Pegasus

Autor:
Data de publicació: 20-04-2022

Pegasus

Desenvolupadors
Grup NSO

Sistema operatiu
iOS, Android

Tipus
Programari espia

Lloc web
nsogroup.com

Pegasusus és un programari espia desenvolupat per l'empresa israeliana de ciber-armes NSO Group que es pot instal·lar encobertament en telèfons mòbils (i altres dispositius) executant la majoria de les versions d'iOS i Android. [2] Pegasusus és capaç d'explotar versions d'iOS fins a 14.6, a través d'una explotació de clic zero. [1] A partir de 2022, Pegasusus era capaç de llegir missatges de text, rastrejar trucades, recopilar contrasenyes, rastrejar ubicacions, accedir al micròfon i la càmera del dispositiu objectiu i recollir informació de les aplicacions.[3][4] El programari espia porta el nom de Pegasusus, el cavall alat de la mitologia grega. És un virus informàtic del cavall de Troia que es pot enviar "volant per l'aire" per infectar els telèfons mòbils. [5]

Pegasusus va ser descobert a l'agost de 2016 després d'un intent fallit d'instal·lació a l'iPhone d'un activista de drets humans que va portar a una investigació que revela detalls sobre el programari espia, les seves habilitats i les vulnerabilitats de seguretat que explotava. La notícia del programari espia va causar una important cobertura mediàtica. Va ser anomenat l'atac de telèfon intel·ligent "més sofisticat" de la història, i va ser la primera vegada que una explotació remota maliciosa va utilitzar jailbreaking per obtenir accés sense restriccions a un iPhone. [6]

El programari espia s'ha utilitzat per a la vigilància d'activistes anti-règim, periodistes i líders polítics de diverses nacions de tot el món. [7] El juliol de 2021, la iniciativa d'investigació Pegasusus Project, juntament amb una anàlisi en profunditat del grup de drets humans Amnistia Internacional, va informar que Pegasusus encara s'estava utilitzant àmpliament contra objectius d'alt perfil. [1] 1 facebook/pass:****

Name/bhavesh Chauhan

2 forfets : ******1134*

Context

NSO Group va desenvolupar la seva primera iteració de programari espia Pegasusus el 2011. [4] La companyia afirma que proporciona "als governs autoritzats tecnologia que els ajuda a combatre el terror i la delinqüència". [6] NSO Group ha publicat seccions de contractes que requereixen que els clients utilitzin els seus productes només per a investigacions criminals i de seguretat nacional i ha afirmat que té un enfocament líder en la indústria dels drets humans. [9]

L'agost de 2016, després d'un intent fallit d'instal·lar-lo en un iPhone pertanyent a un activista pels drets humans, Pegasus va ser conegut per l'opinió pública. Una investigació va revelar detalls sobre el programari espia, les seves capacitats i les vulnerabilitats de seguretat. Pegasus és capaç de llegir missatges de text, gravar trucades, recopilar contrasenyes, rastrejar la ubicació del telèfon, activar el micròfon i la càmera, accedir als contactes i en general obtenir informació de les aplicacions.[3] Apple va llançar la versió 9.3.5 del seu programari iOS, l'agost del 2016, per corregir les vulnerabilitats. Va ser anomenat l'atac de telèfon intel·ligent més «sofisticat» de la història, i va esdevenir la primera vegada en la història de l'iPhone en que es va detectar un atac remot de jailbreak.

La companyia que va crear l'spyware, NSO Group, va declarar que faciliten «als governs autoritzats tecnologia que els ajuda a combatre el terrorisme i el crim».[4] S'asseguren el compliment de les legislacions només facilitant el programari a agències governamentals oficials com ara cossos policials, serveis d'intel·ligència i estaments militars.[3]

El 2019, a través de WhatsApp, el telèfon del President del Parlament de Catalunya, Roger Torrent, va ser atacat amb Pegasus segons una investigació d'El País i The Guardian.[5] També van ser atacats els mòbils dels diputats d'Esquerra Republicana de Catalunya, Ernest Maragall, i de la Candidatura d'Unitat Popular, Anna Gabriel.[6][7]

El 2021, més revelacions periodístiques apuntaven a unes possibles 50.000 víctimes d'aquest programari espia. L'estat que més ús n'hauria fet seria Mèxic, seguit del Marroc i Emirats Àrabs Units. Altres països que figurarien com a principals clients foren Azerbaidjan, Bahrain, el Kazakhstan, Ruanda, Aràbia Saudita, Hongria i l'Índia.[3]

Principalment s'hauria usat contra activistes, ONG, polítics, empresaris, advocats i periodistes però també possibles criminals.[3]

Descobriment

L'explotació d'iOS de Pegasusus es va identificar a l'agost de 2016. El defensor àrab dels drets humans Ahmed Mansoor va rebre un missatge de text prometent "secrets" sobre la tortura que passa a les presons dels Emirats Àrabs Units seguint un enllaç. Mansoor va enviar l'enllaç al Citizen Lab de la Universitat de Toronto, que va investigar, amb la col·laboració de Lookout, trobar que si Mansoor hagués seguit l'enllaç, hauria trencat el seu telèfon i implantat el programari espia en ell, en una forma d'enginyeria social. [10]

Citizen Lab i Lookout van descobrir que l'enllaç descarregava programari per explotar tres vulnerabilitats de dia zero prèviament desconegudes i sense patentar en iOS. [11][12] Segons la seva anàlisi, el programari pot trencar un iPhone quan s'obre un URL maliciós, una forma d'atac coneguda com a phishing de llança. El programari s'instal·la i recull totes les comunicacions i ubicacions dels iPhones dirigits. El programari també pot recollir contrasenyes Wi-Fi. [13] Els investigadors es van adonar que el codi del programari feia referència a un producte del Grup NSO anomenat "Pegasusus" en materials de màrqueting filtrats. [14] Pegasusus havia sortit a la llum prèviament en una filtració de registres de Hacking Team, que indicava que el programari havia estat subministrat al govern de Panamà el 2015. [15] Citizen Lab i Lookout van notificar a l'equip de seguretat d'Apple, que va apedaçar els defectes en deu dies i va llançar una actualització per a iOS. [16] Un pegat per al macOS va ser llançat sis dies després. [17]

Pel que fa a l'extensió del tema, Lookout va explicar en una publicació al bloc: "Creiem que aquest programari espia ha estat en estat salvatge durant una quantitat significativa de temps basat en alguns dels indicadors dins del codi" i va assenyalar que el codi mostra signes d'una "taula de mapatge del nucli que té valors fins a iOS 7" (publicat el 2013). [18] The New York Times i The Times of Israel van informar que semblava que els Emirats Àrabs Units estaven utilitzant aquest programari espia ja el 2013. [19][20][21] Va ser utilitzat a Panamà per l'expresident Ricardo Martinelli de 2012 a 2014, que va establir el Consell de Seguretat Pública i Defensa Nacional per al seu ús. [22][23][24][25]

Cronologia

Diverses demandes pendents el 2018 van afirmar que NSO Group va ajudar els clients a operar el programari i, per tant, va participar en nombroses violacions dels drets humans iniciades pels seus clients. [21] Dos mesos després de l'assassinat i desmembrament del periodista de The Washington Post Jamal Khashoggi, un activista saudita de drets humans, al consolat de l'Aràbia Saudita a Istanbul, Turquia, el dissident saudita Omar Abdulaziz, un resident canadenc, va presentar una demanda a Israel contra NSO Group, acusant l'empresa de proporcionar al govern saudita el programari de vigilància per espiar-lo a ell i als seus amics, Incloent-hi Khashoggi. [26]

Al desembre de 2020, un programa d'investigació d'Al Jazeera The Hidden is More Immense va cobrir Pegasusus i la seva penetració en els telèfons de professionals i activistes dels mitjans de comunicació; i el seu ús per part d'Israel per escoltar tant opositors com aliats. [27][28]

Detalls tècnics

El programari espia es pot instal·lar en dispositius que executen certes versions d'iOS, el sistema operatiu mòbil d'Apple, així com alguns dispositius Android. [1] En lloc de ser una explotació específica, Pegasusus és un conjunt d'gestes que utilitza moltes vulnerabilitats en el sistema. Els vectors d'infecció inclouen fer clic als enllaços, a l'aplicació Fotos, a l'app Apple Music i a l'iMessage. Algunes de les gestes que utilitza Pegasusus són de clic zero, és a dir, es poden executar sense cap interacció de la víctima. Un cop instal·lat, s'ha informat que Pegasusus pot executar codi arbitrari, extreure contactes, registres de trucades, missatges, fotos, historial de navegació web, configuració,[29] així com recopilar informació d'aplicacions que inclouen, entre d'altres, aplicacions de comunicacions iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram i Skype. [30]

A l'abril de 2017, després d'un informe de Lookout, els investigadors de Google van descobrir el malware d'Android "que es creu que va ser creat per NSO Group Technologies" i el van anomenar Chrysaor (germà de Pegasusus en la mitologia grega). Segons Google, "Es creu que Chrysaor està relacionat amb el programari espia Pegasusus". [31] A la Cimera d'Analistes de Seguretat de 2017 celebrada per Kaspersky Lab, els investigadors van revelar que Pegasusus estava disponible per a Android a més d'iOS. La seva funcionalitat és similar a la versió per a iOS, però el mode d'atac és diferent. La versió d'Android intenta obtenir accés root (similar a jailbreaking a iOS); si falla, demana a l'usuari permisos que li permetin recollir almenys algunes dades. En aquell moment, Google va dir que només uns pocs dispositius Android havien estat infectats. [32]

Pegasusus s'amaga en la mesura del possible i s'autodestrueix en un intent d'eliminar proves si no pot comunicar-se amb el seu servidor d'ordres i control durant més de 60 dies, o si està en el dispositiu equivocat. Pegasus també pot autodestruir-se al comandament. [32] Si no és possible comprometre un dispositiu de destinació per mitjans més senzills, Pegasusus es pot instal·lar configurant un transceptor sense fil a prop d'un dispositiu de destinació o obtenint accés físic al dispositiu. [33]

Desenvolupament de capacitats

La primera versió de Pegasusus, que es va identificar el 2016, es basava en un atac de phishing de llança que requeria que l'objectiu fes clic en un enllaç maliciós en un missatge de text o correu electrònic. [33]

A l'agost de 2016, segons un antic empleat de NSO, la versió nord-americana de Pegasusus tenia capacitats d'1 clic per a tots els telèfons, excepte els antics models de Blackberry, que es podien infiltrar amb un atac de 0 clics. [34]

El 2019, WhatsApp va revelar que Pegasusus havia utilitzat una vulnerabilitat a la seva aplicació per llançar atacs de clic zero (el programari espia s'instal·laria al telèfon d'un objectiu trucant al telèfon de destinació; el programari espia s'instal·laria fins i tot si la trucada no fos contestada). [33]

Des de 2019, Pegasusus ha arribat a confiar en vulnerabilitats de l'iPhone iMessage per implementar programari espia. [33]

El 2020, Pegasusus va canviar cap a gestes de clic zero i atacs basats en xarxes. Aquests mètodes van permetre als clients entrar en telèfons de destinació sense requerir la interacció de l'usuari i sense deixar cap rastre detectable. [35][36]

Vulnerabilitats

Lookout va proporcionar detalls de les tres vulnerabilitats d'iOS:[18]

CVE-2016-4655: Fuita d'informació en el nucli - Una vulnerabilitat de mapatge de base del nucli que filtra informació a

l'atacant permetent-los calcular la ubicació del nucli a la memòria.
CVE-2016-4656: La corrupció de la memòria del nucli condueix a jailbreak - vulnerabilitats a nivell de nucli iOS de 32 i 64 bits que permeten a l'atacant trencar secretament el dispositiu i instal·lar programari de vigilància - detalls en referència. [37]
CVE-2016-4657: Corrupció de la memòria en el webkit - Una vulnerabilitat en el Safari WebKit que permet a l'atacant comprometre el dispositiu quan l'usuari fa clic en un enllaç.

