CARNET

Pegasus

CERT.hr-PUBDOC-2022-3-407

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

1.1 *Spyware* Pegasus

Pegasus je *spyware* kojeg razvija izraelska tvrtka NSO Grupa. Nakon zaraze ovim *spywareom,* Pegasus može:

- snimati slike,
- upaliti mikrofon i snimati pomoću njega,
- prikupljati poruke,
- snimati pozive,
- prikupljati lozinke,
- i ostalo.

U početku, do zaraze Pegasusom je moglo doći pritiskom na zlonamjernu poveznicu poslanu putem primjerice SMS poruke. Kasnije se počela koristiti i druga metoda. Korištenjem *zero-click exploita* moglo je doći do zaraze mobilnog uređaja Pegasus *spywareom* bez žrtvine interakcije. *S*am primitak poruke izazvao bi zarazu Pegasus *spywareom*. Pritom, žrtva ne bi dobila nikakvu obavijest o poruci, stoga ne bi imala razloga posumnjati da je na njezin mobilni uređaj instaliran zlonamjerni program. Jedan primjer takvog *exploita* je FORCEDENTRY [1], o kojem će biti više rečeno kasnije [2.3.3].

Pegasus *spyware* može zaraziti i Android i Apple mobilne uređaje. Budući da imamo više dostupnih dokumenata koji opisuju zarazu iOS mobilnih uređaja Pegasusom, u ovom dokumentu ćemo se više fokusirati na njihovu zarazu. Google je dao Android verziji malo drugčije ime – „*Chrysaor*“

1.2 NSO Group

Niv Carmi, Shalev Hulio i Omai Lavie 2010. godine osnivaju tvrtku pod nazivom NSO Group. Središte tvrtke je u Herzliyu, blizu Tel Aviva. NSO Grupa proizvodi Pegasus te ga prodaje državnim agencijama kao pomoć u borbi protiv kriminala i terorizma [2].

Kompanija „Francisco Partners“ 2014. godine kupuje udio u kompaniji, no 2019. godine Hulio i Lavie, uz pomoć kompanije „Novalpine“, ponovno postaju većinski vlasnici.

Tijekom godina, NSO Grupa sklapa ugovore za korištenje Pegasusa s raznim državnim agencijama diljem svijeta, a 2018. godine Citizen Lab objavljuje članak u kojem navodi 36 klijenata koji koriste Pegasus [3].

Zbog optužbi vezanih za navodnu zlonamjernu uporabu Pegasusa, NSO Grupa je relativno često u medijskoj pozornosti. Prema tvrdnjama NSO Grupe, Pegasus prodaju samo državama koje poštuju ljudska prava te svako krivo korištenje Pegasusa (npr. špijunaža običnih ljudi) rezultira prekidanjem ugovora i zabranom daljnjeg korištenja softvera.

1.3 Prvi susret s Pegasusom

Citizen Lab, laboratorij sa sjedištem u Kanadi, je istražujući hakersku skupinu *Stealth Falcon* [4] pronašao domene i IP adrese za koje se kasnije utvrdilo da su dio Pegasus infrastrukture. Do tog su zaključka došli analizom zlonamjerne poveznice poslane na mobitel aktivista za ljudska prava Ahmeda Mansoora. Mansoor je u kolovozu 2016. godine primio SMS poruku koja je sadržavala poveznicu koju je proslijedio kolegama iz kanadskog laboratorija Citizen Lab.
Mansoor nije kliknuo na poveznicu – u suprotnom, Pegasus bi bio instaliran na uređaj korištenjem lanca ranjivosti (engl. *exploit chain*) kojeg su istraživači nazvali „Trident".

Trident lanac ranjivosti uključuje *exploite* za iskorištavanje sljedeće tri ranjivosti:

- *CVE-2016-4657*: ranjivost u *WebKit-u*, pokretačkom dijelu (engl. *engine*) Safari preglednika, koja omogućuje izvršavanje proizvoljnog koda na uređaju pomoću posebno napravljene *web* stranice;

- *CVE-2016-4655*: ranjivost u jezgri iOS operacijskog sustava, koja omogućava napadaču koji može pokretati proizvoljni kod na uređaju dohvaćanje osjetljivih informacija iz jezgre;

- *CVE-2016-4656*: ranjivost u jezgri iOS operacijskog sustava, koja omogućava napadaču koji može pokretati proizvoljni kod na uređaju izvršavanje koda s privilegiranim dopuštenjima i tako zaobilaženje ograničenja koja nameće iOS (engl. *jailbreak*).

2 Kako Pegasus funkcionira?

2.1 Detaljnije o Pegasusu

Hacking Team je 2015. godine bio kompromitiran [5] čime su javnosti postale dostupne i poruke elektroničke pošte. Među njima se između ostalog mogla pronaći i navodna brošura Pegasus *spywarea*. Sama NSO Grupa nikad nije potvrdila da se zaista radi o službenoj brošuri. Brošura sadrži mnogo informacija o tome kako Pegasus funkcionira, instalaciji Pegasusa i kako izgleda njegova struktura. Između ostalog je bio opisan i postupak nakon kojeg bi klijenti NSO Grupe bili spremni za korištenje Pegasusa.

Osim toga, provedena su razna istraživanja nad mobitelima za koje se sumnjalo da su zaraženi Pegasus *spywareom*. Forenzikom procesa na mobitelu kao i posjećenih stranica, istraživači su uspjeli otkriti neke funkcionalnosti Pegasusa, način instalacije, ali i domene koje su povezali s infrastrukturom za koju vjeruju da pripada Pegasusovoj infrastrukturi [6]. O forenzici mobitela koji su bili zaraženi Pegasusom više govori sljedeće poglavlje [2.2].

2.1.1 Infrastruktura

Pegasus infrastruktura se mijenjala tijekom godina. Tijekom istraživanja, Amnesty International je davao nazive toj infrastrukturi. Primjerice, kad bi se referencirali na infrastrukturu 2018. godine, govorili bi o tzv. „Verziji 3“ (V3).

Općenito, infrastruktura Pegasusa je sadržavala mnoštvo domena i poslužitelja. Citizen Lab je uspio pronaći oko 600 domena u V3 infrastrukturi, koja se sastojala od mreže VPN-a, poslužitelja i C&C poslužitelja koji su bili povezani kroz mrežu poslužitelja koja se nazivala *Pegasus Anonymizing Transmission Network (*PATN*).* Takva mreža je otežavala otkrivanje izvora zaraze Pegasus *spywareom*.

Zanimljivo je da su neke od domena iz V2 infrastrukture bile ponovno korištene u V3 infrastrukturi, zbog čega je bilo lakše mapirati nove verzije mreže.

Nakon što je 2018. godine Amnesty International objavio analizu Pegasusa i njegove infrastrukture, mnoge od tih domena iz V3 infrastrukture su bile ugašene.

U kasnijoj verziji infrastrukture, V4, dodani su neki slojevi u mrežu kako bi se zaraza Pegasusom još teže otkrila. No, Amnesty International je uspio otkriti četiri (4) vrste poslužitelja u svakom od lanaca napada:

- validacijski poslužitelj;
- DNS poslužitelj za zarazu;
- poslužitelj za instalaciju Pegasusa;
- C&C poslužitelj.

