Sigurnosne prijetnje na Internetu

Pegasus

Ivan Ljubičić, 6.11.2024.

Pregled predavanja

- Motivacija
- Pegasus – uvod
- Povijest otkrivanja
- Vektor napada "Trident"
- Zero-click vektor napada
- Mogućnosti
- Korištenje Pegasusa u divljini
- Etička pitanja i budući razvoj
- Zaključak

Pitanja za ispite

- Kada je Pegasus prvi put otkriven i kako je otkriven?
- Objasni vektor napada "Trident" koji je koristio Pegasus.
- Što je Cydia Substrate?
- Kako rade zero-click vektori napada?
- Koje mogućnosti ima špijunski program Pegasus?

Motivacija

- Manje više svi koristimo mobitele i digitalne uređaje i to nas automatski čini izloženima
- Ključno je razumjeti kakve sve prijetnje postoje i kako funkcioniraju kako bih se mogli pravilno zaštititi od njih

Pegasus - uvod

- Špijunski softver kojeg je razvio izraelski NSO, osnovan 2010., a 2017. imao oko 500 zaposlenih
- Prvi udaljeni iOS Jailbreak ikad napravljen
- Prodaje se kao rješenje protiv kriminala i terorizma, najčešće državama
- Svaku prodaju mora potvrditi Izraelsko ministarstvo zaštite

Povijest otkrivanja (1)

- 2016. napadnut aktivist za ljudska prava Ahmed Mansoor [3]
- Citizen labs dobio kopiju Pegasusa koji je iskorištavao tri zero-day ranjivosti na iOS 9.3.3
- Kasnije se otkrilo da je Pegasus počeo koristiti u UAE od 2013.

Povijest otkrivanja (2)

- Spear phishing poruka za Ahmeda Moonsora
- Na poruci piše: "New secrets about torture of Emiratis in state prisons"

[3]

Vektor napada "Trident" (1)

- Tri CVE-a iskorištena
  - CVE-2016-4655 – iOS curenje podataka iz jezgre
  - CVE-2016-4656 – Mogućnost pokretanja arbitrarnog koda pod podignutim ovlastima u jezgri
  - CVE-2016-4657 – Izvršavanje proizvoljnog koda preko web stranice
- Cijena koju je Apple spreman platiti da im se javi ovakav vektor napada je $250K [4]
- NSO naplaćuje samo postavljanje Pegasusa za neku vladu $600k, a cijena aktivnog praćenja iPhona je $65k [5]

Vektor napada "Trident" (2)

1. Nakon klikanja linka skida se prvi teret (eng. payload) i pokreće se taj kod (CVE-2016-4657)
2. Kod dohvaća memorijsku lokaciju jezgre (CVE-2016-4655)
3. Koristi se CVE-2016-4656 kako bih se isključio *code-signing*
4. Dohvaća se finalni teret koji je zapravo Pegasus špijunski softver
5. Pegasus postavlja aplikaciju Cydia Substrate

Vektor napada "Trident" (3)

- Cydia Substrate
  - Razvojni okvir koji omogućava ubacivanje koda u aplikacije i operacijski sustav
  - Time se omogućava pristup porukama, mikrofonu i kameri zaraženog mobitela
- Pegasus za Android
  - Poznatiji kao Chrysaor
  - Iste mogućnosti kao iOS verzija samo iskorištava druge ranjivosti
  - Nije toliko pouzdan, ako ne uspije Rootanje, pita korisnika za dopuštenje da eksfiltrira podatke [6]

Zero-click vektor napad

- Zero-click najčešće iskorištavaju ranjivosti u aplikacijama kao što su iMessage, Find My, aplikacija za pozive
- Takve aplikacije automatski obrađuju i provjeravaju dobivene poruke
- FORCEDENTRY [7]
  - Procesiranjem malicioznih PDF-a dovodi do izvršavanja arbitrarnog koda (CVE-2021-30860)
  - Zahvaća iOS < 14.8, macOS < 11.6, watchOS < 7.6.2

