diverse entità commerciali associate a Intellexa.

Predatore: Osservare, ascoltare, estrarre

Tuttavia, queste misure severe non hanno scoraggiato le attività di Intellexa. L'offerta di servizi dell'azienda si è evoluta nel tempo, diventando sempre più difficile da rilevare e sempre più efficace nell'infettare i dispositivi target. In genere, la società civile, gli attivisti per i diritti umani e i giornalisti sono nel mirino.

Il 3 dicembre, Google ha annunciato che gli obiettivi di Intellexa ammontano ad almeno "diverse centinaia", con persone potenzialmente interessate residenti in Angola, Egitto, Kazakistan, Pakistan, Arabia Saudita, Tagikistan, Uzbekistan e altrove.

Strumento di punta di Intellexa, Predator infetta i dispositivi target tramite metodi "one-click" e "zero-click", integrandosi persino tramite annunci online. Una volta installato, saccheggia silenziosamente foto, password, messaggi e chat su Signal, Telegram e WhatsApp, oltre alle registrazioni dei microfoni.

Questi dati rubati vengono poi instradati attraverso un labirinto di server anonimi fino ai loro client.
Questi clienti sono per la maggior parte governi autoritari, che spesso prendono di mira attivisti e giornalisti.

Predator vanta anche una serie di funzionalità esclusive progettate per nascondere la sua installazione su un dispositivo ai bersagli. Ad esempio, lo strumento spia valuta il livello della batteria di un dispositivo e se è connesso a Internet tramite dati della scheda SIM o Wi-Fi. Ciò consente di

processo di estrazione personalizzato, che garantisce che i dispositivi non siano palesemente privi di rete o di energia, per evitare di alimentare sospetti negli utenti.

La grotta di Aladino

Se Predator rileva di essere stato rilevato, lo spyware si autodistruggerà, eliminando ogni traccia della sua presenza sul dispositivo colpito. I metodi con cui Intellexa installa la sua tecnologia maligna sui dispositivi di destinazione sono altrettanto ingegnosi e insidiosi.

Oltre agli attacchi "one-click", Intellexa è pioniera nel campo dell'infiltrazione "zero-click". La sua risorsa "Aladdin" sfrutta gli ecosistemi pubblicitari online, in modo che agli utenti sia sufficiente visualizzare un annuncio pubblicitario, senza interagire con esso, perché lo spyware infetti un dispositivo.

Tali annunci possono apparire su siti web o app affidabili, simili a qualsiasi altro annuncio che un utente visualizzerebbe normalmente. Questo approccio richiede a Intellexa di identificare un "identificatore univoco", come l'indirizzo email, la posizione geografica o l'indirizzo IP dell'utente, per presentargli con precisione un annuncio dannoso.

I clienti governativi di Intellexa possono spesso accedere facilmente a queste informazioni, semplificando il targeting accurato. Ricerca pubblicata Secondo Recorded Future, un'azienda statunitense di sicurezza informatica, Intellexa ha segretamente creato delle società dedicate alla pubblicità su dispositivi mobili per creare "annunci esca", tra cui annunci di lavoro, per attirare i bersagli.

Aladdin è in fase di sviluppo almeno dal 2022 e nel tempo è diventato sempre più sofisticato. È preoccupante che Intellexa non sia l'unica azienda attiva in questo innovativo campo di spionaggio. Amnesty International suggerisce "infezione basata sulla pubblicità"

Le metodologie vengono sviluppate e utilizzate attivamente da numerose società di spyware mercenarie e da governi specifici che hanno creato sistemi di infezione ADINT simili."

Il fatto che l'ecosistema della pubblicità digitale sia stato sovvertito per hackerare i telefoni di cittadini ignari richiede un intervento urgente da parte del settore, che al momento non è ancora stato intrapreso.

Altrettanto inquietante è il fatto che un video di formazione di Intellexa trapelato mostri come l'azienda di spyware possa "accedere e monitorare da remoto i sistemi Predator attivi dei clienti". In pratica, è in grado di tenere d'occhio chi i suoi clienti stanno spiando e quali dati privati stanno estraendo, in tempo reale.

Registrato a metà del 2023, il video inizia con un istruttore che si collega direttamente a un sistema Predator distribuito tramite TeamViewer. Un popolare software commerciale di accesso remoto. I suoi contenuti suggeriscono che Intellexa può visualizzare almeno 10 diversi sistemi dei clienti contemporaneamente.

Questa capacità è ampiamente evidenziata nel video trapelato, quando un membro dello staff chiede al proprio formatore se si sta connettendo a un ambiente di test. In risposta, il formatore afferma di aver invece effettuato l'accesso a un "ambiente cliente" in tempo reale.

L'istruttore avvia quindi una connessione remota, mostrando che lo staff di Intellexa può accedere a informazioni altamente sensibili raccolte dai clienti, tra cui foto, messaggi, indirizzi IP, sistemi operativi e versioni software degli smartphone e altri dati di sorveglianza raccolti dalle vittime di Predator.