Što se tiče fizičke lokacije poslužitelja koji su dio infrastrukture Pegasusa, oni se uglavnom nalaze u Europi i Sjevernoj Americi, t.j. barem su se nalazili u trenutku istraživanja Amnesty Internationala [6].

2.1.2 Instalacija

Za instalaciju Pegasusa na mobilni uređaj Apple je potreban broj mobilnog uređaja ili AppleID korisničko ime. Nakon što je mobilni uređaj inficiran, s njega se miču restrikcije koje nameće iOS (engl. *jailbreak*) te se instalira softverska komponenta (tzv. „agent“) koja je zadužena za prikupljanje podataka te njihovo slanje kontrolnim poslužiteljima (engl. *C&C server*). Prema analizi *Lookouta* iz 2016. godine, nakon instalacije Pegasus *spyware* koristi mehanizme trajnosti (engl. *persistence mechanisms*), dok novije analize pokazuju kako to više ne mora vrijediti. To znači da ponovno pokretanje mobilnog uređaja (engl. *reboot*) može maknuti Pegasus *spyware* s njega. No korištenjem *zero-click exploita* može lako doći do ponovne zaraze.

Za zarazu uređaja se iskorištavaju razne ranjivosti iOS sustava – nekad su to i *zero-day* ranjivosti. U tom slučaju, redovito ažuriranje mobilnog uređaja ne bi spriječilo zarazu *spywareom*.

Neki od zabilježenih načina zaraze Pegasus *spywareom* su:

- *man-in-the-middle* napad: tijekom posjećivanja *web* stranice bez korištenja TLS enkripcije, veza se može preusmjeriti na zlonamjernu stranicu koja iskorištava ranjivosti u žrtvinom pregledniku čime dolazi do zaraze Pegasusom.

- *one-click exploit*: žrtva može primiti poruku s poveznicom. Žrtva je navedena na posjećivanje dobivene poveznice, čime započinje instalacija *spywarea.*

- *zero-click exploit*: instalacija Pegasusa započinje nakon primljene poruke, no u ovom slučaju poruka nije prikazana žrtvi – za instalaciju NIJE potrebna žrtvina interakcija.

2.1.2.1 *Man-in-the-middle* napad

Jedna od žrtava ovakvog napada bio je Maati Monjib kada je jednom prilikom preko Safari preglednika pokušao posjetiti stranicu *yahoo.fr*. Nakon što ju je ručno upisao u adresnu traku (engl. *address bar*), preglednik je prvotno probao uspostaviti vezu s ***http****://yahoo.fr.* U normalnim okolnostima došlo bi do preusmjeravanja na TLS-sigurnu stranicu ***https****://yahoo.fr.* No pregledavanjem povijesti pretraživanja, uspostavilo se da je došlo do preusmjeravanja na sumnjivu stranicu za koju se vjeruje da je služila za instalaciju *spywarea.*

2.1.2.2 One-click exploit

Kako bi započela instalacija *spywarea* ovim putem, potrebno je kliknuti na poveznicu. Poveznica može pristići putem poruke koja može biti običan SMS, poruka elektroničke pošte ili poruka neke aplikacije za razmjenu poruka (engl. *messaging apps*).

Kao što je već spomenuto, jedna od žrtava ovakvog napada bio je Ahmed Mansoor. Primio je SMS poruku koja je sadržavala sumnjivu poveznicu te poruku koja ga navodi na posjećivanje poveznice („*Nove tajne o mučenju stanovnika Emirata u državnim*

zatvorima"). Posjećivanjem poveznice bi rezultiralo instalacijom *spywarea* Pegasus. Nakon što je Mansoor odnio mobilni uređaj Citizen Labu na analizu, Citizen Lab ju je detaljnije istražio – što je opisano u prethodnom poglavlju [1.3].

Slika 1 *Phishing* poruka koju je Mansoor primio *(izvor)*

Kao što je već navedeno, poslana poruka ne mora biti samo SMS poruka, već i poruka neke aplikacije za razmjenu poruka. Tako je primjerice novinar Ben Hubbard 2018. godine primio Whatsapp poruku. Sadržaj poruke moli Hubbarda da napravi reportažu o demonstracijama u Washingtonu[1], te ga navodi da klikne na poveznicu. Posjećivanje poveznice rezultira instalacijom Pegasus *spywarea.*

Slika 2 *Phishing* poruka koju je Hubbard primio (izvor)

Kao što se može vidjeti iz gornja dva primjera, zanimljivo je napomenuti kako su sadržaji poslanih poruka prilagođeni svakoj žrtvi kako bi ona bila motiviranija da posjeti poveznicu – takva *phishing* poruka ima poseban naziv, *spearphishing.*

[1] Prijevod: *„Gospodine Ben Hubbard je li moguće da napravite reportažu o demonstracijama za vašeg brata zadržanog u Saudijskoj Arabiji, ispred ambasade Saudijske Arabije u Washingtonu? Moj brat je zadržan tijekom Ramadana, a ja sam na školarini ondje, tako da Vas molim da me ne povezujete sa tim događajem [link]*
Napravite reportažu sada, započinje za manje od sat vremena. Molim Vas, trebamo Vašu podršku"

2.1.2.3 Zero-click exploit

U novije vrijeme, instalacija se obavlja potajno kako žrtva ne bi bila svjesna da je njezin mobilni uređaj ugrožen. Za to je zaslužan *zero-click exploit* o kojem će biti nešto više rečeno u sljedećem poglavlju [2.3].

2.1.3 Mehanizmi važni Pegasusu

Pegasus ima nekoliko mehanizama koji olakšavaju njegov rad:

- Ako dođe do nenadanih aktivnosti i izvanrednog gašenja (engl. *crash*) procesa, datoteke dnevnika (engl. *logs*) tog događaja se šalju Appleu. Pegasus to sprječava tako što tijekom instalacije, datoteka *com.apple.CrashReporter.plist.file* se stvara na lokaciji */private/var/root/Library/Preferences,* čime je onemogućeno slanje dnevničkih zapisa i dojavljivanje sumnjivih aktivnosti Appleu.

- Praćenje stanja baterije mobilnog uređaja, kao i dostupnih konekcija olakšava detektiranje idealnog vremena za slanje podataka prema kontrolnim poslužiteljima.

- *Self-destruction mechanism*[2]: u slučaju opasnosti od detekcije, aktivira se mehanizam za samouništenje koji miče apsolutno sve datoteke povezane s Pegasusom.

2.1.4 Prikupljanje i prijenos podataka

Nakon uspješne instalacije, agent započinje prikupljanje podataka:

- lozinke;
- ostalih osobnih podataka: liste kontakta, podaci koji se nalaze u kalendaru…;
- poruka: sadržaj SMS poruka ili poruke aplikacija za razmjenu poruka;
- sadržaja poziva;
- audio: postoji mogućnost uključivanja mikrofona;
- video/slike: postoji mogućnost uključivanja kamere;
- …

Agent prethodno prikupljene podatke šalje kontrolnim poslužiteljima indirektno, putem konekcija kriptiranim jakim algoritmima.

