PurpleBox

An Extremely Sophisticated Spyware

- PEGASUS -

www.prplbx.com

$whoami

Ömer Faruk Çulha

PurpleBox -> Cyber Security Engineer

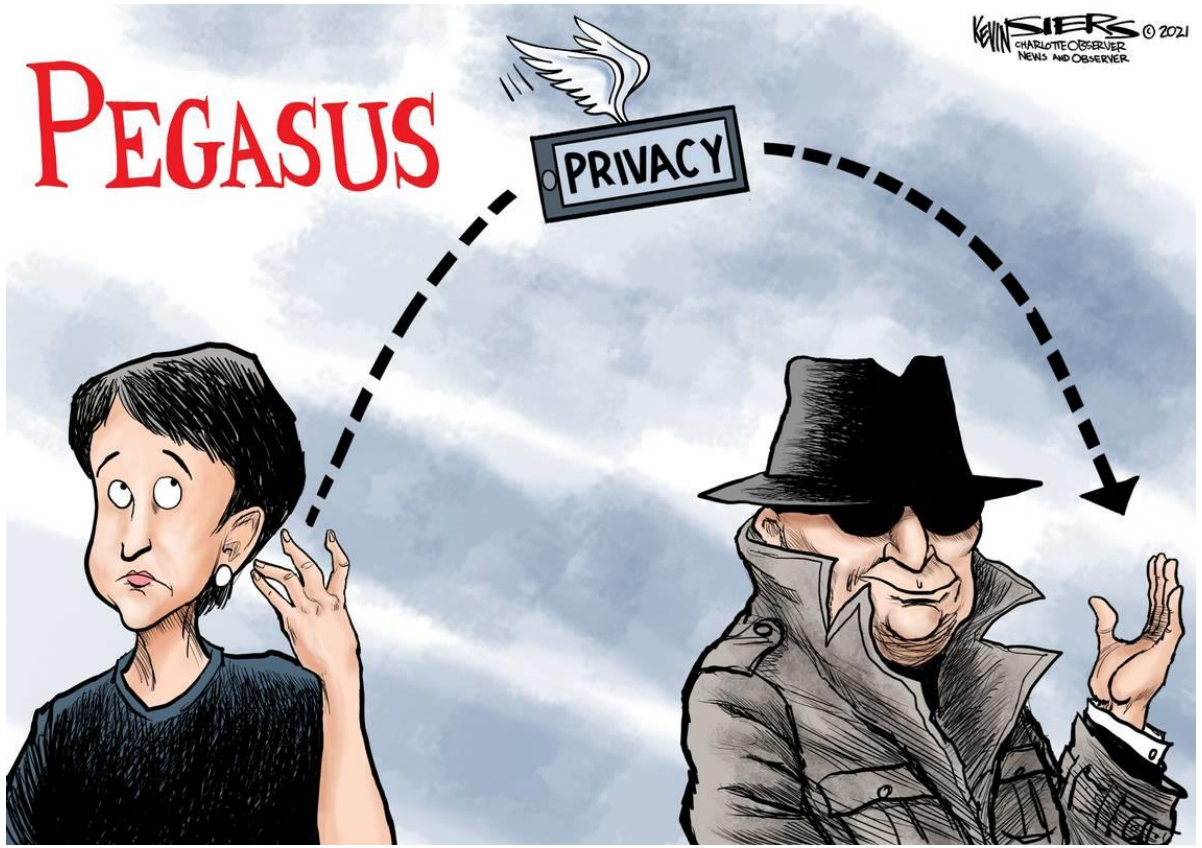
Sakarya Üniversitesi -> Makine Müh.

https://twitter.com/0x1337root

https://tryhackme.com/p/0x1337root

https://www.linkedin.com/in/ömer-faruk-çulha-b95880195

PEGASUS Nedir ?



PEGASUS Kim Tarafından Geliştirildi ?