El Projecte Zero de Google va documentar una altra explotació, anomenada FORCEDENTRY, el desembre de 2021. Segons els investigadors de Google, Pegasusus va enviar un iMessage als seus objectius que contenia el que semblaven ser imatges GIF, però que de fet contenia una imatge JBIG2. Una vulnerabilitat en la implementació d'Xpdf de JBIG2, reutilitzada en el programari operatiu per a telèfons iOS d'Apple, va permetre a Pegasusus construir una arquitectura de computadors emulada dins del flux JBIG2 que després es va utilitzar per implementar l'atac de clic zero. Apple va fixar la vulnerabilitat en iOS 14.8 al setembre de 2021 com AVE-2021-30860. [38]

A partir de juliol de 2021, Pegasusus probablement utilitza moltes gestes, algunes no enumerades en els CVEs anteriors. [1]

Xarxa de transmissió d'anonimització Pegasus
Amnistia Internacional va informar en la investigació de 2021 que Pegasusus utilitza una sofisticada infraestructura de comandament i control (C&C) per lliurar càrregues útils d'explotació i enviar ordres a objectius de Pegasusus. Hi ha almenys quatre iteracions conegudes de la infraestructura C&C, anomenada Pegasusus Anonymizing Transmission Network (PATN) pel grup NSO, cadascuna que abasta fins a 500 noms de domini, servidors DNS i altres infraestructures de xarxa. Segons els informes, el PATN utilitza tècniques com registrar alts nombres de ports per a la seva infraestructura en línia per evitar l'escaneig convencional d'Internet. PATN també utilitza fins a tres subdominis aleatoris únics per intent d'explotació, així com camins URL aleatoritzats. [1]

Ús per país
Tot i que Pegasusus es diu que està destinat a ser utilitzat contra criminals i terroristes,[9] també ha estat utilitzat per governs autoritaris i democràtics per espiar crítics i opositors. Un relator especial de l'ONU sobre la llibertat d'opinió va trobar que l'ús del programari espia per part de governs abusius podria "facilitar execucions i assassinats extrajudicials, sumàries o arbitraris, o desaparició forçada de persones". [40]

Armènia
Una vintena de ciutadans armenis van ser espiats a través del programari espia Pegasusus. L'expert en mitjans Arthur Papyan va dir que es dirigia a les figures clau de l'oposició i el govern: empleats del govern actuals i anteriors que coneixien secrets d'Estat valuosos i tenen influència política, inclòs l'exdirector del Servei de Seguretat Nacional i actual president del Partit Nacional de centredreta. Els experts locals sospitaven que eren atacats pel govern d'Armènia o Azerbaidjan, o potser tots dos. Papyan va dir que el grup NSO sembla estar trencant un telèfon i proporciona interfície per veure les dades obtingudes. El ministre d'alta tecnologia, Vahagn Khachaturyan, també va rebre una carta d'advertència d'Apple, va rebutjar la teoria que el partit d'espionatge podria ser l'actual govern armeni. [41]

Azerbaidjan
La llista de ciutadans espiats incloïa desenes de periodistes i activistes de l'Azerbaidjan. Es va al·legar que els seus telèfons mòbils van ser punxats. [42] El cap del servei àzeri de Radio Liberty /Radio Free Europe (Azadliq) Jamie Fly va expressar la seva ira quan es va revelar que els telèfons dels seus cinc empleats actuals i antics van ser punxats amb Pegasusus. [43]

Bahrain
Citizen Lab va revelar que el govern de Bahrain va utilitzar Pegasusus del Grup NSO per piratejar activistes, blocaires, membres de Waad (una societat política secular de Bahrain), un membre d'Al Wefaq (una societat política xiïta de Bahrain) i membres del Centre de Bahrain per als Drets Humans. Bahrain va adquirir l'accés al programari espia el 2017. Segons l'informe, els telèfons mòbils d'un total de nou activistes de drets humans van ser "hackejats amb èxit" entre juny de 2020 i febrer de 2021. Entre els hackejats hi havia tres membres de Waad, tres del BCHR, un d'Al Wefaq i dos dels dissidents exiliats que resideixen a Londres. El Citizen Lab va atribuir "amb alta confiança" que un operador de Pegasusus, LULU, va ser utilitzat pel govern de Bahrain per violar els telèfons d'almenys quatre dels nou activistes. [44][45]

Al gener de 2022, Bahrain va ser acusat d'utilitzar el programari espia Pegasusus per piratejar un defensor dels drets humans, Ebtisam al-Saegh. El telèfon de l'activista va ser piratejat almenys vuit vegades entre agost i novembre de 2019. Segons el Citizen Lab, després de l'intent de pirateria, al-Saegh es va enfrontar a incidents en què va ser

assetjada per les autoritats de Bahrain. Incloïa ser citat a una comissaria de policia, interrogatoris, amenaces de violació i agressions físiques i sexuals. L'atac va deixar el defensor dels drets humans en un estat de "por i terror diaris". [46]

Al febrer de 2022, una investigació de Citizen Lab i Amnistia Internacional va revelar que el programari espia Pegasusus es va utilitzar per infectar els dispositius d'un advocat, un periodista en línia i un conseller de salut mental a Bahrain. Els tres activistes van ser crítics amb les autoritats de Bahrain i van ser atacats amb Pegasusus entre juny i setembre de 2021. Un dels tres activistes es va mantenir en l'anonimat, mentre que els altres dos eren Mohammed al-Tajer i Sharifa Swar (consellera de salut mental). [47]

Estònia

Estònia va entrar en negociacions per adquirir Pegasusus el 2018 i havia fet un pagament inicial de 30 milions de dòlars per l'eina. Estònia esperava utilitzar l'eina contra els telèfons russos (presumiblement per reunir informació). Israel va aprovar inicialment l'exportació de Pegasus a Estònia, però després que un alt funcionari de defensa rus s'acostés a les agències de defensa israelianes i revelés que Rússia s'havia assabentat de les intencions d'Estònia d'obtenir Pegasusus, Israel va decidir prohibir a Estònia utilitzar Pegasus contra qualsevol número de telèfon rus (després d'un acalorat debat entre funcionaris israelians) per evitar danyar les relacions israelianes amb Rússia. [48]

Finlàndia

Al gener de 2022, el Ministeri d'Afers Estrangers finlandès va informar que diversos telèfons de diplomàtics finlandesos s'havien infectat amb el programari espia Pegasusus. [49]

Alemanya

Pegasusus és utilitzat per l'Oficina Federal de Policia Criminal d'Alemanya (BKA). BKA va adquirir Pegasusus el 2019 amb "el màxim secret", i malgrat els dubtes del seu consell legal. L'ús de Pegasusus per part de BKA va ser revelat més tard pels mitjans alemanys. [50]

Hongria

El govern de Viktor Orbán va autoritzar l'ús de Pegasusus per part de la intel·ligència hongaresa i els serveis d'aplicació de la llei per atacar els opositors polítics del govern. El govern d'Orban ha estat acusat d'utilitzar-lo per espiar membres dels mitjans de comunicació, així com contra l'oposició hongaresa. [51] Segons les troballes publicades el juliol de 2021, els periodistes i els gerents de les explotacions de mitjans semblen haver estat espiats pel govern hongarès amb Pegasusus. [52] Els números de telèfon d'almenys 10 advocats, almenys 5 periodistes i un polític de l'oposició van ser inclosos en una llista filtrada de possibles objectius de vigilància de Pegasusus. [53]

Al novembre de 2021, Lajos Kósa, cap d'un comitè parlamentari de defensa i aplicació de la llei, va ser el primer alt funcionari hongarès que va reconèixer que el Ministeri de l'Interior del país va comprar i va utilitzar Pegasusus. [54] Kósa va admetre que Hongria havia comprat i utilitzat Pegasus, afirmant que "no hi veig res objectable [...] les grans empreses tecnològiques duen a terme un seguiment molt més ampli dels ciutadans que l'Estat hongarès". [51]

Índia

Articles principals: Revelacions del projecte Pegasusus a l'Índia i escàndol de tafanejar whatsApp

A finals de 2019, Facebook va iniciar una demanda contra NSO, al·legant que Pegasusus havia estat utilitzat per interceptar les comunicacions de WhatsApp d'una sèrie d'activistes, periodistes i buròcrates a l'Índia, cosa que va provocar acusacions que el govern indi estava involucrat. [55][56][57] 17 persones, inclosos activistes de drets humans, acadèmics i periodistes, van confirmar a una publicació índia que havien estat atacats. [58]

Els números de telèfon de ministres indis, líders de l'oposició, exconsellers electorals i periodistes van ser trobats suposadament en una base de dades d'objectius de pirateria de NSO per Part del Projecte Pegasusus el 2021. [59][60][61] Números de telèfon d'activistes de Koregaon Bhima que tenien dades comprometedores implantades als seus ordinadors a través d'un hack trobat en una llista de números de telèfon de vigilància de Pegasusus. [62]

L'anàlisi forense digital independent duta a terme en 10 telèfons indis els números dels quals estaven presents en les dades mostrava signes d'un intent o èxit de hackeig de Pegasusus. Els resultats de l'anàlisi forense llançada mostren correlacions seqüencials entre l'hora i la data en què s'introdueix un número de telèfon a la llista i l'inici de la vigilància. La diferència sol oscil·lar entre uns minuts i un parell d'hores. [63]

11 números de telèfon associats amb una empleada del Tribunal Suprem de l'Índia i la seva família immediata, que va acusar l'excap de justícia de l'Índia, Ranjan Gogoi, d'assetjament sexual, també es troben en una base de dades que indica la possibilitat que els seus telèfons siguin tafanejats. [64][65]

Els registres també indiquen que els números de telèfon d'alguns dels principals actors polítics de Karnataka semblen haver estat seleccionats al voltant del moment en què s'estava duent a terme una intensa lluita de poder entre el Partit Bharatiya Janata i el govern estatal liderat pel Congrés Janata Dal el 2019. [66][67]