[2] Unutar navodne brošure Pegasus *spywarea* može se pronaći sljedeća izjava u kontekstu samouništenja agenta: „*Generalno, razumijemo da je važnije da izvor [napada] ne bude otkriven i da meta [napada] ne bude sumnjičava, nego da softverski agent ostane funkcionalan i još uvijek u radu.*“ [25]

2.2 Forenzika mobitela zaraženih Pegasusom

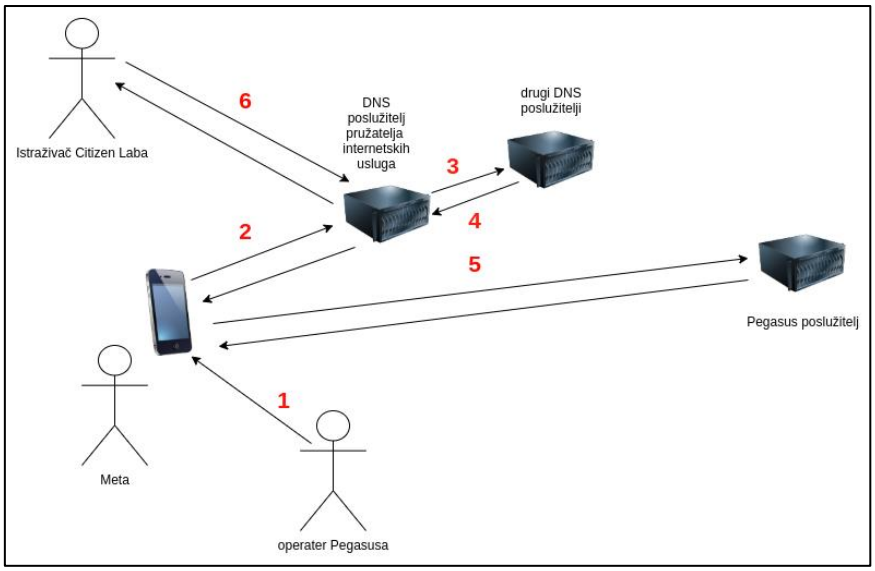
Nakon što je Ahmed Mansoor proslijedio ranije spomenutu *phishing* poruku Citizen Labu, istraživači Citizen Laba su posjetili URL u poruci i zabilježili ponašanje *web* stranice. Prema ponašanju *web* stranice razvili su digitalni otisak (*engl. fingerprint*) na temelju kojeg su mogli prepoznati poslužitelje koji su dio Pegasus infrastrukture. Pomoću masovnog skeniranja mrežnog prostora, istraživači Citizen Laba su pronašli 237 poslužitelja koji su dio digitalne infrastrukture Pegasusa. Iako su poslužitelji ubrzo bili ugašeni, nakon nekoliko tjedana nekolicina poslužitelja su ponovno postali dostupni te su istraživači uspjeli razviti novi digitalni otisak.

U periodu od dvije (2) godine (od kolovoza 2016. do kolovoza 2018.) istraživači su uspjeli identificirati preko 1.000 poslužitelja koji su odgovarali digitalnom otisku.

Istraživači Citizen Laba su na temelju imena otkrivenih domena pretpostavili u kojim državama se nalaze mete pojedinih Pegasus operatera. Osim toga, razvili su i forenzičku tehniku koja se oslanja na DNS međuspremnike (*engl. DNS cache)* pružatelja internetskih usluga (*engl. internet service providers*). Naime kada žrtva klikne na poveznicu, žrtvin preglednik mora napraviti DNS zahtjev kako bi odredio IP adresu *web* sjedišta. Neki DNS poslužitelji pohranjuju rezultate nedavnih DNS upita u interni međuspremnik kako bi mogli brže odgovoriti na buduće DNS upite. Mobilni uređaji su često konfigurirani tako da koriste DNS poslužitelje koji pripadaju korisnikovom pružatelju internetskih usluga. Ako su ti poslužitelji konfigurirani tako da pohranjuju rezultate DNS upita u međuspremnik, istraživači mogu iskoristiti tu funkcionalnost da relativno pouzdano saznaju gdje se nalaze žrtve koje su nedavno kliknule na Pegasus *phishing* poveznicu.

Kako bi istraživač saznao nalazi li se odgovor u DNS međuspremniku, može u DNS upit postaviti zastavicu "*norecursive*", u tom slučaju dobit će odgovor s IP adresom vezanom uz domenu jedino ako se rezultat DNS upita već nalazi u međuspremniku. Alternativno, ako DNS poslužitelj ne podržava tu opciju istraživač može i uspoređivati vremena odgovora kako bi saznao nalazi li se rezultat DNS upita u međuspremniku (odgovor će biti brži ako se nalazi).

Na temelju imena domena, istraživači Citizen Laba su zaključili da je jedan Pegasus operater vjerojatno ciljao i hrvatske mete, no nisu to uspjeli potvrditi pomoću prethodno opisane DNS analize.



Slika 3 Opis dijagrama:

1) operator Pegasusa šalje žrtvi poruku sa zlonamjernom poveznicom
2) Meta klikne na poveznicu, njen preglednik napravi DNS upit prema DNS poslužitelju svoj pružatelja internetski usluga
3) DNS poslužitelj pružatelja internetskih usluga prosljeđuje upit drugim DNS poslužiteljima
4) DNS poslužitelj pružatelja internetskih usluga dobije odgovor (IP adresu vezanu za domenu) i prosljeđuje ga meti
5) Preglednik mete se poveže na Pegasus poslužitelj te meta biva inficiranom
6) Istraživač Citizen Laba šalje DNS upit s poznatom Pegasus domenom DNS poslužitelju pružatelja internetskih usluga i na temelju odgovora sazna je li itko od klijenata tog pružatelja internetskih usluga nedavno kliknuo na zlonamjernu poveznicu

U lipnju 2018., jedan od članova organizacije Amnesty International je primio poruku sa zlonamjernom poveznicom. Radilo se o poruci koja je imala gotovo identičan sadržaj kao poruka koju je u otprilike isto vrijeme primio Ben Hubbard [2.1.2.2].

Analizirajući poveznice u toj i sličnim porukama, Amnesty International je na temelju sljedeća tri razloga zaključio da su ove poruke povezane s NSO Grupom:

1. Slično kao i Citizen Lab, Amnesty International je na temelju ponašanja poslužitelja stvorio digitalni otisak poslužitelja. Zatim je masovnim skeniranjem otkrio preko 600 drugih poslužitelja, među kojima su bili i poslužitelji vezani uz domene koje je Citizen Lab još prije povezao s NSO Grupom.

2. Otkrivene domene su uglavnom bile registrirane na radne dane u Izraelu, gdje se nalazi sjedište NSO Grupe (radni dani u Izraelu su nedjelja-četvrtak).

3. Kada su u sigurnom okruženju otvorili malicioznu poveznicu koju je primio član Amnesty Internationala, bili su preusmjereni na legitimnu stranicu. Takvo ponašanje odgovara onom opisanoj u navodnoj brošuri Pegasusa, gdje piše da ako iz nekog razloga nije moguće instalirati Pegasus, meta će biti preusmjerena na web stranicu koju je operator unaprijed definirao.

U srpnju 2021, Amnesty International je objavio forenzičku metodologiju [6] koju su koristili kako bi pronašli infrastrukturu Pegasusa, ali i kako bi detektirati tragove Pegasusa na mobilnom uređaju.