Il video sembra anche mostrare tentativi di infezione "in diretta" da parte di Predator contro obiettivi reali dei clienti di Intellexa. Vengono fornite informazioni dettagliate su almeno un tentativo di infezione rivolto a un individuo residente in Kazakistan, incluso il link dannoso su cui l'individuo ha cliccato inconsapevolmente, consentendo l'infiltrazione nel suo dispositivo.

Altrove, vengono visualizzati nomi di dominio che imitano siti web di notizie kazaki autentici, progettati per ingannare gli utenti. Il paese dell'Asia centrale, pronto ad aderire simbolicamente agli Accordi di Abramo, è un cliente confermato di Intellexa, e i giovani attivisti locali sono stati precedentemente presi di mira dal famigerato spyware Pegasus, anch'esso incubato in Israele.

Dietro gli schermi: oscurità legale e accesso dall'estero

Il video trapelato solleva una serie di gravi preoccupazioni sulle attività di Intellexa. Innanzitutto, l'oscura entità di spionaggio digitale ad alta tecnologia utilizzava TeamViewer, il che solleva importanti preoccupazioni in termini di sicurezza. sono da tempo disponibili per accedere alle informazioni sugli obiettivi dei clienti.

Ciò solleva ovvi interrogativi su chi altro potrebbe essere in grado di accedere a questo tesoro, all'insaputa dell'azienda. Inoltre, non vi è alcuna indicazione che i clienti di Intellexa abbiano approvato questo accesso per il processo di formazione, o che il tutorial sia stato condotto con misure di sicurezza anche di base.

Pertanto, gli obiettivi delle risorse di spionaggio di Intellexa rischiano non solo di vedere i loro segreti più sensibili rivelati a un governo ostile senza la loro conoscenza o il loro consenso, ma anche a una società di sorveglianza straniera.

La misura in cui Intellexa è consapevole di come la sua tecnologia viene utilizzata dai suoi clienti è un punto centrale della controversia legale greca in corso. Storicamente, le società di spyware mercenarie hanno insistito fermamente non sono a conoscenza dei dati sequestrati in modo illecito dai loro clienti. Amnesty International afferma:

> "La scoperta che Intellexa aveva una potenziale visibilità sulle operazioni di sorveglianza attiva dei propri clienti, inclusa la visione di informazioni tecniche sugli obiettivi, solleva nuove questioni legali sul ruolo di Intellexa in relazione allo spyware e sulla potenziale responsabilità legale o penale dell'azienda per le operazioni di sorveglianza illegali eseguite utilizzando i suoi prodotti."

Le ultime rivelazioni su Intellexa hanno tutti gli elementi per uno scandalo storico, internazionale, nel modo preciso che l'uso di Pegasus da parte di entità statali e aziendali in tutto il mondo ha suscitato proteste internazionali, indagini penali e contenziosi duraturi
molti anni.

Tuttavia, la proliferazione di inquietanti strumenti di spionaggio privato – e il loro abuso su scala industriale da parte di clienti paganti – non è un bug aberrante, ma una conseguenza intenzionale dell'incessante crociata di Israele per la supremazia nella guerra informatica. Nel 2018, il Primo Ministro israeliano Benjamin Netanyahu si vantava:

> "La sicurezza informatica cresce attraverso la cooperazione, e la sicurezza informatica come business è enorme... Abbiamo speso una cifra enorme per la nostra intelligence militare, il Mossad e lo Shin Bet. Una cifra enorme. Una parte enorme di questa cifra viene dirottata verso la sicurezza informatica... Riteniamo che ci sia un'enorme opportunità di business nella ricerca infinita della sicurezza."

Questo investimento si manifesta in quasi ogni ambito della società israeliana. Numerose università a Tel Aviv, con il sostegno dello Stato, perfezionare nuove tecnologie e addestrare le future generazioni di spie informatiche e guerrieri digitali, che poi si uniranno ai ranghi delle forze armate di occupazione.

Una volta terminato il servizio militare, gli ex-alunni si ritrovano spesso a dover affrontare aziende in patria e all'estero che offrono gli stessi mostruosi servizi, già sperimentati sui palestinesi, a enti del settore privato e ai governi, senza alcuna supervisione o garanzia che queste risorse non vengano utilizzate per scopi malevoli.

I fallimenti dell'intelligence che ha permesso il successo dell'operazione Al-Aqsa Flood del 7 ottobre 2023 ha inferto un duro colpo alla credibilità di Israele come leader della sicurezza informatica, devastando al contempo la sua "Startup Nation" marchio, con gli investimenti esteri nel settore tecnologico dell'entità che crollano precipitosamente.

Il vero scandalo non è solo l'esistenza di aziende come Intellexa. È l'impunità internazionale di cui godono, le partnership occidentali che intrattengono e la complicità dei governi che chiudono un occhio sulla guerra informatica israeliana esportata in tutto il mondo.