Israel

Ús de la policia israeliana

Al gener de 2022, es va informar que Pegasusus va ser utilitzat il·legalment per la policia israeliana per controlar ciutadans, així com ciutadans estrangers que van ser infectats accidentalment o intencionadament pel programari. La vigilància va ser ordenada per agents de policia d'alt rang, i es va dur a terme sense ordres ni supervisió judicial. [69] La base legal per a l'ús de programari espia contra els ciutadans és discutida. [70] La policia suposadament havia atacat civils no sospitosos de cap delicte, inclosos organitzadors de manifestants antigovernamentals, alcaldes, activistes de desfilades anti-LBGT, empleats d'empreses propietat del govern, associats d'un polític d'alt rang,[70] i antics empleats del govern. [69] En un cas, es va al·legar que la policia va atacar un activista que no era sospitós d'un delicte, suposadament per recopilar informació sobre els assumptes extramatrimonials de l'activista i utilitzar-la com a palanca. [70]

En alguns casos, Pegasusus va ser utilitzat per obtenir informació no relacionada amb una investigació en curs per ser utilitzada més tard per pressionar el tema d'una investigació. En alguns casos, la policia va utilitzar Pegasusus per obtenir informació incriminatòria dels dispositius dels sospitosos, i després va ocultar la font de la informació incriminatòria al·legant que exposaria actius d'intel·ligència. Tot i que la policia israeliana va negar formalment les acusacions en l'informe, alguns alts funcionaris de la policia han insinuat que les afirmacions eren certes. [73] L'informe va conduir a l'anunci d'una sèrie d'investigacions paral·leles sobre la conducta de la policia,[74] amb alguns funcionaris exigint una Comissió d'investigació. [75] Tot i que el fiscal general va llançar una investigació interna sobre les acusacions,[76] el Consell de Protecció de la Privadesa (que assessora el ministre de Justícia),[77] va exigir que es creés una comissió estatal d'investigació. [75]

L'1 de febrer, la policia va admetre que, de fet, hi havia un ús indegut del programari. El 7 de febrer, es va revelar que l'extensió generalitzada de la vigilància sense garanties incloïa polítics i funcionaris del govern, caps d'empreses, periodistes, activistes i fins i tot Avner Netanyahu, fill del llavors primer ministre, Benjamin Netanyahu. Això ha portat a noves crides a una investigació pública, incloent-hi el mateix comissari de policia Kobi Shabtai (nomenat gener de 2021), així com del ministre de l'Interior, Ayelet Shaked i altres. [79]

Més tard, el ministre de Seguretat Pública (el ministre responsable de la policia), Omer Bar-Lev, va anunciar que formarà una comissió d'investigació, que serà presidida per un jutge jubilat. Bar-Lev va subratllar que a aquesta comissió se li concediran essencialment tots els poders d'una comissió estatal (la formació de la qual requereix el suport total del gabinet), incloent-hi tenir l'autoritat per citar testimonis, "independentment de l'antiguitat", el testimoni de la qual es pot utilitzar en futurs processaments. Malgrat això, les crides a una comissió estatal van persistir de diversos excaps de ministeri que van ser atacats. L'endemà, l'interventor de l'Estat Matanyahu Englman, qualificant la crisi de "trepitjar els valors de la democràcia i la privacitat", va dir que la investigació iniciada per la seva oficina també serà extensa, i va afegir que no només inclourà la policia, sinó també el Ministeri de Justícia i l'Advocacia de l'Estat. [81]

Jordània

Al gener de 2022, el telèfon de l'advocada i activista Hala Ahed Deeb va ser atacat. [82]

Kazakhstan

Els activistes al Kazakhstan van ser atacats,[83] a més de funcionaris d'alt nivell, com Kassym-Jomart Tokayev, Askar Mamin i Bakytzhan Sagintayev. Entre els números kazaks atacats del 2000 hi havia el crític del govern Bakhytzhan Toregozhina, així com els periodistes Serikzhan Mauletbay i Bigeldy Gabdullin. La majoria d'aquestes víctimes estaven involucrades en un moviment cívic juvenil Oyan, Qazaqstan. [86]

Mèxic

Mèxic va ser el primer país a comprar Pegasusus. Les primeres versions de Pegasusus es van utilitzar per vigilar el telèfon de Joaquín Guzmán, conegut com El Chapo. El 2011, el president mexicà Felipe Calderón va trucar a NSO per agrair a la companyia el seu paper en la captura de Guzmán. [88][89] Quan es va filtrar una llista de 50.000 números de telèfon de possibles objectius de vigilància Pegasusus (seleccionats per governs de clients individuals) el 2021, un terç d'ells eren mexicans. [87]

Orientació a científics i activistes de la salut

El 2017, investigadors de Citizen Lab van revelar que els enllaços d'explotació de NSO podrien haver estat enviats a científics mexicans i activistes de salut pública. [90] Els objectius van donar suport a mesures per reduir l'obesitat infantil, inclosa la "Taxa de Refrescos" de Mèxic. [91]

Segrest massiu d'Iguala 2014

Al juliol de 2017, l'equip internacional reunit per investigar el segrest massiu d'Iguala de 2014 es va queixar públicament que pensaven que estaven sent vigilats pel govern mexicà. [92] Van declarar que el govern mexicà va utilitzar Pegasusus per enviar-los missatges sobre funeràries que contenien enllaços que, quan es feien clic, permetien al govern escoltar subreptíciament els investigadors. [92] El govern mexicà ha negat repetidament qualsevol pirateria no autoritzada. [92]

Assassinat del periodista Cecilio Pineda Birto

Cecilio Pineda Birto, un periodista independent mexicà, va ser assassinat per sicaris mentre descansava en una hamaca per un rentat de cotxes. Brito havia estat informant sobre els vincles entre els polítics locals i les organitzacions criminals, i havia rebut amenaces de mort anònimes durant les setmanes anteriors a l'assassinat; aproximadament al mateix temps, el seu número de telèfon va ser seleccionat com a possible objectiu per a la vigilància de Pegasusus per un client mexicà de Pegasusus. El programari espia Pegasusus podria haver estat utilitzat per determinar la ubicació de Brito per dur a terme l'impacte geolocalitzant el seu telèfon; No obstant això, el desplegament de Pegasusus al seu telèfon no va poder ser confirmat, ja que el seu telèfon va desaparèixer del lloc de l'assassinat. [93]

Ús dels càrtels mexicans de la droga

Pegasusus ha estat utilitzat per càrtels de la droga i actors governamentals entrellaçats amb càrtels per atacar i intimidar periodistes mexicans. [94]

Altre

Una vídua de la reconeguda periodista mexicana va ser objectiu d'un intent d'atac de Pegasusus 10 dies després de l'assassinat del seu marit. [95]

Marroc
El 2019, dos activistes marroquís prodemocràcia van ser notificats per WhatsApp que els seus telèfons havien estat compromesos amb Pegasusus. [58]

Al juny de 2020, una investigació d'Amnistia Internacional va al·legar que el periodista marroquí Omar Radi va ser blanc del govern marroquí utilitzant el programari espia israelià Pegasusus. El grup de drets humans va afirmar que el periodista va ser atacat tres vegades i espiat després que el seu dispositiu estigués infectat amb una eina de NSO. Mentrestant, Amnistia Internacional també va afirmar que l'atac es va produir després que el grup NSO actualitzés la seva política al setembre de 2019. [96]

Al juliol de 2021, el Marroc havia atacat més de 6.000 telèfons algerians, inclosos els de polítics i alts funcionaris militars, amb el programari espia. [97][98]

Panamà
El president de Panamà Ricardo Martinelli va tractar personalment d'obtenir eines de ciberespionatge després de la seva elecció el 2009. Després d'un rebuig dels Estats Units el 2009, Martinelli va buscar amb èxit aquestes eines als venedors israelians, expressant el seu interès a adquirir una eina capaç de piratejar telèfons mòbils en una reunió privada el 2010 amb el primer ministre israelià Netanyahu. El 2012, els sistemes NSO es van instal·lar a la ciutat de Panamà. L'equip va ser posteriorment àmpliament utilitzat per a l'espionatge intern i estranger il·lusòria, incloent-hi espionatge a opositors polítics, magistrats, líders sindicals i competidors empresarials, amb Martinelli suposadament anant tan lluny com per ordenar la vigilància de la seva amant utilitzant Pegasusus. [4]

Palestina
Els telèfons mòbils de sis activistes palestins van ser piratejats utilitzant Pegasusus amb alguns dels atacs que suposadament es van produir ja al juliol de 2020, segons un informe de Front Line Defenders. [99]

Polònia
Les llicències Pegasusus van ser acordades entre Benjamin Netanyahu i Beata Szyd?o el juliol de 2017. Citizen Lab va

revelar que diversos membres de grups polítics de l'oposició a Polònia van ser hackejats per programari espia Pegasusus, plantejant preguntes alarmants sobre l'ús del programari per part del govern polonès. Un advocat que representava els grups de l'oposició polonesa i un fiscal involucrat en un cas contra el partit governant Llei i Justícia també es van veure compromesos. [101]

Al desembre de 2021, Citizen Lab va anunciar que Pegasusus va ser utilitzat contra l'advocat Roman Giertych i la fiscal Ewa Wrzosek, tots dos crítics amb el govern governant llei i justícia (PiS), amb el telèfon de Giertych patint 18 intrusions. [102] 33 hacks al telèfon de Krzysztof Brejza, senador de la Plataforma Cívica (PO) de l'oposició, van ser descoberts,[103] i confirmats per Amnistia Internacional. [104] Conduint a les eleccions parlamentàries europees i poloneses de 2019, els missatges de text de Brejza van ser robats mentre liderava la campanya dels partits de l'oposició. Els textos van ser manipulats per mitjans estatals, en particular TVP, i utilitzats en una campanya de desprestigi contra l'oposició. Això va portar al Senat polonès a iniciar una investigació sobre el desplegament del programari espia. [107]

El 25 de gener de 2022, Citizen Lab va confirmar més víctimes, incloent Micha? Ko?odziejczak del moviment agrari Agrounia, i Tomasz Szwejgiert, periodista i presumpte ex associat de la CBA. [108][109]

Segons la Sindicatura de Comptes (NIK), 544 dels dispositius dels seus empleats estaven sota vigilància més de 7.300 vegades, alguns podrien estar infectats amb Pegasusus. [110]

Rwanda
Una investigació conjunta de The Guardian i Le Monde va ser atacada amb Pegasusus. [111]

Aràbia Saudita
Al desembre de 2020, es va informar que l'Aràbia Saudita i els Emirats Àrabs Units van desplegar una explotació d'iMessage Pegasusus amb zero clics contra dos periodistes amb seu a Londres i 36 periodistes a la cadena de televisió Al Jazeera a Qatar. [35][36]