Iako je NSO grupa često mijenjala svoju infrastrukturu kako bi ju bilo teže pronaći, Amnesty International bi pronašao poveznicu između starije i novije verzije infrastrukture, te bi zatim pomoću digitalnog otiska pronašao i ostale dijelove novije infrastrukture. Istraživači su također uspjeli iskoristiti datoteke dnevnika koje Pegasus nije izbrisao kako bi pronašli imena procesa, URL-ove i Apple ID-ove povezane s Pegasusom. Amnesty International je objavio indikatore kompromitiranja (IOCs) i alat "*Mobile Verification Toolkit*" kako bi drugim istraživačima olakšali da saznaju je li neki mobilni uređaj zaražen Pegasusom.

2.2.1 MVT alat

Amnesty International Security Lab je 2021. godine napravio softverski paket *Mobile Verification Toolkit*, ili skraćeno „MVT“, koji služi za forenzičku analizu mobilnih uređaja i detekciju potencijalne zaraze Pegasus *spywareom*. Cijeli kod se može pronaći na GitHub stranici, te je popraćen detaljnom dokumentacijom. Amnesty International ga je koristio u analizi mobilnih uređaja 2021. godine o kojoj su također napravili detaljni izvještaj [6].

Potrebno je napomenuti kako korištenje alata zahtjeva poznavanje osnova forenzičke analize i terminala, budući da se program pokreće pomoću terminala. Zato, ako netko želi provjeriti je li njegov mobilni uređaj zaražen Pegasusom, savjetuje mu se da potraži pomoć stručnjaka.

Grupa nezavisnih novinara je 2021. uspješno koristila MVT kako bi analizirala svoje mobilne uređaje za potencijalnu zarazu Pegasus *spywareom*, te je nakon toga kontaktirala „Sigurnosnu Digitalnu Liniju za Pomoć“ (*Digital Security Helpline*) Access Nowa. Citizen Lab je u suradnji s Access Nowom započeo istragu vezanu uz hakiranja Pegasusom u El Salvadoru [7]. Otkriveno je da je 35 mobilnih uređaja od 37 testiranih zaraženo *spywareom.*

Nakon instalacije MVT-a (upute za instalaciju se mogu pronaći na gore spomenutoj Github stranici), kako bi započeli analizu mobilnog uređaja, potrebno je napraviti sigurnosnu kopiju (engl. *backup*) te ju premjestiti na drugo računalo na kojem je potrebno pokrenuti alat. MVT prima indikatore kompromitiranja u STIX2 formatu, te će pronaći takve indikatore u mobilnom uređaju ako oni postoje – MVT može pomoći u određivanju je li mobilni uređaj kompromitiran.

Alat je namijenjen za forenziku android i iOS mobilnih uređaja. Ponekad alat ne radi savršeno, što treba imati na umu dok se obavlja analiza pomoću njega.

Kako bi se spriječilo zlonamjerno korištenje MVT-a i narušavanje privatnosti ljudi s njim, MVT je izdan s posebnom licencom – alat se može koristiti samo na podacima ljudi koji su dali svoj pristanak.

2.3 Zero-click exploiti

Zero-click exploit je naziv za *exploit* koji ne zahtijevaju žrtvinu interakciju. Dakle, žrtva ne treba kliknuti link, niti izvršiti ikakvu drugu radnju da omogući napadaču da izvrši ranjivost.

U nastavku će biti više rečeno o nekim od *zero-click exploita* koje je Pegasus koristio.

2.3.1 WhatsApp *exploit* (*CVE-2019-3568*)

U svibnju 2019. zabilježeni su slučajevi instalacije Pegasusa na žrtvin uređaj iskorištavanjem ranjivosti unutar aplikacije WhatsApp. Radilo se o ranjivosti prepisivanja spremnika[3] (engl. *buffer overflow*) u kodu koji je procesirao mrežne pakete WhatsApp poziva. Žrtva nije morala odgovoriti na poziv da bude zaražena Pegasus spywareom.

WhatsApp je upozorio oko 1.400 korisnika za koje vjeruje da su bili obuhvaćeni ovim napadom. Incident je otkriven nakon što je odvjetnik iz Londona, koji je bio uključen u pravne slučajeve protiv NSO Grupe, primijetio propuštene pozive u čudno vrijeme s nepoznatog broja. WhatsApp je tužio NSO Grupu nakon ovog incidenta.

2.3.2 KISMET

Citizen Lab je u prosincu 2020. objavio članak u kojem otkriva kako su 36 mobilnih uređaja osoblja televizijske kuće *Al Jazeera* bili zaraženi Pegasus spywareom [8]. Za zarazu Pegasus spywareom korišten je *exploit chain* kojeg su istraživači nazvali KISMET.

KISMET iskorištava *zero-click* ranjivost u *iMessageu*, aplikaciji za razmjenu poruka između Appleovih uređaja. Ovaj *exploit chain* je napravljen na način da bude „nevidljiv" – žrtva ne bi vidjela da je primila ikakvu poruku.

U vrijeme pisanja ovog dokumenta, ranjivosti koje KISMET iskorištava nisu javno identificirane. Na temelju forenzičke analize mobitela zaraženih Pegasusom istraživači Citizen Laba su zaključili da napadač pri iskorištavanju ranjivosti pošalje JPEG privitak [9].

Iako ranjivosti koje KISMET iskorištava nisu javno identificirane, istraživači vjeruju da mobilni uređaji s verzijom iOS operacijskog sustava 14 i više ne mogu biti zaraženi putem KISMET *exploit chaina* zbog raznih sigurnosnih poboljšanja koje je Apple dodao u tu verziju.

Jedno od poboljšanja je dodavanje *BlastDoor* servisa za obradu gotovo svih podataka koje korisnik prima kroz *iMessage*. Prije uvođenja *BlastDoor* servisa velik dio podataka se obrađivao pomoću komponenti napisanih u jeziku *Objective C*. *BlastDoor* je napisan u programskom jeziku *Swift* koji je manje podložan klasičnim memorijskim ranjivostima, poput ranjivosti prepisivanja spremnika.

[3] Nacionalni CERT je pripremio dokument u kojem možete više pročitati o prepisivanju spremnika

2.3.3 FORCEDENTRY

Unatoč tome što je Apple dodavanjem *BlastDoor* servisa znatno smanjio površinu napada (engl. *attack surface*), Amnesty International i Citizen Lab su u veljači 2021. počeli primjećivati dokaze koji su upućivali na to da Pegasus koristi novi *zero-click exploit chain* koji može zaobići *BlastDoor* servis. Citizen Lab je taj *exploit chain* nazvao FORCEDENTRY.

Googleov Project Zero, tim istraživača koji se bavi istraživanjem *zero-day exploita*, je objavio detaljnu analizu prvog dijela FORCEDENTRY *exploit chaina*.

iMessage poruke podržavaju *gif* datoteke, te je glavni „trik" ovog *exploita* upravo iskoristiti način na koji se te datoteke obrađuju unutar iOS-a.

Pri procesiranju *iMessage* poruke koja sadrži privitak s „.gif" ekstenzijom, unutar komponente *IMTranscoderAgent* se poziva metoda *copyGifFromPath*. Prema procjeni Googleovih istraživača, svrha pozivanja ove metode je bila samo kopiranje GIF datoteke. Problem je što metoda interno ne bi jednostavno kopirala GIF datoteku, već bi ju i obradila. Komponenta *IMTranscoderAgent* nije dio *BlastDoor* servisa, što ju čini više podložnom klasičnim memorijskim ranjivostima, a pri obradi kompleksnijih formata datoteka lako je uvesti ranjivosti.