Mogućnosti

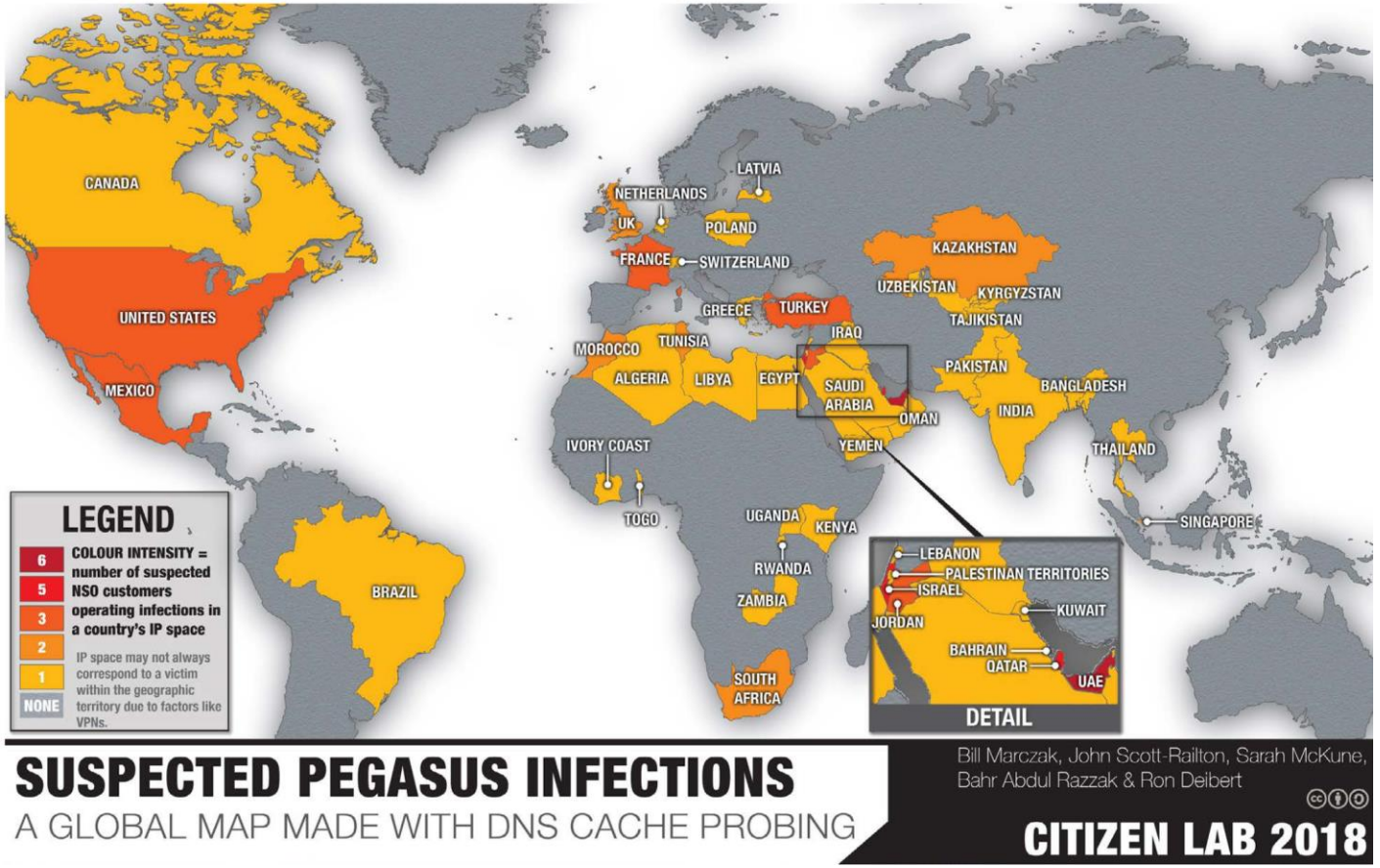
- Jednostavno korisničko sučelje za napadača
  - Dovoljno samo upisati broj mobitela žrtve
- Potpuni nadzor uređaj i eksfiltracije podataka na C2 server
- Ugrađena detekcija je li špijunski programi instaliran na krivom uređaju, provjerava broj na SIM kartici
- Može se sam izbrisati automatski ili na naredbu
  - Ako 60 dana nije mogao pristupiti C2 serveru, automatski se briše

Korištenje Pegasusa u divljini (1)

- Curenje podataka u srpnju 2021. otkrilo:
  - 50k potencijalnih žrtava špijunaže između 2016. i 07.2021., od kojih je najmanje 200 novinara
  - Tadašnji klijenti su bili sljedećih 11 država: Azerbajdžan, Bahrein, Mađarska, Indija, Kazahstan, Meksiko, Maroko, Ruanda, Saudijska Arabija, Togo, Ujedinjeni Arapski Emirati
- Neki primjeri slučajeva zlouporabe
  - Meksiko – novinar Cecilio Pineda špijuniran tjedne prije ubojstva, još minimalno 25 novinara špijunirano u Meksiku u periodu od dvije godine
  - Azerbajdžan - 40 novinara špijunirano, jedan novinar praćen dvije godine
  - Napadnuti i novinari CNN-a, The New York Timesa i Reutersa