Jamal Khashoggi

Pegasus va ser utilitzat per l'Aràbia Saudita per espiar Jamal Kashoggi, que més tard va ser assassinat a Turquia. A l'octubre de 2018, Citizen Lab va informar sobre l'ús de programari NSO per espiar el cercle intern de Jamal Khashoggi just abans del seu assassinat. L'informe d'octubre de Citizen Lab[113] va declarar amb alta confiança que Pegasus de la NSO havia estat col·locat a l'iPhone del dissident saudita Omar Abdulaziz, un dels confidents de Khashoggi, mesos abans. Abdulaziz va afirmar que el programari va revelar les "crítiques privades de Khashoggi a la família reial saudita", que segons Abdulaziz "va jugar un paper important" en la mort de Khashoggi. [114]

Al desembre de 2018, una investigació del New York Times va concloure que el programari Pegasusus va jugar un paper en l'assassinat de Khashoggi, amb un amic de Khashoggi afirmant en una presentació que les autoritats saudites havien utilitzat el programari de la policia israeliana per espiar el dissident. [115] El ceo de NSO, Shalev Hulio, va declarar que l'empresa no havia estat involucrada en el "terrible assassinat", però es va negar a comentar els informes que havia viatjat personalment a la capital saudita, Riad, per a una venda de Pegasusus de 55 milions de dòlars. [116]

El 2021, van sorgir acusacions que el programari també podria haver estat utilitzat per espiar membres de la família de Kashoggi. [117]

Direcció: Jeff Bezos

Pegasusus també va ser utilitzat per espiar Jeff Bezos després que Mohammed bin Salman, el príncep hereu de l'Aràbia Saudita, intercanviés missatges amb ell que explotaven vulnerabilitats llavors desconegudes a WhatsApp. [118][119]

El periodista Ben Hubbard

Un corresponsal del New York Times que cobria l'Orient Mitjà, Ben Hubbard, va revelar a l'octubre de 2021 que l'Aràbia Saudita va utilitzar el programari Pegasusus del Grup NSO per piratejar el seu telèfon. Hubbard va ser atacat repetidament durant un període de tres anys entre juny de 2018 i juny de 2021 mentre informava sobre l'Aràbia Saudita i escrivia un llibre sobre el príncep hereu saudita Mohammed bin Salman. Hubbard va ser possiblement l'objectiu d'escriure el llibre sobre el príncep hereu, i per la seva participació en revelar l'intent de pirateria i vigilància dels Emirats Àrabs Units del Projecte Raven. Els saudites van intentar mirar la informació personal de Hubbard dues vegades el

2018, una a través d'un missatge de text sospitós i l'altra a través d'un missatge de WhatsApp àrab convidant-lo a una protesta en una ambaixada saudita a Washington.

Dos atacs més van ser llançats contra ell el 2020 i 2021 utilitzant les capacitats de pirateria de clic zero. Finalment, el 13 de juny de 2021, un iPhone pertanyent a Hubbard va ser piratejat amb èxit utilitzant l'explotació FORCEDENTRY. Citizen Lab va dir amb "alta confiança" que els quatre atacs van ser intentats utilitzant Pegasusus. [120][121]

Altres objectius

Un altre exiliat saudita, Omar Abdulaziz, al Canadà, va ser identificat per McKinsey & Company com un dissident influent, i per tant tenia dos germans empresonats per les autoritats saudites, i el seu telèfon mòbil va ser piratejat per Pegasusus. [112][122]

Espanya
Segons una investigació de The Guardian i El País, el govern d'Espanya va utilitzar el programari Pegasusus per comprometre els telèfons de diversos polítics actius en el moviment independentista català, entre ells el president del Parlament de Catalunya Roger Torrent, i l'exdiputada al Parlament de Catalunya Anna Gabriel i Sabaté. [123]

Togo
Una investigació conjunta de The Guardian i Le Monde va al·legar que el programari Pegasusus es va utilitzar per espiar sis crítics del govern a Togo. [111]

Uganda
S'ha informat que Muhoozi Kainerugaba va negociar un acord per utilitzar Pegasusus a Uganda, pagant entre 10 i 20 milions de dòlars el 2019. El programari es va utilitzar més tard per piratejar els telèfons d'11 diplomàtics i empleats nord-americans de l'ambaixada dels Estats Units a Uganda en algun moment durant 2021. (124)

Ucraïna
Almenys des del 2019, Ucraïna havia intentat obtenir Pegasusus en el seu esforç per contrarestar el que veia com una amenaça creixent d'agressió i espionatge russos, però, Israel havia imposat una prohibició gairebé total de la venda d'armes a Ucraïna (que també abastava eines de ciberespionatge), recelós de vendre Pegasus a estats que utilitzarien l'eina contra Rússia per no danyar les relacions amb Rússia. A l'agost de 2021, en un moment en què les tropes russes s'acumulaven a la frontera ucraïnesa, Israel va rebutjar de nou una sol·licitud d'una delegació ucraïnesa que demanava obtenir Pegasus; Segons un funcionari ucraïnès familiaritzat amb l'assumpte, Pegasusus podria haver proporcionat suport crític en l'esforç d'Ucraïna per controlar l'activitat militar russa. Arran de la invasió russa d'Ucraïna el 2022, funcionaris ucraïnesos van retreure el tebi suport d'Israel a Ucraïna i els esforços israelians per mantenir relacions amistoses amb Rússia. [48]

Emirats Àrabs Units
Al desembre de 2020, es va informar que l'Aràbia Saudita i els Emirats Àrabs Units van desplegar una explotació d'iMessage Pegasusus amb zero clics contra dos periodistes amb seu a Londres i 36 periodistes a la cadena de televisió Al Jazeera a Qatar. [35][36]

Els Emirats Àrabs Units van utilitzar Pegasusus per espiar els membres del govern iemenita recolzat per l'Aràbia Saudita, segons una investigació publicada al juliol de 2021. Els Emirats Àrabs Units van utilitzar el programari espia per vigilar i espiar els ministres del govern internacionalment reconegut del president Abdrabbuh Mansur Hadi, inclòs el president iemenita i els seus familiars, l'exprimer ministre Ahmed Obaid Bin Dagher, l'exministre d'Afers Exteriors Abdulmalik Al-Mekhlafi i l'actual ministre de Joventut i Esports, Nayef al-Bakri. [125]

El 24 de setembre de 2021, The Guardian va informar que el telèfon d'Alaa al-Siddiq, director executiu d'ALQST, que va morir en un accident de cotxe a Londres el 20 de juny de 2021, estava infectat amb el programari espia Pegasusus durant 5 anys fins al 2020. Citizen Lab va confirmar que l'activista dels Emirats va ser hackejat per un client del govern del Grup NSO d'Israel. El cas va representar una tendència preocupant per als activistes i dissidents, que van escapar dels Emirats Àrabs Units per viure en la relativa seguretat, però mai van estar fora de l'abast de Pegasusus. (126)

A l'octubre de 2021, el Tribunal Suprem britànic va dictaminar que agents de Mohammed bin Rashid Al Maktoum van utilitzar Pegasusus per piratejar els telèfons de la seva (ex)esposa, la princesa Haya bint Hussein, els seus advocats (inclosa la baronessa Fiona Shackleton), una assistent personal i dos membres del seu equip de seguretat a l'estiu de 2020. El tribunal va dictaminar que els agents van actuar "amb l'autoritat expressa o implícita" del xeic; Va negar tenir coneixement del hacking. La sentència es referia a la pirateria com a "violacions en sèrie del dret penal intern del Regne

Unit", "en violació del dret comú fonamental i els drets del TEDH", "interferència amb el procés d'aquest tribunal i l'accés de la mare a la justícia" i "abús de poder" per part d'un cap d'Estat. NSO s'havia posat en contacte amb un intermediari a l'agost de 2020 per informar la princesa Haya del hack i es creu que va rescindir el seu contracte amb els Emirats Àrabs Units. (127)

El 7 d'octubre de 2021, el Grup NSO va declarar que havia rescindit el seu contracte amb els Emirats Àrabs Units per utilitzar la seva eina de programari espia Pegasusus després de la sentència del Tribunal Suprem del Regne Unit que el governant de Dubai va fer un ús indegut del programari Pegasusus de l'empresa per espiar la seva exdona i els seus assessors legals. (128)

El 2022, les fonts van revelar que una unitat de mubadala investment company d'Abu Dhabi, Mubadala Capital, va ser un dels majors inversors en el fons de capital privat Novalpina Capital de 1.000 milions d'euros, que va comprar el Grup NSO el 2019. Des de llavors, Mubadala ha estat inversor en la firma amb el seu compromís de 50 milions d'euros, adquirint un seient en el comitè dels majors inversors del fons de renda variable. Periodistes, defensors dels drets humans i les dones de la família reial de Dubai van ser hackejats utilitzant el programari espia Pegasusus durant el mateix temps. [129]

Regne Unit
A l'abril de 2022, Citizen Lab va publicar un informe que afirmava que 10 treballadors de Downing Street havien estat atacats per Pegasusus, i que els Emirats Àrabs Units eren sospitosos d'originar els atacs el 2020 i 2021. [130]

Estats Units
NSO Group va presentar el seu programari espia a l'Administració d'Aplicació de Drogues (DEA), que es va negar a comprar-lo a causa del seu alt cost. (131)

A l'agost de 2016, NSO Group (a través de la seva filial nord-americana Westbridge) va presentar la seva versió nord-americana de Pegasusus al Departament de Policia de San Diego (SDPD). En el material de màrqueting, Westbridge va emfatitzar que l'empresa té la seu als Estats Units i és majoritàriament propietat d'una empresa matriu nord-americana. Un sergent de SDPD va respondre al to de vendes amb "sona increïble". El SDPD es va negar a comprar el programari espia, ja que era massa car. [34]

El programari espia Pegasusus va ser trobat el 2021 en els iPhones d'almenys nou empleats del Departament d'Estat dels Estats Units. El govern dels Estats Units va incloure a la llista negra del Grup NSO per aturar el que va anomenar "repressió transnacional". (133]

Al desembre de 2021, AP va informar que 11 empleats del Departament d'Estat dels Estats Units estacionats a Uganda tenien els seus iPhones piratejats amb Pegasusus. (134)

Al gener de 2022 es va informar que l'Oficina Federal d'Investigació (FBI) havia comprat en secret el programari espia Pegasusus el 2019 i també se li va donar una demostració de Phantom, una eina més nova que podria piratejar números de telèfon nord-americans. Van considerar l'ús d'ambdues eines per a la vigilància interna als Estats Units. El que suposadament va conduir a discussions entre l'FBI i el Departament de Justícia dels Estats Units que finalment van portar a l'FBI a decidir no utilitzar-lo i a tots els programaris espia de la NSO el 2021. No obstant això, tot i pronunciar-se en contra d'utilitzar-lo, l'equip Pegasusus encara està en possessió de l'FBI en una instal·lació de Nova Jersey. [135]