Uz to, interno korištena biblioteka *ImageIO* bi ignorirala činjenicu da datoteka ima ekstenziju „.gif" već bi odabrala *parser* za obradu datoteka na temelju bajtova koji se nalaze na početku datoteke, tzv. zaglavlja datoteke (engl. *file header*). To je znatno povećalo moguću površinu napada budući da napadač nije morao pronaći ranjivost u kodu za obradu GIF datoteka, već je bilo dovoljno da pronađe ranjivost u kodu za obradu bilo kojeg podržanog formata datoteka.

FORCEDENTRY *exploit chain* iskorištava ranjivost u kodu za obradu PDF datoteka koje sadrže niz podataka u JBIG2 formatu.

JBIG2 je format za kompresiju bitonalnih[4] slika. Korišten je kod nekih skenera, za kompresiju crnog teksta na bijeloj pozadini. Pri kompresiji se različite instance znakova zamjenjuju jednom inačicom znaka, primjerice ako postoji više inačica znaka „A" koje različito izgledaju, za potrebe kompresije svugdje će se koristiti samo jedna inačica znaka „A". Pri takvom komprimiranju se gube informacije (engl. *lossy compression*) što za neke svrhe nije pogodno. Zbog toga postoji i drugi način kompresije pri kojem se informacije ne gube (engl. *lossless compression*) ili se bar gube manje. U takvom načinu rada se pohranjuje (i također komprimira) razlika između reprezentativne inačice znaka i originalnog znaka. Dekompresija je implementirana tako da se primjenom logičkih operacija (AND, OR, XOR i XNOR) između razlike i reprezentativne inačice dobije originalan znak ili bar nešto što približno liči originalnom znaku.

Pri obradi JBIG2 podataka, javlja se ranjivost aritmetičkog prelijeva (engl. *integer overflow*), koja zatim kroz niz drugih koraka dopušta napadaču da čita s proizvoljne lokacije, odnosno piše proizvoljne podatke na bilo koju proizvoljnu lokaciju unutar memorije procesa *IMTranscoderAgent*.

[4] Bitonalne slike su slike koje se sastoje samo od crnih i bijelih piksela

U vrijeme pisanja ovog dokumenta nije javno objavljeno koje ranjivosti je FORCEDENTRY iskorištavao za dobivanje daljnjeg pristupa mobilnom uređaju, no poznato je da je za daljnje iskorištavanje ranjivosti morao izvršavati različite računske operacije (primjerice moguće je da je morao izračunati memorijsku adresu na koju treba zapisati neku vrijednost). Način na koji je FORCEDENTRY to postigao je posebno zanimljiv. Naime korištenjem ranije spomenutih osnovnih logičkih operacija koje se izvršavaju pri dekompresiji, autori FORCEDENTRY-a sagradili su malo virtualno računalo koje se koristi za izvršavanje svih operacija potrebnih za daljnje iskorištavanje ranjivosti.

3 Istraživanje Pegasusa

3.1 Projekt Pegasus

Projekt Pegasus je naziv za istragu koja uključuje više od 80 novinara 17 medijskih organizacija diljem svijeta. Forbidden Stories, neprofitna organizacija sa središtem u Parizu, koordinira djelatnost Projekta Pegasus, dok Amnesty International Security Lab pruža tehničku podršku – oni su zaduženi za obavljanje raznih forenzičkih analiza nad mobitelima potencijalnih žrtva, i po potrebi razvijaju alate koji pomažu pri tome. Jedan od alata kojeg su razvili je i alat MVT (*Mobile Verification Toolkit*) o kojem je nešto više rečeno u prethodnom poglavlju [2.2.1].

Na službenoj stranici Forbidden Storiesa se mogu pronaći najnovije vijesti vezane za Pegasus *spyware*. Svaka vijest je u obliku kratkog teksta koji sadržava poveznice koje vode do novinskih članaka koji daju potpunu reportažu o toj vijesti. Novinski članci pripadaju novinama koje su dio Projekta Pegasus.

Nastanak ovog projekta je potaknut time što je 50,000 brojeva mobilnih uređaja za koje se sumnja da pripadaju žrtvama Pegasusa ili budućim žrtvama Pegasusa postalo dostupno široj javnosti. Na popisu su se našli brojevi novinara, aktivista i članova vlada, uključujući kralja, predsjednike, ministre.

Smatra se kako je Pegasus igrao veliku ulogu u ubojstvu saudijskog novinara *Washington Posta* Jamala Khashoggija. Naime, 2. listopada 2018., oko 13 sati, Khashoggi je bio ubijen u saudijskom konzulatu u Turskoj. Broj mobilnog uređaja Khasoggija nije bio pronađen na prethodno spomenutom popisu, ali brojevi osoba bliskih njemu jesu. NSO grupa negira svoju umiješanost u ubojstvo Khashoggija. Najnoviji pronalasci upućuju na to da je Pegasus instaliran na mobitel Khashoggijeve zaručnice Hatice Cengiz samo 4 dana nakon ubojstva.

Taj popis brojeva je podijeljen s više medijskih organizacija, te je Amnesty International Security Lab napravio analizu nad mobilnim uređajima čiji su se brojevi našli na tom popisu. Uspostavljeno da je od 67 analiziranih mobilnih uređaja 37 bilo zaraženo Pegasusom.

Tijekom godina, neke od žrtava su bili i novinari koji su dio Projekta Pegasus.

Neke od medijskih organizacija koje sudjeluju u ovom projektu su: The Guardian, Le Monde, The Washington Post, The Wire, Direkt36, Die Zeit…

3.2 Reakcija javnosti

U svibnju 2019. godine, WhatsApp aplikacija je imala jako ozbiljnu ranjivost koja je bila iskorištena za instalaciju Pegasus spywarea – više o tome rečeno je u prethodnom poglavlju [2.3.1]. WhatsApp je krajem iste godine odlučio tužiti NSO Grupu koju je optužio za napad na mobilne uređaje putem WhatsApp aplikacije iskorištavanjem te ranjivosti. Do zaključka kako je upravo NSO Grupa iza tog napada su došli u suradnji sa Citizen Labom, koji su volontirali kako bi otkrili tko su bile žrtve tog napada.

Krajem sljedeće, 2020. godine, Microsoft, Google, Cisco i ostale velike tvrtke su podnijele *amicus curiae*[5] izvješće u prilog WhatsAppu. Microsoft na svojoj stranici u objavi bloga [10] navodi kako je opasno da NSO Grupa proizvodi *spyware* bez ikakvih pravnih obaveza ili posljedica kada on jednom bude zlouporabljen.

Krajem prošle 2021. godine, Apple tuži NSO Grupu, kao i njezinu roditeljsku tvrtku, za špijuniranje Apple korisnika. Naime, u rujnu 2021. godine, izašla je sigurnosna zakrpa Apple operacijskog sustava koja onemogućava iskorištavanje FORCEDENTRY *zero-day exploita.* U objavi za novinare (engl. *press release*) u kojoj najavljuju tužbu protiv NSO Grupe [11], navode kako ozbiljno shvaćaju sigurnost svojih korisnika, iako je samo mali broj njih bio zahvaćen *spywareom*. Isto tako, u sklopu tužbe zahtijevaju zabranu korištenja Appleovih proizvoda i servisa NSO Grupi.