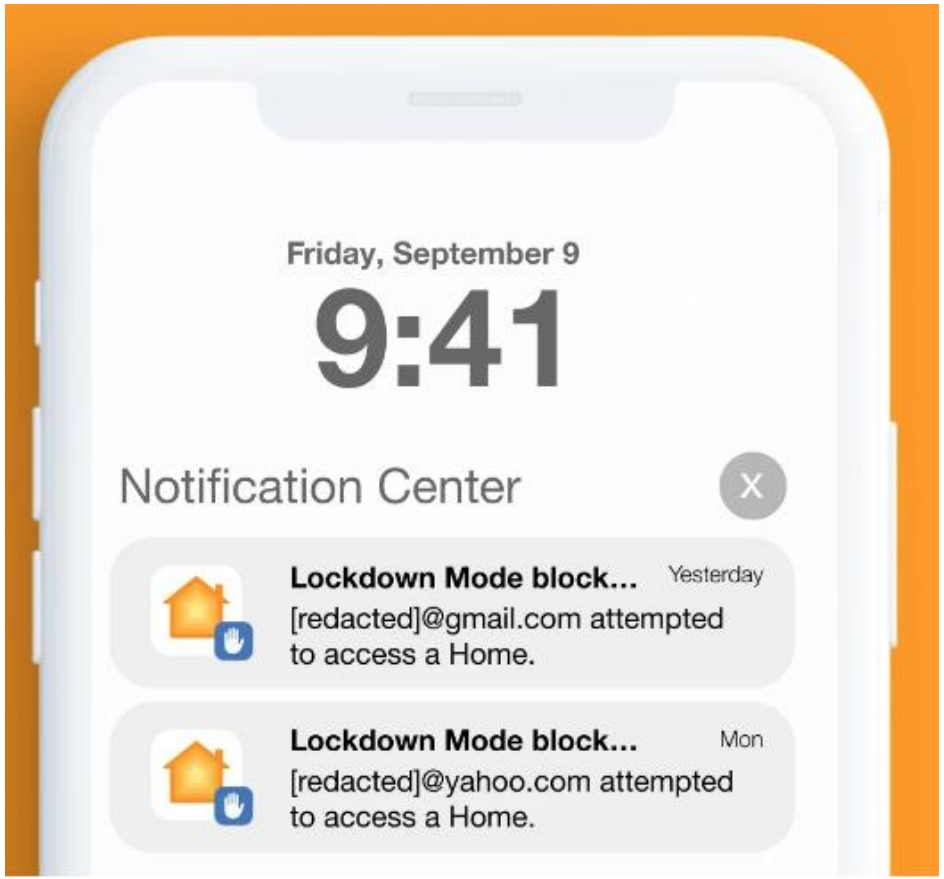
Korištenje Pegasusa u divljini (2)

- Prikaz žrtava po državama do 2018. godine



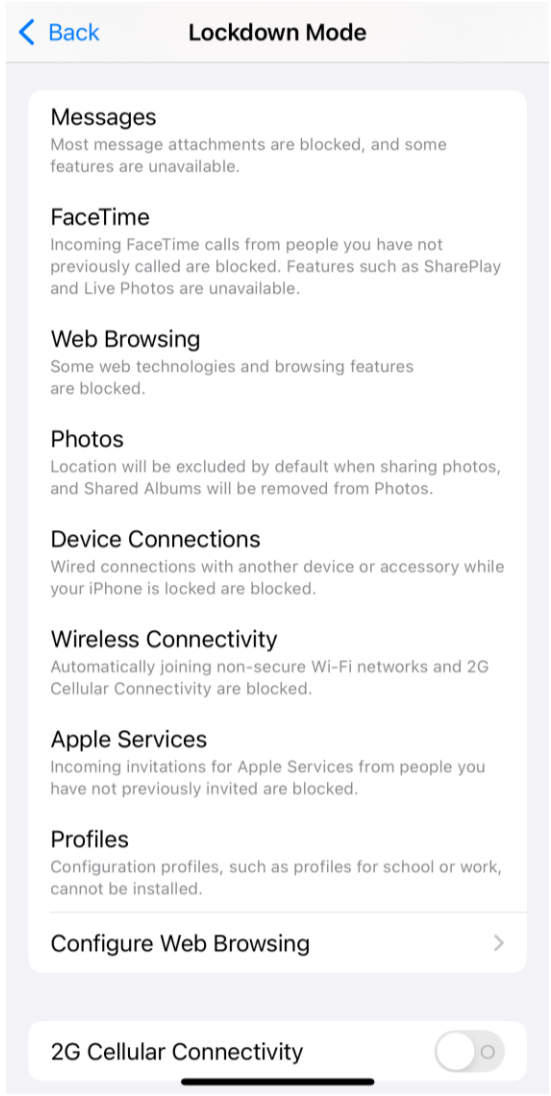
Kako se zaštititi (1)