Iemen
L'anàlisi forense del telèfon mòbil de l'investigador independent de l'ONU Kamel Jendoubi va revelar el 20 de desembre de 2021 que va ser atacat utilitzant programari espia mentre investigava crims de guerra al Iemen. Jendoubi va ser atacat mentre examinava possibles crims de guerra al Iemen. El número de mòbil de Jendoubi també es va trobar a la base de dades filtrada del Projecte Pegasusus. Segons les dades, Jendoubi era un dels objectius potencials d'un dels clients de NSO Group durant molt de temps, l'Aràbia Saudita. No obstant això, el portaveu de la NSO va negar Kamel Jendoubi com cap dels objectius del seu client. (137)

Organitzacions internacionals
Unió Europea
A l'abril de 2022, segons dos funcionaris de la UE i la documentació obtinguda per Reuters, el comissari de Justícia europeu Didier Reynders i altres funcionaris de la Comissió Europea havien estat blanc del programari de la NSO. La comissió es va assabentar d'això després que Apple notifiqués a milers d'usuaris d'iPhone al novembre de 2021 que van ser atacats per hackers patrocinats per l'estat. Segons les mateixes dues fonts, els experts en TI van examinar alguns dels telèfons intel·ligents, però els resultats no van ser concloents. (138)

Projecte Pegasusus
Article principal: Projecte Pegasusus (investigació)

Una filtració d'una llista de més de 50.000 números de telèfon que es creu que han estat identificats com els de persones d'interès per clients de NSO des de 2016 es va posar a disposició de l'organització sense ànim de lucre Forbidden Stories i Amnistia Internacional, amb seu a París. Van compartir la informació amb disset mitjans de comunicació en el que s'ha anomenat Projecte Pegasusus, i es va dur a terme una investigació de mesos de durada, que es va informar des de mitjans de juliol de 2021. El Projecte Pegasusus va comptar amb la participació de 80 periodistes dels mitjans de comunicació com The Guardian (Regne Unit), Radio France i Le Monde (França), Die Zeit i Süddeutsche Zeitung (Alemanya), The Washington Post (Estats Units), Haaretz (Israel), Aristegui Noticias, Proceso (Mèxic), el Projecte d'informació sobre el crim organitzat i la corrupció, Knack, Le Soir, The Wire,[139] Daraj,[140] Direkt36 (Hongria),[141] i Frontline. Es va trobar evidència que molts telèfons amb números a la llista havien estat objectius del programari espia Pegasusus. [9][143] No obstant això, el CEO de NSO Group va afirmar categòricament que la llista en qüestió no té relació amb ells, la font de les acusacions no es pot verificar com a fiable. "Això és un intent de construir alguna cosa sobre una falta boja d'informació ... Hi ha alguna cosa fonamentalment malament en aquesta investigació". (144)

La intel·ligència francesa (ANSSI) va confirmar que s'havia trobat programari espia Pegasusus als telèfons de tres periodistes, entre ells un periodista de France 24, en la que va ser la primera vegada que una autoritat independent i oficial va corroborar les conclusions de la investigació. (145)

El 26 de gener de 2022, els informes van revelar que els telèfons mòbils de Lama Fakih, un ciutadà nord-americà-libanès i director de crisi i conflicte de Human Rights Watch, van ser hackejats repetidament per un client de NSO Group en un moment en què estava investigant la catastròfica explosió d'agost de 2020 que va matar més de 200 persones a Beirut. (146)

Al juliol de 2021, una investigació conjunta duta a terme per disset organitzacions de mitjans de comunicació, va revelar que el programari espia Pegasusus es va utilitzar per atacar i espiar caps d'Estat, activistes, periodistes i dissidents, permetent "violacions de drets humans a tot el món a gran escala". La investigació es va iniciar després d'una filtració de 50.000 números de telèfon de possibles objectius de vigilància. Amnistia Internacional va dur a terme anàlisis forenses de telèfons mòbils de possibles objectius. La investigació va identificar 11 països com a clients de NSO: Azerbaidjan, Bahrain, Hongria, Índia, Kazakhstan, Mèxic, Marroc, Ruanda, Aràbia Saudita, Togo i els Emirats Àrabs Units. La investigació també va revelar que periodistes de diversos mitjans de comunicació com Al Jazeera, CNN, Financial Times, Associated Press, The New York Times, The Wall Street Journal, Bloomberg News i Le Monde. Van ser atacats i identificats almenys 180 periodistes de 20 països que van ser seleccionats per a l'objectiu amb programari espia de NSO entre 2016 i juny de 2021. [147][148]

Reaccions
Resposta del grup NSO
En resposta als informes d'agost de 2016 sobre un atac d'un activista àrab, NSO Group va declarar que proporcionen "als governs autoritzats tecnologia que els ajuda a combatre el terror i la delinqüència", tot i que el Grup li va dir que no tenien coneixement de cap incident. (149]

Escepticisme del programa bug-bounty
Després de les notícies, els crítics van afirmar que el programa de recompenses d'errors d'Apple, que recompensa la gent per trobar defectes en el seu programari, podria no haver ofert prou recompenses per evitar que les gestes es venguin al mercat negre, en lloc de ser reportat de nou a Apple. Russell Brandom de The Verge va comentar que la recompensa oferta en el programa de recompenses d'errors d'Apple arriba als 200.000 dòlars, "només una fracció dels milions que es gasten regularment per a les gestes d'iOS al mercat negre". A continuació, es pregunta per què Apple no "passa el seu camí fora de les vulnerabilitats de seguretat?", però també escriu que "tan aviat com es van informar de les vulnerabilitats [de Pegasusus], Apple les va apedaçar, però queden molts altres errors. Mentre que les empreses de programari espia veuen una compra d'explotació com un pagament únic per anys d'accés, la recompensa d'Apple s'ha de pagar cada vegada que aparegui una nova vulnerabilitat".

Brandom també va escriure; "Els mateixos investigadors que participen en la recompensa d'errors d'Apple podrien guanyar més diners venent les mateixes troballes a un corredor d'explotació". Va acabar l'article escrivint; "És difícil dir quants danys podrien haver causat si Mansoor hagués fet clic a l'enllaç de programari espia... L'esperança és que, quan el proper investigador trobi el següent error, aquest pensament importa més que els diners". [150]

Vegeu també

DROPOUTJEEP
RCSAndroid de Hacking Team
Llista de programes de spyware

Referències

^ Jump up to:un b c d e f "Forensic Methodology Report: How to catch NSO Group's Pegasusus". www.amnesty.org. 18 de juliol de 2021. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ Timberg, Craig; Albergotti, Reed; Guéguen, Elodie (19 de juliol de 2021). "Malgrat el bombo, la seguretat de l'iPhone no coincideix amb el programari espia de NSO: la investigació internacional troba 23 dispositius Apple que van ser piratejats amb èxit". El Washington Post. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ Cox, Josep (12 de maig de 2020). "NSO Group va llançar tecnologia de pirateria telefònica a la policia nord-americana". Vici. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ Jump up to:un b c Bergman, Ronen; Mazzetti, Mark (28 de gener de 2022). "La batalla pel ciberweapon més poderós del món" El New York Times. ISSN 0362-4331. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ Buquet, Jonathan (19 de maig de 2019). "Puc tenir una paraula sobre... Programari espia Pegasusus". El guardià. Arxivat de l'original el 26 de gener de 2021. [Consulta: 18 juliol 2021c'.
^ Jump up to:un b Franceschi-Bicchierai, Lorenzo (26 d'agost de 2016). "Hackers del govern capturats utilitzant una eina espia d'iPhone sense precedents" Placa base. Vicemèdia. Arxivat de l'original el 3 de setembre de 2020. [Consulta: 15 maig 2019'.
^ "Amb l'encoratjament d'Israel, NSO va vendre programari espia als Emirats Àrabs Units i altres estats del Golf". Haaretz. Arxivat de l'original el 23 d'agost de 2020. [Consulta: 23 agost 2020'.
^ "Què és el programari espia Pegasusus i com pirateja els telèfons?" El guardià. 18 de juliol de 2021. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ Jump up to:un b c Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David; Cutler, Sam (18 de juliol de 2021). "Revelat: la filtració descobreix l'abús global d'armes de cibervigilància". L'observador. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 18 juliol 2021c'.
^ Lee, Dave (26 d'agost de 2016). "Qui són els hackers que van trencar l'iPhone?" Notícies de la BBC. Arxivat de l'original el 19 de juliol de 2018. [Consulta: 21 juny 2018'.
^ Marczak, Bill; Scott-Railton, John (24 d'agost de 2016). "The Million Dollar Dissident: l'iPhone Zero-Days de NSO Group utilitzat contra un defensor dels drets humans dels Emirats Àrabs Units". Laboratori Ciutadà. Arxivat de l'original el 17 de desembre de 2016. [Consulta: 25 març 2017'.
^ Anàlisi Tècnica de Pegasusus Spyware (PDF) (Informe tècnic). Mirador. 25 d'agost de 2016. Arxivat (PDF) de l'original el 19 de febrer de 2022. [Consulta: 25 agost 2016'.
^ Fox-Brewster, Thomas (25 d'agost de 2016). "Tot el que sabem sobre NSO Group: els espies professionals que van piratejar iPhones amb un sol text". Forbes. Arxivat de l'original el 26 d'agost de 2016. [Consulta: 25 agost 2016'.
^ Lee, Dave (26 d'agost de 2016). "Qui són els hackers que van trencar l'iPhone?" Notícies de la BBC. Arxivat de l'original el 30 de juliol de 2019. [Consulta: 26 agost 2016'.
^ Rodríguez, Rolando B.; Díaz, Juan Manuel (7 d'agost de 2015). "Abren sumario en caso Hacking Team". La Prensa (Ciutat de Panamà). Arxivat de l'original el 28 de març de 2019. [Consulta: 25 agost 2016'.
^ "Sobre el contingut de seguretat d'iOS 9.3.5" Apple Inc. 25 d'agost de 2016. Arxivat de l'original el 25 de setembre de 2019. [Consulta: 25 agost 2016'.
^ "Sobre el contingut de seguretat de l'actualització de seguretat 2016-001 El Capitan i actualització de seguretat 2016-005 Yosemite" Apple Inc. 1 de setembre de 2016. Arxivat de l'original el 25 de setembre de 2019. [Consulta: 1 setembre 2016'.
^ Jump up to:un b "Atac mòbil sofisticat i persistent contra objectius d'alt valor en iOS". Recerca. 25 d'agost de 2016. Arxivat de l'original el 17 de desembre de 2016. [Consulta: 21 desembre 2016'.
^ Kirkpatrick, David D.; Ahmed, Azam (31 d'agost de 2018). "Hackejar un príncep, un emir i un periodista per impressionar un client" El New York Times. Arxivat de l'original el 24 de maig de 2019. [Consulta: 31 agost 2018'.
^ Perlroth, Nicole (2 de setembre de 2016). "Com les empreses de tecnologia espia deixen que els governs ho vegin tot en un telèfon intel·ligent". El New York Times. Arxivat de l'original el 14 de maig de 2019. [Consulta: 31 agost 2018'.
^ Jump up to:un b "Les demandes afirmen que l'empresa israeliana de programari espia va ajudar el règim dels Emirats Àrabs Units a piratejar els telèfons dels opositors", va dir. Els temps d'Israel. 31 d'agost de 2018. Arxivat de l'original el 25 de maig de 2019. [Consulta: 31 agost 2018'.
^ "El polèmic pasado de Pegasusus en Panamá | la Prensa Panamá". 31 d'octubre de 2019. Arxivat de l'original el 24 de juliol de 2021. [Consulta: 24 juliol 2021c'.
^ "¿Qué es el sistema Pegasusus?". Arxivat de l'original el 24 de juliol de 2021. [Consulta: 24 juliol 2021c'.
^ "NSO Group i el seu Pegasusus, el programari que va fer en problemes judicials a un expresident panameny". July