Budući da je Pegasus *spyware* nađen na mobitelima članova vlada, novinara i aktivista, BIS (*Bureau of Industry and Security*) je u studenom 2021. godina zabranio američkim firmama prodavanje svojih proizvoda NSO Grupi – NSO Grupa je stavljena na tzv. *Entity List.*

[5] lat. „prijatelj suda“ : odnosi se na stranku koja ne sudjeluje u tužbi, ali pomoću izvješća (engl. *brief*) daje korisne informacije ili uvide u prilog ili protiv jedne od stranaka u tužbi

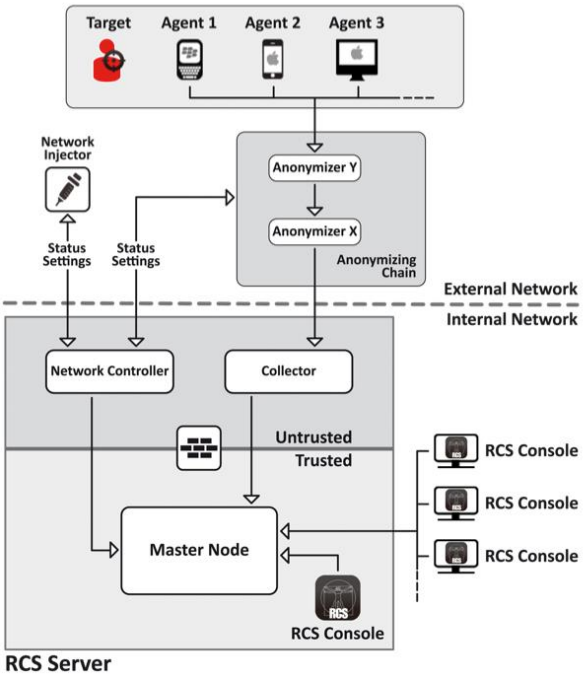
4 Konkurencija

4.1 Hacking Team

Talijanska firma Hacking Team je razvijala RCS (engl *Remote Control System*), znan između ostalog i kao Galileo. RCS je softver koji se instalira na računalo ili mobilni uređaj žrtve bez njenog znanja, te nakon instalacije on može:

- preuzeti poruke elektroničke pošte,
- kopirati datoteke iz stalne memorije,
- snimati video pozive,
- preuzeti lozinke utipkane u *web* preglednik,
- upaliti mikrofon i kameru te snimati žrtvu,
- …

Citizen Lab je tijekom svoje istrage Hacking Teama dobio i navodnu dokumentaciju koja opisuje kako se postavlja RCS te što sve on nudi klijentima [12]. U dokumentaciji se detaljnije objašnjava arhitektura cijelog RCS-a.



Slika 4 Logička arhitektura RCS-a (izvor)

U dokumentu se spominje i korištenje softverskog agenta izviđača (engl. *scout agent*) koji određuje treba li se na uređaj instalirati softverski agent. Nakon što se utvrdi da je instalacija „sigurna“, agent izviđač se zamijeni s običnim agentom. Agenti imaju razne funkcionalnosti za preuzimanje podataka (navedene iznad) koje se mogu po potrebni uključiti ili isključiti. Ukoliko postoji mogućnost detekcije agenta, postoji mogućnost

trenutnog zaustavljanja njegovih funkcionalnosti, primjerice pauziranje sinkronizacije ili prikupljanja audio podataka. Ako je to potrebno, može se pokrenuti i potpuno brisanje agenta na računalu ili mobilnom uređaju žrtve. Hacking Team tvrdi kako se agent ne može povezati s operaterom, no Citizen Lab je svojim istraživanjem ipak to uspio [13].

Sigurnosni istraživač Claudio Guarnieri je 2014. napravio alat *Detekt* [14] koji je mogao detektirati zarazu RCS-om skeniranjem memorije računala. U početku je alat bio uspješan u detekciji, no kasnije nije mogao detektirati zarazu RCS-om radi ažuriranja RCS-a koji se dogodio nakon objave Detekta.

RCS se prodavao vladama diljem svijeta kao pomoć u borbi protiv kriminala i terorizma. Klijenti Hacking Teama su se morali obvezati da neće zloupotrebljavati RCS. U protivnom, Hacking Team će zaustaviti održavanje softvera, čime bi on nedugo kasnije postao neiskoristiv – sve je to navedeno na tadašnjoj stranici Hacking Teama koja je u trenutku pisanja ovog dokumenta nedostupna.

Tijekom 2015. godine, Phineas Fisher[6] je kompromitirala Hacking Team, čime su privatni podaci kao što su poruke elektroničke pošte, postali dostupni široj javnosti. Poruke elektroničke pošte su potvrdile neke od klijenata Hacking Teama koji su do tada bili samo potencijalni kupci RCS-a. 2019. godine, InTheCyber je kupio Hacking Team, te ga preimenovao u Memento Labs.

4.2 Gamma Group

Gamma Group je tvrtka koja je razvila FinFisher, koji se negdje navodi i kao FinSpy ili Wingbird. FinFisher je *spyware* koji može djelovati na računalima i pametnim telefonima (engl. *smartphones*) te služi za nadgledanje iz daljine (engl. *remote monitoring*). S računala ili mobilnog uređaja žrtava prikuplja niz raznih podataka kao što su:

- lozinke,
- snimke zaslona,
- sms poruke,
- lokacije i
- ostalo.

Službena brošura FinFishera spominje kako se uz proizvod nudi i treniranje za njegovo korištenje [15].

Jedan od načina zaraze ovim *spywareom* je putem *phishing* poruke elektroničke pošte koja sadrži neku zlonamjernu datoteku. Jednom je zabilježeno kako se FinFisher instalirao nakon što se skinulo lažno ažuriranje za Adobe Flash Player preko stranice koja je glumila pravu stranicu za ažuriranje Flash Playera [16].

[6] Hakerica nepoznatog identiteta

Microsoft je proveo analizu nad uzorcima FinFishera te je otkrio korištenje raznih tehnika zbog kojih ga je bilo teže analizirati.

„*[FinFisher je] Komplicirana slagalica koju mogu riješiti reverzni inženjeri s dosta vremena, kodiranja, automatizacije i kreativnosti*“ [17].

Phineas Fisher je 2014. godine kompromitirala Gamma Group (kao i Hacking Team godinu dana kasnije), i široj javnosti je postalo dostupno oko 40GB do tad privatnih podataka.

4.3 Cytrox

Cytrox je započeo kao makedonski *startup,* a danas je on dio Intellexe, udruge kompanija koja je osnovana kao suparnik NSO Grupi. Cytroxov proizvod Predator je *spyware* koji može prikupiti informacije s mobitela žrtve kao i iz servisa na oblaku (engl. *cloud service*). Predator je otkriven kod egipatskog političara Aymana Noura nakon što je on odnio mobitel Citizen Labu na analizu zato što je primijetio da je prevruć. Otkrilo se naime da je njegov mobitel bio zaražen Pegasusom i Predatorom u isto vrijeme. Mobitel je zaražen nakon što je Nour primio Whatsapp poruku koja je sadržavala poveznice koji su vodili na malicioznu stranicu. Korištene domene su bile vrlo slične legitimnim domenama stranica za vijesti i domenama YouTubea.