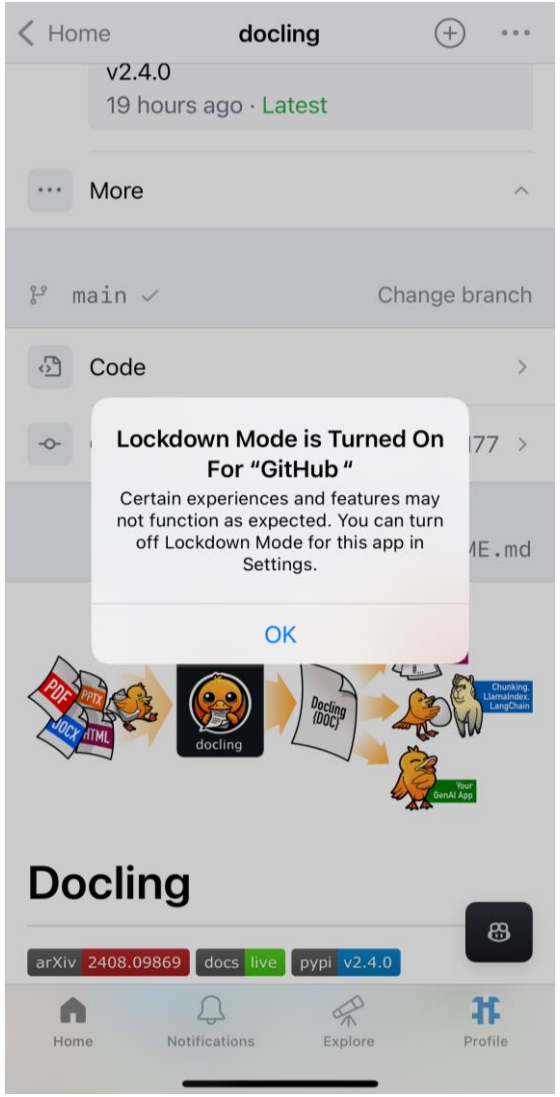
- Obavezno redovito ažurirati
- I Android i iOS imaju ugrađene mehanizme automatskog ažuriranja softvera u slučaju velike ranjivosti
- Appleovi proizvodi imaju tzv. Lockdown mode
  - Spasio od PWNYOURHOME



Kako se zaštititi (2)

- Izgled sučelja za iPhoneov Lockdown mode





Etička pitanja i budući razvoj

- Trebaju li antivirusi prijaviti da su detektirali Pegasus na uređaju?
- Smije li NSO uopće postojati kao profitna firma?
- Od 2020. do 2024. NSO potrošio $3.1M na lobiranje u Washingtonu
  - Minimalno $897K potrošeno samo u 2023.

Zaključak

- Pegasus je napredan špijunski softver kojeg je razvila izraelska firma NSO
- Napada Android i iOS uređaje i konstantno evoluira kako bi mogao raditi na što novijim verzijama operacijskog sustava
- Najveća prijetnja su zero-click ranjivosti koje Pegasus jedino koristi od 2020. i nadalje

Literatura (1)

[1] - John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. “Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware,” Citizen Lab Research Report No. 93, University of Toronto, June 2017. - pristupljeno 1.11.2024.

[3] - Citizen Lab – 08.2016. The Million Dollar Dissident - https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ - pristupljeno 4.11.2024.

[4] - Apple Security – Bounty categories - https://security.apple.com/bounty/categories/, pristupljeno 4.11.2024.

[5] - New York Times – 09.03.2016. How Spy Tech Firms Let Governments See Everything on a Smartphone - https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?referringSource=articleShare - pristupljeno 4.11.2024.

[6] - Kaspersky – 11.04.2017. - Pegasus: The ultimate spyware for iOS and Android - https://www.kaspersky.com/blog/pegasus-spyware/14604/ - pristupljeno 4.11.2024.

Literatura (1)

[7] - Citizen Lab – 13.09.2021. - FORCEDENTRY- https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/ - pristupljeno 4.11.2024.

[8] - Citizen Lab – 18.04.2021. - Triple Threat - https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/ - pristupljeno 4.11.2024.

[9] - Forbidden Labs – 18.07.2021. - Pegasus: The new global weapon for silencing journalists - https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ - pristupljeno 1.11.2024.

[10] -

Dodatna literatura

- Darknet Diaries – 100. NSO - https://darknetdiaries.com/transcript/100/ pristupljeno 1.11.2024.
- Forensic Architecture - Digital Violence: Pegasus Stories - https://www.youtube.com/watch?v=NhwGV1xHt8Y - pristupljeno 4.11.2024.
- Black Hat - Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks - https://www.youtube.com/watch?v=Y6e_ctKqSqM - pristupljeno 4.11.2024.
- Al Jazeera English - Will WhatsApp win its lawsuit against NSO - https://www.youtube.com/watch?v=J1lVL2m_tp0 - pristupljeno 4.11.2024.

Hvala!