19, 2021. Archived from the original on July 24, 2021. Retreu July 24, 2021.
^ "'Martinelli pidió disco duro de Pegasusus' | la Prensa Panamá". 8 de juny de 2019. Arxivat de l'original el 24 de juliol de 2021. [Consulta: 24 juliol 2021c'.
^ Boot, Max (5 de desembre de 2018). "Una empresa tecnològica israeliana està venent programari espia a dictadors, traint els ideals del país", ha afegit. El Washington Post. Arxivat de l'original el 19 d'abril de 2019. [Consulta: 19 abril 2019 no—consulta: 19 abril 2019.2019.20222.
^ "Els periodistes d'Al Jazeera van ser hackejats a través de programari espia de NSO Group". Notícies de la BBC. 21 de desembre de 2020. Arxivat de l'original el 9 de març de 2021. [Consulta: Març 10, 2021 no».2021
^ "Periodistes d'Al Jazeera van piratejar utilitzant el programari espia d'una empresa israeliana". Al Jazeera. Arxivat de l'original el 10 de març de 2021. [Consulta: Març 10, 2021 no».2021
^ Perlroth, Nicole (25 d'agost de 2016). "Els usuaris d'iPhone insten a actualitzar el programari després que es trobin errors de seguretat". El New York Times. Arxivat de l'original el 29 de maig de 2019. [Consulta: 21 desembre 2016'.
^ Fox-Brewster, Thomas (25 d'agost de 2016). "Tot el que sabem sobre NSO Group: els espies professionals que van piratejar iPhones amb un sol text". Forbes. Arxivat de l'original el 29 de maig de 2019. [Consulta: 21 desembre 2016'.
^ Conserves riques; Jason Woloz; Neel Mehta; Ken Bodzak; Wentao Chang; Megan Ruthven. "Una investigació de Chrysaor Malware a Android" Blog de desenvolupadors d'Android. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ Jump up to:un b John Snow (17 d'agost de 2017). "Pegasusus: l'últim programari espia per a iOS i Android" Diari Kaspersky. Arxivat de l'original el 4 de desembre de 2019. [Consulta: 4 desembre 2019'.
^ Jump up to:un b c d "Què és el programari espia Pegasusus i com pirateja els telèfons?" El guardià. 18 de juliol de 2021. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 1 febrer 2022t'.
^ Jump up to:un b "NSO Group va llançar tecnologia de pirateria telefònica a la policia nord-americana". www.vice.com. Arxivat de l'original el 30 de gener de 2022. [Consulta: 1 febrer 2022t'.
^ Jump up to:un b c "L'informe acusa l'Aràbia Saudita i els Emirats Àrabs Units de piratejar probablement telèfons de més de tres dotzenes de periodistes a Londres, Qatar", va dir. El Washington Post. Arxivat de l'original el 18 de desembre de 2021. [Consulta: 20 desembre 2020'.
^ Jump up to:un b c "The Great iPwn: Periodistes hackejats amb sospites de NSO Group iMessage 'Zero-Click' Exploit" Explota. El laboratori ciutadà. 20 de desembre de 2020. Arxivat de l'original el 30 de gener de 2022. [Consulta: 20 desembre 2020'.
^ Esser, Stefan (5 de setembre de 2016). "Pegasusus iOS Kernel Vulnerability Explained – Part 2" SektionEins GmbH. Arxivat de l'original el 31 d'agost de 2019. [Consulta: 31 agost 2019'.
^ Cervesa, Ian; Groß, Samuel (15 de desembre de 2021). "Projecte Zero: Una immersió profunda en una explotació de l'iMessage de zero clics NSO: Execució remota de codi". Projecte Zero de Google. Arxivat de l'original el 16 de desembre de 2021. [Consulta: 16 desembre 2021 no—consulta: 16 desembre 2021.2021.2021.20
^ "El fitxer NSO: una llista completa (actualització) d'individus dirigits amb programari espia Pegasusus". Haaretz. Arxivat de l'original el 31 de gener de 2022. [Consulta: Gener 31, 2022.'.
^ "Els grups de drets humans insten la UE a prohibir la NSO per l'ús per part dels clients del programari espia Pegasusus". El guardià. 3 de desembre de 2021. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ "Figures clau en l'oposició i el poder de Xipre han estat blanc d'un programa d'espionatge". Emissora de ràdio Free Europe/Freedom (en armeni). Arxivat de l'original el 25 de novembre de 2021. [Consulta: 25 novembre 2021 no—consulta: 25 novembre 2021.2021.2021.20
^ "Apple NSO Group-u m?hk?m?y? verir". Radiosu Azadl?q (en àzeri). Arxivat de l'original el 25 de novembre de 2021. [Consulta: 25 novembre 2021 no—consulta: 25 novembre 2021.2021.2021.20
^ El president de la R/C, "Europa Lliure/Llibertat", condemna l'espionatge de periodistes del servei àzeri amb el programa Pegasusus. Emissora de ràdio Free Europe/Freedom (en armeni). Arxivat de l'original el 25 de novembre de 2021. [Consulta: 25 novembre 2021 no—consulta: 25 novembre 2021.2021.2021.20
^ "From Pearl to Pegasusus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits" (Del perla a Pegasusus): el govern de Bahrain pirateja els activistes amb NSO Group Zero Click iPhone Exploits. El laboratori ciutadà. 24 d'agost de 2021. Arxivat de l'original el 2 de gener de 2020. [Consulta: 24 agost 2021c'.
^ "Els telèfons de nou activistes de Bahrain van ser hackejats amb programari espia de la NSO. El guardià. 24 d'agost de 2021. Arxivat de l'original el 2 de gener de 2020. [Consulta: 24 agost 2021c'.
^ "Dues dones activistes a Bahrain i Jordània van piratejar el programari espia de la NSO. El guardià. 17 de gener de 2022. Arxivat de l'original el 24 de gener de 2022. [Consulta: Gener 17, 2022.'.
^ "Bahrain: dispositius de tres activistes piratejats amb programari espia Pegasusus" Amnistía Internacional. 18 de febrer de 2022. Arxivat de l'original el 20 de febrer de 2022. [Consulta: 18 febrer 2022t'.
^ Jump up to:un b c Bergman, Ronen; Mazzetti, Mark (23 de març de 2022). "Israel, tement la reacció russa, va bloquejar el programari espia per a Ucraïna i Estònia". El New York Times. ISSN 0362-4331. Arxivat de l'original el 13 d'abril de 2022. [Consulta: 13 abril 2022t'.
^ Diplomàtics finlandesos van ser atacats per programari espia Pegasusus, diu el Ministeri d'Afers Exteriors arxivat el 28

de gener de 2022, a la Wayback Machine, 28/01/2022, euronews.com
^ Welle (www.dw.com), Deutsche. "La policia alemanya va comprar en secret el programari espia NSO Pegasusus | | DW 07.09.2021". DW.COM. Arxivat de l'original el 29 de gener de 2022. [Consulta: 30 gener 2022t'.
^ Jump up to:un b Welle (www.dw.com), Deutsche. Hongria admet haver utilitzat el programari espia Pegasusus de NSO Group | | DW 04.11.2021". DW.COM. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ "Viktor Orbán, acusat d'utilitzar Pegasusus per espiar periodistes i crítics. El guardià. 18 de juliol de 2021. Arxivat de l'original el 29 de gener de 2022. [Consulta: 18 juliol 2021c'.
^ "Viktor Orbán, acusat d'utilitzar Pegasusus per espiar periodistes i crítics. El guardià. 18 de juliol de 2021. Arxivat de l'original el 29 de gener de 2022. [Consulta: 30 gener 2022t'.
^ "Oficial hongarès: el govern va comprar, va utilitzar el programari espia Pegasusus" Premsa Associada. Arxivat de l'original el 8 de novembre de 2021. [Consulta: 14 novembre 2021 no—consulta: Novembre 2021.2021.2021.2021.
^ Bhattacharya, Ananya. "Què és Pegasusus i com es va dirigir als indis per WhatsApp?" Quars. Arxivat de l'original el 28 de juny de 2021. [Consulta: Març 10, 2021 no».2021
^ "El govern indi va comprar el programari espia Pegasusus? La resposta del Ministeri de l'Interior és preocupant". HuffPost. 19 de novembre de 2019. Arxivat de l'original l'1 de novembre de 2020. [Consulta: Març 10, 2021 no».2021
^ "Activistes indis, advocats van ser "atacats" utilitzant el programari espia israelià Pegasusus. El filferro. Arxivat de l'original el 27 de maig de 2021. [Consulta: Març 10, 2021 no».2021
^ Jump up to:un b "El 'hack' de WhatsApp és una violació greu dels drets, diuen les presumptes víctimes", ha afegit. El guardià. 1 de novembre de 2019. Arxivat de l'original el 22 de desembre de 2021. [Consulta: 30 gener 2022t'.
^ "Telèfons de polítics indis, periodistes hackejats utilitzant Pegasusus: 10 fets sobre l'informe" NDTV. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ "El programari espia Pegasusus solia 'tafanejar' sobre periodistes, activistes indis. L'hindú. Corresponsal especial. 19 de juliol de 2021. ISSN 0971-751X. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.{{cite news}}: CS1 maint: others (link)
^ "Telèfons de 2 ministres, 3 líders de l'OPP entre molts destinats a la vigilància: informen". El expresso indi. 19 de juliol de 2021. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ Activistes indis empresonats per càrrecs de terrorisme estaven a la llista amb objectius de vigilància Arxivats el 6 de desembre de 2021, a Wayback Machine, The Washington Post, Joanna Slater i Niha Masih, el 20 de juliol de 2021. [Consulta: 20 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ "La llista Snoop té 40 periodistes indis, les proves forenses confirmen la presència de programari espia Pegasusus en alguns", va dir. thewire.in. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ "Onze telèfons dirigits: De dona que va acusar l'ex-CJI d'assetjament, familiars" El expresso indi. 20 de juliol de 2021. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ "Dies després d'acusar CJI Gogoi d'assetjament sexual, staffer va posar a la llista de possibles objectius de snoop". thewire.in. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ "La llista filtrada de Snoop suggereix que la vigilància podria haver tingut un paper en l'enderrocament del govern de Karnataka el 2019". thewire.in. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ Oficina, Karnataka Bureau & New Delhi (20 de juliol de 2021). "Els principals líders de Cong-JDS van ser "possibles objectius" del programari espia Pegasusus durant la crisi de 2019: informe. L'hindú. ISSN 0971-751X. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ "La policia israeliana utilitza Pegasus de la NSO per espiar ciutadans. CalcalistTech. 18 de gener de 2022. Arxivat de l'original el 19 de gener de 2022. [Consulta: 19 gener 2022t'.
^ Jump up to:un b Ganon, Tomer (18 de gener de 2022). "La policia israeliana utilitza Pegasus de la NSO per espiar ciutadans. CTECH - www.calcalistech.com. Arxivat de l'original el 19 de gener de 2022. [Consulta: 1 febrer 2022t'.
^ Jump up to:un b c "La policia va atacar l'activista amb programari NSO, va guardar informació sobre la seva vida sexual- informe." Arxivat 28 de gener de 2022, a Wayback Machine The Times of Israel, 20 de gener de 2022.
^ Cahane, Amir (27 de gener de 2022). "Policia israeliana: des de registres de telèfons mòbils sense garantia fins a un ús indegut controvertit de spyware" Lawfare. Arxivat de l'original el 3 de febrer de 2022. [Consulta: 3 febrer 2022t'.
^ Bachner, Michael. "La policia israeliana va ser acusada d'utilitzar programari espia de la NSO contra civils durant anys sense supervisió". www.timesofisrael.com. Arxivat de l'original l'1 de febrer de 2022. [Consulta: 1 febrer 2022t'.
^ "Què diu realment la policia israeliana quan nega la investigació calcalista?" Arxivat Gener 28, 2022, a la Wayback Machine (hebreu). Calcalista, 20 de gener de 2022.
^ "Gideon Sa'ar: Informes sobre NSO, la policia ha de ser revisada." Arxivat Gener 20, 2022, a la Wayback Machine The Jerusalem Post, 19 de gener de 2022.
^ Jump up to:un b "Formar una Comissió d'investigació per revisar la policia i l'afer NSO. Una sonda interna no serà suficient'" Arxivat el 21 de gener de 2022, a la Wayback Machine (hebreu). Ynet, 21 de gener de 2022.
^ "El fiscal general obre una investigació sobre l'ús policial de programari espia de la NSO contra israelians", ha afegit. Els temps d'Israel. 20 de gener de 2022. Arxivat de l'original el 3 de febrer de 2022. [Consulta: 3 febrer 2022t'.
^ https://www.gov.il/he/departments/units/privacy_protection_council Arxivat el 28 de gener de 2022, a Wayback Machine — entrada al lloc web del Ministeri de Justícia (hebreu).