Istraživači Citizen Laba su pronašli mehanizam trajnosti Predatora na iOS-u, no ne i na Androidu. Ako Predator zaista nema mehanizam trajnosti za Android i ako se koristi samo *one-click exploiti* putem poveznica koje vode na zlonamjernu stranicu, tada bi žrtva koja koristi Android mogla ukloniti Predator *spyware* jednostavnim ponovnim pokretanjem (engl. *reboot*) mobilnog uređaja. Ako Predator nema sposobnost korištenja *zero-click exploita* tada bi žrtva morala ponovno kliknuti na zlonamjernu poveznicu da bude zaražena.

Meta (bivši Facebook) je u prosincu 2021. objavila izvješće u kojem navodi da su uklonili oko 300 korisničkih računa s Instagrama i Facebooka za koje su vjerovali da ih je koristila tvrtka Cytrox [18].

4.4 QuaDream

QuaDream je mala izraelska tvrtka koja prodaje alat namijenjen špijunaži pametnih mobilnih uređaja vladama diljem svijeta. Njihov proizvod se zove Reign. Reign može čitati poruke, gledati slike, snimati pozive, upaliti kameru i mikrofon. Mobiteli koji su bili zaraženi Reignom su isto bili zaraženi iskorištavanjem *zero-click exploita* kao što su bili i mobilni uređaji zaraženi Pegasusom. Glasnogovornik NSO Grupe demantira da je NSO Grupa surađivala s QuaDreamom.

5 Zaključak

Pegasus *spyware* je dovoljno napredan da standardni sigurnosni savjeti koji štite od klasičnog *spywarea* nisu dovoljni.

Po trenutno dostupnim informacijama Pegasus se koristi u ciljanim napadima, a ranjivosti koje Pegasus koristi za instalaciju se ne iskorištavaju masovno što bi značilo da prosječni korisnik vjerojatno neće biti zaražen Pegasusom.

Prosječnim korisnicima savjetujemo redovno ažuriranje i izbjegavanje posjećivanja sumnjivih poveznica.

Ako netko od korisnika smatra kako bi mogao postati meta Pegasus *spywarea,* preporučujemo neke od sljedećih mjera:

- isključivanje *iMessagea* i *FaceTimea* – time se smanjuje vjerojatnost dobivanja *phishing* poruka. Treba napomenuti da postoje razne druge aplikacije koje služe za slanje poruka putem kojih se mogu dobiti poruke koje sadržavaju zlonamjerne poveznice.

- redovito ažuriranje mobilnog uređaja i aplikacija – iako i dalje postoji opasnost od *zero-day exploita,* redovitim ažuriranjem se smanjuje mogućnost iskorištavanja ranjivosti koje su popravljene u najnovijim sigurnosnim zakrpama (engl. *security patches*).

- ponovnim pokretanjem (engl. *reboot*) postoji mogućnost micanja softverskih agenata *spywarea* ako oni nemaju mehanizme trajnosti.

- izbjegavanje posjećivanja sumnjivih poveznica dobivenih putem poruka ili putem poruka elektroničke pošte.

NSO grupa je razvila Pegasus kao alat za borbu protiv terorizma i kriminala, no i sami kažu da su postojali neki slučajevi zloupotrebe Pegasusa te da su od 2016. do 2021. godine morali zabraniti upotrebu Pegasusa petorici klijenata. Istrage organizacija poput Citizen Laba, Amnesty Internationala i ostalih istraživača su pokazale da je Pegasus bio instaliran na mobilnim uređajima aktivista, odvjetnika, političara, novinara i diplomata.

Za detekciju infekcije Pegasus *spywareom,* postoji mogućnost korištenja Amnestyevog alata MVT (*Mobile Verification Toolkit*) [19]. Više o njemu je rečeno u prethodnom poglavlju [2.2.1]. Treba napomenuti kako je alat namijenjen istraživačima i profesionalcima, a ne krajnjim korisnicima. Za ispravno donošenje zaključka pomoću ovog alata potrebno je poznavati osnove forenzičke analize, pa se u slučaju sumnje na zarazu Pegasusom preporučuje tražiti pomoć stručnjaka.

6 Literatura

1. **Ian Beer, Samuel Gross.** A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution. [Mrežno] 16. prosinca 2021. [Citirano: 22. prosinca 2021.] https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html?m=1.

2. **NSO Group.** Human Rights Policy. [Mrežno] [Citirano: 22. prosinca 2021.] https://www.nsogroup.com/governance/human-rights-policy/.

3. **Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, Ron Deibert.** Hide and Seek. [Mrežno] 18. rujna 2018. [Citirano: 22. prosinca 2021.] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

4. **Bill Marczak, John Scott-Railton.** Keep Calm and (Don't) Enable Macros. [Mrežno] 29. svibnja 2016. [Citirano: 28. prosinca 2021.] https://citizenlab.ca/2016/05/stealth-falcon/.

5. **Franceschi-Bicchierai, Lorenzo.** Spy Tech Company 'Hacking Team' Gets Hacked. [Mrežno] 6. srpnja 2015. [Citirano: 24. siječnja 2022.] https://www.vice.com/en/article/gvye3m/spy-tech-company-hacking-team-gets-hacked.

6. **Amnesty International.** Forensic Methodology Report: How to catch NSO Group's Pegasus. [Mrežno] 18. srpnja 2021. [Citirano: 24. siječnja 2022.] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

7. **John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, Ron Deibert.** Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware. [Mrežno] 12. siječnja 2022. [Citirano: 15. ožujka 2022.] https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

8. **Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, Ron Deibert.** Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit. [Mrežno] 20. prosinca 2020. [Citirano: 21. veljače 2022.] https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

9. **John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, Ron Deibert.** Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware. [Mrežno] 12. siječnja 2022. [Citirano: 21. veljače 2022.] https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

10. **Burt, Tom.** Cyber mercenaries don't deserve immunity. [Mrežno] 21. prosinca 2020. [Citirano: 11. ožujka 2022.] https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

11. **Apple.** Apple sues NSO Group to curb the abuse of state-sponsored spyware. [Mrežno] 23. studenog 2021. [Citirano: 11. ožujka 2022.] https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/.

12. **Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, Katie Kleemola.** Hacking Team's Government Surveillance Malware. [Mrežno] 24. lipnja 2014. [Citirano: 24. veljače 2022.] https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/#part2.

13. **Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, John Scott-Railton.** Mapping Hacking Team's "Untraceable" Spyware. [Mrežno] 17. veljače 2014. [Citirano: 24. veljače 2022.] https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/.

14. **Singh, Amitpal.** Detekt spyware detection tool released. [Mrežno] 24. studenog 2014. [Citirano: 24. veljače 2022.] https://citizenlab.ca/2014/11/detekt-spyware-detection-tool/.

15. **Gamma Group.** FinFisher: Governmental IT Intrusion and Remote Monitoring Solutions. [Mrežno] [Citirano: 25. veljače 2022.] https://www.documentcloud.org/documents/267876-merged-finfisher-brochure-english.html.

16. **Amnesty International.** German-made FinSpy spyware found in Egypt and Mac and Linux versions revealed. [Mrežno] 25. rujna 2020. [Citirano: 25. veljače 2022.] https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/.

17. **Office 365 Threat Research Team, Microsoft Defender Security Research Team.** FinFIsher exposed: A researcher's tale of defeating traps, tricks, and complex virtual machines. [Mrežno] 1. svibnja 2018. [Citirano: 25. veljače 2022.] https://www.microsoft.com/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/.

18. **Meta.** Threat Report on the Surveillance-for-Hire Industry. [Mrežno] 16. prosinca 2021. [Citirano: 2. ožujka 2022.] https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

19. **Amnesty International Security Lab.** Mobile Verification Toolkit. [Mrežno] 2021. [Citirano: 1. ožujka 2022.] https://github.com/mvt-project/mvt.

20. **Travère, Audrey.** The Rise and Fall of NSO Group. [Mrežno] 19. srpnja 2021. [Citirano: 22. prosinca 2021.] https://forbiddenstories.org/the-rise-and-fall-of-nso-group/.

21. **Kirchgaessner, Stephanie.** Israeli spyware company NSO Group placed on US blacklist. [Mrežno] 3. studenoga 2021. [Citirano: 22. prosinca 2021.] https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist.

22. **Clark, Mitchell.** NSO's Pegasus spyware: here's what we know. [Mrežno] 23. srpnja 2021. [Citirano: 22. prosinca 2021.] https://www.theverge.com/22589942/nso-group-pegasus-project-amnesty-investigation-journalists-activists-targeted.

23. **Bill Marczak, John Scott-Railton.** The Milion Dollar Dissident. [Mrežno] 24. kolovoza 2016. [Citirano: 22. prosinca 2021.] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

24. **NSO Group.** First Annual Report Highlights Extensive Safeguards Against Misuse of Technology, Outlines Internal Governance and Compliance Processes. [Mrežno] [Citirano: 24. siječnja 2022.] https://www.nsogroup.com/Newses/cyber-intelligence-sector-leader-nso-group-unveils-the-industrys-first-transparency-and-responsibility-report/.

25. —. Pegasus-Product Description. [Mrežno] [Citirano: 24. siječnja 2022.] https://www.documentcloud.org/documents/4599753-NSO-Pegasus.

26. **Lookout.** Technical Analysis of Pegasus Spyware. [Mrežno] [Citirano: 26. siječnja 2021.] https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf.

27. —. Techincal Analysis of the Pegasus Exploits on iOS. [Mrežno] [Citirano: 31. sijecnja 2022.] https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf.

28. **The Forbidden Stories.** About The Pegasus Project. [Mrežno] [Citirano: 21. veljače 2022.] https://forbiddenstories.org/about-the-pegasus-project/.

29. **Washington Post Staff.** Takeaways from the Pegasus Project. [Mrežno] 2. veljače 2022. [Citirano: 21. veljače 2022.] https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

30. **Whatsapp.** Protecting our users from a video calling cyber attack. [Mrežno] [Citirano: 21. veljače 2022.] https://faq.whatsapp.com/general/security-and-privacy/protecting-our-users-from-a-video-calling-cyber-attack/?lang=hr.

31. **Facebook.** [Mrežno] 13. kolovoza 2019. [Citirano: 21. veljače 2022.] https://www.facebook.com/security/advisories/cve-2019-3568.

32. **Perlroth, Nicole.** WhatsApp Says Israeli Firm Used Its App in Spy Program. [Mrežno] 29. listopada 2019. [Citirano: 21. veljače 2022.] https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html.

33. **Kenyon, Miles.** WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone. [Mrežno] 13. svibnja 2019. [Citirano: 21. veljače 2022.] https://citizenlab.ca/2019/05/whatsapp-voice-calls-used-to-inject-nso-group-spyware-in-phones/ .

34. **Gross, Samuel.** A Look at iMessage in iOS 14. [Mrežno] 28. siječnja 2021. [Citirano: 21. veljače 2022.] https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html.

35. —. Remote iPhone Exploitation Part 1: Poking Memory via iMessage and CVE-2019-8641. [Mrežno] 9. siječnja 2020. [Citirano: 21. veljače 2022.] https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-1.html.

36. **Swift.** Memory Safety. [Mrežno] [Citirano: 21. veljače 2022.] https://docs.swift.org/swift-book/LanguageGuide/MemorySafety.html.

37. **Kirchgaessner, Stephanie.** FBI confirms it obtained NSO's Pegasus spyware. [Mrežno] 2. veljače 2022. [Citirano: 21. veljače 2022.] https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware.

38. **Bill Marczak, John Scott-Railton, Sarah McKune.** Hacking Team Reloaded? US-based Ethiopian Journalists Again Targeted with Spyware. [Mrežno] 9. ožujka 2015. [Citirano: 24. veljače 2022.] https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

39. **Hern, Alex.** Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. [Mrežno] 6. srpnja 2015. [Citirano: 24. veljače 2022.] https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

40. **Cox, Joseph.** A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher. [Mrežno] 7. kolovoza 2014. [Citirano: 25. veljače 2022.] https://www.vice.com/en/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher.

41. **Morgan Marquis-Boire, Bill Marczak.** FinFisher's Spy Kit Exposed. [Mrežno] 25. srpnja 2012. [Citirano: 25. veljače 2022.] https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/.

42. **Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri.** FinFisher Goes Mobile? [Mrežno] 29. kolovoza 2012. [Citirano: 25. veljače 2022.] https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/.

43. **Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, Ron Deibert.** Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. [Mrežno] 16. prosinca 2021. [Citirano: 25. veljače 2022.] https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

44. **Christopher Bing, Raphael Satter.** EXCLUSIVE iPhone flaw exploited by second Israeli spy firm - sources. [Mrežno] 2. veljače 2022. [Citirano: 25. veljače 2022.] https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/.

45. **Bill Marczak, Ali Abdulemam, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, Ron Deibert.** Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits. [Mrežno] 24. kolovoza 2021. [Citirano: 8. ožujka 2022.]

https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/.

46. **Amnesty International.** Marocco: Human Rights Defenders Targeted with NSO Group's Spyware. [Mrežno] 10. listopada 2019. [Citirano: 9. ožujka 2022.] https://www.amnesty.org/en/latest/research/2019/10/Morocco-Human-Rights-Defenders-Targeted-with-NSO-Groups-Spyware/.

47. **Bill Marczak, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, Ron Deibert.** New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts. [Mrežno] 24. listopada 2021. [Citirano: 10. ožujka 2022.] https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/.

48. **Cathcart, Will.** Opinion: Why WhatsApp is pushing back on NSO Group hacking. [Mrežno] 29. listopada 2019. [Citirano: 11. ožujka 2022.] https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/.

49. **U.S. Department of Commerce.** Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities. [Mrežno] 3. studenog 2021. [Citirano: 11. ožujka 2022.] https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

50. **Rueckert, Phineas.** Pegasus: The New Global Weapon For Silencing Journalists. [Mrežno] 18. srpnja 2021. [Citirano: 11. ožujka 2022.] https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

51. **Amnesty International.** Amnesty International Among Targets of NSO-powered Campaign. [Mrežno] 1. kolovoza 2018. [Citirano: 15. ožujka 2022.] https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.