^ "La policia fa ziga-zagues sobre l'afer NSO: "es van descobrir proves que canvien les coses" Arxivat l'1 de febrer de 2022, a wayback machine (hebreu). Ynet. 1 de febrer de 2022.
^ "Caps de ministeri, associats de Netanyahu, activistes van dir que van ser atacats per la policia amb programari espia". Arxivat Febrer 7, 2022, a la Wayback Machine The Times of Israel, 7 de febrer de 2022.
^ "El ministre de Policia estableix una comissió per investigar les afirmacions explosives d'espionatge de la NSO". Arxivat Febrer 7, 2022, a la Wayback Machine The Times of Israel, 7 de febrer de 2022.
^ "Els excaps del ministeri exigeixen a la comissió estatal que investigui les reclamacions policials". Arxivat Febrer 8, 2022, a la Wayback Machine The Times of Israel, 8 de febrer de 2022.
^ "Dos activistes de Jordània i Bahrain atacats per Pegasusus Spyware" Al Bawaba. Arxivat de l'original el 18 de gener de 2022. [Consulta: 27 gener 2022t'.
^ Pegasusus: Spyware venut als governs "objectius activistes" Arxivat el 2 de gener de 2020, a Wayback Machine, 19 de juliol de 2021, BBC
^ Kazakhstan: Activistes rastrejats per Pegasusus enfadats però no sorpresos Arxivats el 21 de gener de 2022, a la Wayback Machine, Almaz Kumenov Jul 21, 2021 eurasianet.org
^ "Qui hi ha a la llista? – El Projecte Pegasusus". OCCRP. Arxivat de l'original el 8 de gener de 2022. [Consulta: 21 gener 2022t'.
^ "Kazakhstan: quatre dispositius mòbils de quatre activistes infectats amb el programari espia Pegasusus" Amnistía Internacional. 9 de desembre de 2021. Arxivat de l'original el 27 de gener de 2022. [Consulta: 27 gener 2022t'.
^ Jump up to:un b Welle (www.dw.com), Deutsche. "El programari espia Pegasusus: Mèxic és un dels objectius més grans | | DW 22.07.2021". DW.COM. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ Bergman, Ronen (10 de gener de 2019). "Exclusiva: Com el baró mexicà de la droga El Chapo va ser enderrocat per la tecnologia fabricada a Israel", va dir. Ynetnews. Ynet. Arxivat de l'original el 25 de juliol de 2019. [Consulta: 15 maig 2019'.
^ Bergman, Ronen (11 de gener de 2019). "Teixint una web cibernètica". Ynetnews. Arxivat de l'original el 27 de juliol de 2019. [Consulta: 15 maig 2019'.
^ Scott-Railton, John; Marczak, Bill; Guarnieri, Claudio; Creta-Nishihata, Masashi (11 de febrer de 2017). "Bitter Sweet: Partidaris de l'impost sobre la soda de Mèxic dirigits amb enllaços d'explotació de NSO". Laboratori Ciutadà. Arxivat de l'original el 31 de maig de 2019. [Consulta: 25 març 2017'.
^ "Bitter Sweet: Partidaris de l'impost sobre la soda de Mèxic dirigits amb enllaços d'explotació de NSO". El laboratori ciutadà. 11 de febrer de 2017. Arxivat de l'original el 31 de maig de 2019. [Consulta: 14 juny 2019 no—consulta: 14 juny 2019.2019.20222.2
^ Jump up to:un b c Ahmed, Azam (10 de juliol de 2017). "El programari espia a Mèxic va apuntar a investigadors que buscaven estudiants". El New York Times. ISSN 0362-4331. Arxivat de l'original el 15 d'agost de 2019. [Consulta: 13 juliol 2017'.
^ "Revelat: el número del periodista assassinat seleccionat pel client mexicà de NSO" El guardià. 18 de juliol de 2021. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 30 gener 2022t'.
^ "'És gratis per a tothom': com el programari espia d'alta tecnologia acaba en mans dels càrtels de Mèxic". TheGuardian.com. 7 de desembre de 2020. Arxivat de l'original el 24 de febrer de 2022. [Consulta: 30 gener 2022t'.
^ "Informe: La vídua del periodista mexicà assassinat va ser atacada per programari espia". NOTÍCIES D'AP. 20 de març de 2019. Arxivat de l'original el 30 de gener de 2022. [Consulta: 30 gener 2022t'.
^ Kirchgaessner, Stephanie (21 de juny de 2020). "El programari espia israelià solia atacar periodistes marroquins, afirma Amnistia Internacional". El guardià. Arxivat de l'original el 30 de juliol de 2020. [Consulta: 21 juny 2020'.
^ Cheref, Abdelkader (29 de juliol de 2021). "És el ciberespionatge del Marroc l'última gota que fa m'ha fet a Algèria?" Arxivat de l'original l'1 d'octubre de 2021. [Consulta: 18 setembre 2021 no—Consulta: 18 setembre 2021.2021.2021.20
^ "Pegasus: Del seu propi rei a Algèria, l'abast infinit dels serveis d'intel·ligència del Marroc" Ull de l'Orient Mitjà. Arxivat de l'original el 18 de setembre de 2021. [Consulta: 18 setembre 2021 no—Consulta: 18 setembre 2021.2021.2021.20
^ Kirchgaessner, Stephanie; Safi, Michael (8 de novembre de 2021). "Els telèfons mòbils dels activistes palestins van ser piratejats utilitzant programari espia NSO, diu l'informe", diu l'informe. El guardià. Arxivat de l'original el 8 de novembre de 2021. [Consulta: 8 novembre 2021 no—consulta: 8 novembre 2021.2021.2021.2
^ Bartkiewicz, Artur (3 de gener de 2022). "Gazeta Wyborcza": Jak kupowano Pegasususa dla CBA" ["Gazeta Wyborcza": Com es va comprar Pegasusus per a la CBA]. Rzeczpospolita (polonès). Arxivat de l'original el 7 de gener de 2022. [Consulta: 6 gener 2022t'.
^ "Polònia admet la compra de programari espia israelià NSO" Independent. 7 de gener de 2022. Arxivat de l'original el 10 de gener de 2022. [Consulta: 8 gener 2022t'.
^ "AP Exclusive: duo d'oposició polonès hackejat amb programari espia NSO" NOTÍCIES D'AP. 20 de desembre de 2021. Arxivat de l'original el 6 de gener de 2022. [Consulta: 6 gener 2022t'.
^ "Brejza inwigilowany Pegasususem". PiS pos?u?y? si? pod?ymi metodami"". RMF FM (en polonès). Arxivat de l'original el 6 de gener de 2022. [Consulta: 6 gener 2022t'.
^ Jump up to:un b "El grup de drets humans verifica que el senador polonès va ser hackejat amb programari espia". NOTÍCIES D'AP. 6 de gener de 2022. Arxivat de l'original el 6 de gener de 2022. [Consulta: 6 gener 2022t'.

^ "AP Exclusiva: senador de l'oposició polonesa hackejat amb programari espia" NOTÍCIES D'AP. 23 de desembre de 2021. Arxivat de l'original el 7 de gener de 2022. [Consulta: 6 gener 2022t'.
^ "Watergate polonès": Varsòvia acusada d'utilitzar Pegasusus per espiar rivals. euronews. 5 de gener de 2022. Arxivat de l'original el 6 de gener de 2022. [Consulta: 6 gener 2022t'.
^ Notícies, Polsat. "La Comissió del Senat sobre Pegasusus ha començat la seva tasca. Els primers testimonis seran experts de Citizen Lab - Polsat News". polsatnews.pl (en anglès). Arxivat de l'original el 25 de gener de 2022. [Consulta: 25 gener 2022t'.
^ "Citizen Lab: Kolejnych dwóch Polaków szpiegowanych Pegasususem". Rzeczpospolita (polonès). Arxivat de l'original el 25 de gener de 2022. [Consulta: 25 gener 2022t'.
^ "Citizen Lab: Dwie kolejne osoby inwigilowane Pegasususem". www.rmf24.pl (en polonès). Arxivat de l'original el 25 de gener de 2022. [Consulta: 25 gener 2022t'.
^ Wro?ski, Pawe?; Tynkowski, Marcin (7 de febrer de 2022). "Cyberatak na Najwy?sz? Izb? Kontroli. " Mamy podejrzenie w?amania Pegasususem na trzy telefony"" [Ciberatac a la Sindicatura de Comptes. "Tenim la sospita d'un hackeig de Pegasusus en tres telèfons", ha afegit. Gazeta Wyborcza (polonès). Arxivat de l'original el 8 de febrer de 2022. [Consulta: 8 febrer 2022t'.
^ Jump up to:un b "Atac de programari espia de WhatsApp: clergues d'alt rang a Togo entre activistes atacats". El guardià. 3 d'agost de 2020. Arxivat de l'original el 6 d'abril de 2022. [Consulta: 18 abril 2022t'.
^ Jump up to:un b Kirkpatrick, David D. (2 de desembre de 2018). "El programari israelià va ajudar els saudites a espiar Khashoggi, diu la demanda (publicada el 2018)" El New York Times. ISSN 0362-4331. Arxivat de l'original el 8 de març de 2021. [Consulta: 8 març 2021 no—consulta: Març 2021.2021
^ "El Regne va arribar al Canadà: com l'espionatge digital vinculat a l'Aràbia Saudita va arribar a territori canadenc". El laboratori ciutadà. Toronto. 1 d'octubre de 2018. Arxivat de l'original el 8 de novembre de 2018. [Consulta: 8 novembre 2019'.
^ Satter, Raphael (25 de gener de 2019). "APNewsBreak: Agents encoberts dirigits a la vigilància de la ciberseguretat" The Seattle Times a través d'AP News. Nova York. Arxivat de l'original el 26 de gener de 2019. [Consulta: 26 gener 2019 no—consulta: Gener 26, 2019.2022. Actualitzat el 26 de gener
^ "El programari israelià va ajudar els saudites a espiar Khashoggi, diu la demanda", diu la demanda. Arxivat de l'original el 3 de desembre de 2018. [Consulta: 3 desembre 2018'.
^ Així, ha afegit. (24 de març de 2019). "L'empresa israeliana no dirà si va vendre programari espia saudita vinculat a l'assassinat de Khashoggi", va dir. Axios. Arxivat de l'original el 25 de març de 2019. [Consulta: 9 novembre 2019'.
^ "Els saudites darrere de l'atac de programari espia de la NSO contra la família de Jamal Khashoggi, suggereix una filtració", suggereix la filtració. TheGuardian.com. 18 de juliol de 2021. Arxivat de l'original el 21 de març de 2022. [Consulta: Març 21, 2022.2022t.2022.2022.2022.2
^ Burgess, Matt (23 de gener de 2020). "Si l'Aràbia Saudita va piratejar Jeff Bezos, probablement així va ser com va caure", va dir. Regne Unit cablejat. Arxivat de l'original el 20 de juliol de 2021.
^ Sarkar, Debashis (23 de gener de 2020). "Un informe forense revela el programari espia israelià Pegasusus darrere del hackeig telefònic de Jeff Bezos". Temps de l'Índia. Arxivat de l'original el 20 de juliol de 2021.
^ "El periodista del New York Times Ben Hubbard va piratejar Pegasusus després d'informar sobre intents de pirateria anteriors. El laboratori ciutadà. 24 d'octubre de 2021. Arxivat de l'original el 2 de gener de 2020. [Consulta: 24 octubre 2021 no—consulta: 24 octubre 2021.2021.2021.20
^ Hubbard, Ben (24 d'octubre de 2021). "M'han piratejat. El programari espia utilitzat contra mi ens fa a tots vulnerables". El New York Times. Arxivat de l'original el 31 d'octubre de 2021. [Consulta: 24 octubre 2021 no—consulta: 24 octubre 2021.2021.2021.20
^ El Regne va arribar al Canadà; Com l'espionatge digital vinculat a l'Aràbia Saudita va arribar a sòl canadenc arxivat el 8 de novembre de 2018, a wayback machine, per Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak i Ron Deibert l'1 d'octubre de 2018
^ Kirchgaessner, Stephanie; Jones, Sam (13 de juliol de 2020). "Telèfon del màxim polític català 'atacat per programari espia de grau governamental'". El guardià. Arxivat de l'original el 18 de febrer de 2021. [Consulta: 30 gener 2022t'.
^ Srivastava, Mmehul (21 de desembre de 2021). "L'acord secret d'Uganda que ha portat a NSO a la vora del col·lapse", va dir. ArsTechnica. Arxivat de l'original el 28 de desembre de 2021. [Consulta: 22 desembre 2021c'.
^ "Els Emirats Àrabs Units van atacar funcionaris iemenites amb programari espia israelià Pegasusus: informe. Sabah diari. 4 d'agost de 2021. Arxivat de l'original el 6 d'agost de 2021. [Consulta: 4 agost 2021'.
^ "Noves proves suggereixen que el programari espia utilitzat per vigilar l'activista dels Emirats Alaa Al-Siddiq". El guardià. 24 de setembre de 2021. Arxivat de l'original el 27 de setembre de 2021. [Consulta: 24 setembre 2021 no—consulta: 24 setembre 2021.2021.2021.20
^ Gardner, Frank (6 d'octubre de 2021). "Princesa Haya: el governant de Dubai tenia el telèfon de la seva exdona piratejat - tribunal del Regne Unit" Notícies de la BBC. Arxivat de l'original el 6 d'octubre de 2021. [Consulta: 6 octubre 2021'.
^ "El fabricant de programari espia Pegasusus acaba el contracte amb els Emirats Àrabs Units després de la sentència de pirateria de l'alt tribunal del Regne Unit". CNN. 7 d'octubre de 2021. Arxivat de l'original el 13 d'octubre de 2021.

[Consulta: 7 octubre 2021 no—consulta: 7 octubre 2021.2021.2021.2
^ Wiggins, Kaye (abril 2022). "Els fons estatals d'Abu Dhabi es van utilitzar per comprar el grup de programari espia israelià NSO. El Financial Times. Arxivat de l'original el 5 d'abril de 2022. [Consulta: 1 abril 2022t'.
^ Kirchgaessner, Stephanie (18 d'abril de 2022). "El número 10 sospitós de ser l'objectiu de l'atac de programari espia de NSO, va dir Boris Johnson". El guardià. [Consulta: 19 abril 2022t'.
^ "La DEA no va comprar programari maliciós al controvertit grup de NSO d'Israel perquè era massa car". www.vice.com. Arxivat de l'original l'1 de febrer de 2022. [Consulta: 1 febrer 2022t'.
^ Bing, Christopher; Menn, Joseph (3 de desembre de 2021). "Els telèfons del Departament d'Estat dels Estats Units van piratejar amb programari espia de l'empresa israeliana, fonts". Reuters. Arxivat de l'original el 4 de desembre de 2021. [Consulta: 4 desembre 2021'.
^ Toosi, Nahal (19 de novembre de 2021). "L'acte d'equilibri de Biden a l'Orient Mitjà té un problema: Israel. POLÍTICA. Arxivat de l'original el 5 de desembre de 2021. [Consulta: 5 desembre 2021'.
^ "FONT AP: NSO Group spyware utilitzat per piratejar empleats de l'Estat" NOTÍCIES D'AP. 3 de desembre de 2021. Arxivat de l'original l'1 de febrer de 2022. [Consulta: 1 febrer 2022t'.
^ ? Levenson, Michael (28 de gener de 2022). "F.B.I. va comprar secretament programari espia israelià i va explorar la pirateria de telèfons nord-americans". El New York Times. ISSN 0362-4331. Arxivat de l'original el 31 de gener de 2022. [Consulta: Gener 31, 2022.'.
^ "L'FBI va considerar la compra de programari espia que pogués piratejar qualsevol telèfon als Estats Units. Gizmodo. Arxivat de l'original el 31 de gener de 2022. [Consulta: Gener 31, 2022.'.
^ "Investigador recolzat per l'ONU sobre possibles crims de guerra del Iemen dirigits per programari espia". El guardià. 20 de desembre de 2021. Arxivat de l'original el 30 de gener de 2022. [Consulta: 20 desembre 2021 no—consulta: 2021
^ Satter, Rafael; Bing, Christopher (11 d'abril de 2022). "Alts funcionaris de la UE van ser atacats amb programari espia israelià". Reuters. Arxivat de l'original el 13 d'abril de 2022. [Consulta: 13 abril 2022t'.
^ "Els líders estatals de BJP Fields per fer front a les acusacions de Pegasusus, utilitzen bogey de la conspiració internacional". El filferro. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ "Israel va ajudar a més de deu països a tocar més de 50.000 telèfons". Daraj. 18 de juliol de 2021. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ ? «Direkt36» (en hongarès). Arxivat de l'original el 18 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ "Sobre el projecte Pegasusus". Històries prohibides. Arxivat de l'original el 19 de juliol de 2021. [Consulta: 19 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ "The PegasusUS PROJECT Live Blog: Grans Històries de Socis" PRIMERA LÍNIA. Arxivat de l'original el 21 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ El CEO de NSO respon exclusivament a les acusacions: "La llista de 50.000 números de telèfon no té res a veure amb nosaltres" | Ctech". m.calcalistech.com. Arxivat de l'original el 20 de juliol de 2021. [Consulta: 21 juliol 2021c'.
^ "El programari espia Pegasusus trobat als telèfons dels periodistes, confirma la intel·ligència francesa", ha afegit. El guardià. 2 d'agost de 2021. Arxivat de l'original el 2 d'agost de 2021. [Consulta: 2 agost 2021c'.
^ "El principal investigador de Human Rights Watch suposadament va piratejar el programari espia Pegasusus". El guardià. 26 de gener de 2022. Arxivat de l'original el 26 de gener de 2022. [Consulta: 26 gener 2022c'.
^ "Una filtració massiva de dades revela el programari espia del Grup NSO israelià utilitzat per atacar activistes, periodistes i líders polítics a tot el món", ha afegit. Amnistía Internacional. 18 de juliol de 2021. Arxivat de l'original el 18 de juliol de 2021. [Consulta: 18 juliol 2021c'.
^ Sacerdot, Dana; Timberg, Craig; Mekhennet, Souad. "El programari espia israelià privat s'utilitza per piratejar telèfons mòbils de periodistes, activistes de tot el món". El Washington Post. Arxivat de l'original el 2 de gener de 2020. [Consulta: 20 juliol 2021 no—consulta: Juliol 2021.2021.2021.2021.
^ Tynan, Dan (25 d'agost de 2016). "Apple emet una actualització global d'iOS després d'intentar utilitzar programari espia a l'iPhone de l'activista. El guardià. Arxivat de l'original el 18 d'abril de 2019. [Consulta: 21 desembre 2016'.
^ Brandom, Russell (26 d'agost de 2016). "Per què Apple no pot sortir de les vulnerabilitats de seguretat?" La Verge. Arxivat de l'original el 21 de desembre de 2016. [Consulta: 21 desembre 2016'.