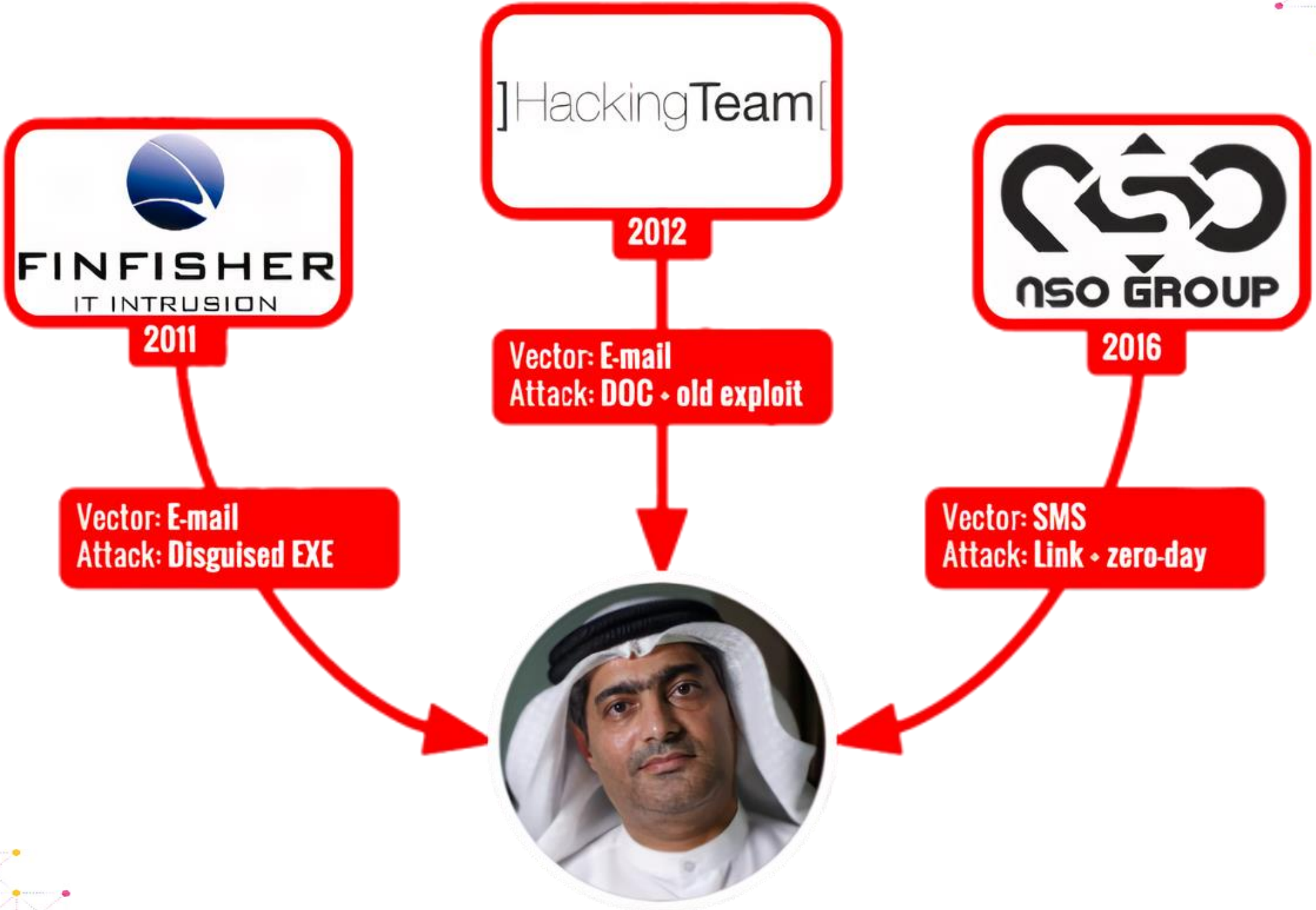
- PEGASUS İsrail merkezli bir siber savaş şirketi olan NSO Group tarafından geliştirilmiştir.
- NSO Group'un bir Amerikan risk sermayesi şirketi olan Francisco Partners Management'a ait olduğu bildiriliyor.

NSO Group Kim ?

- Niv Carmi
- Shalev Hulio
- Omri Lavie
- Kaymera
- NSO Websitesi
- Siber savaşın iki tarafında da oyna

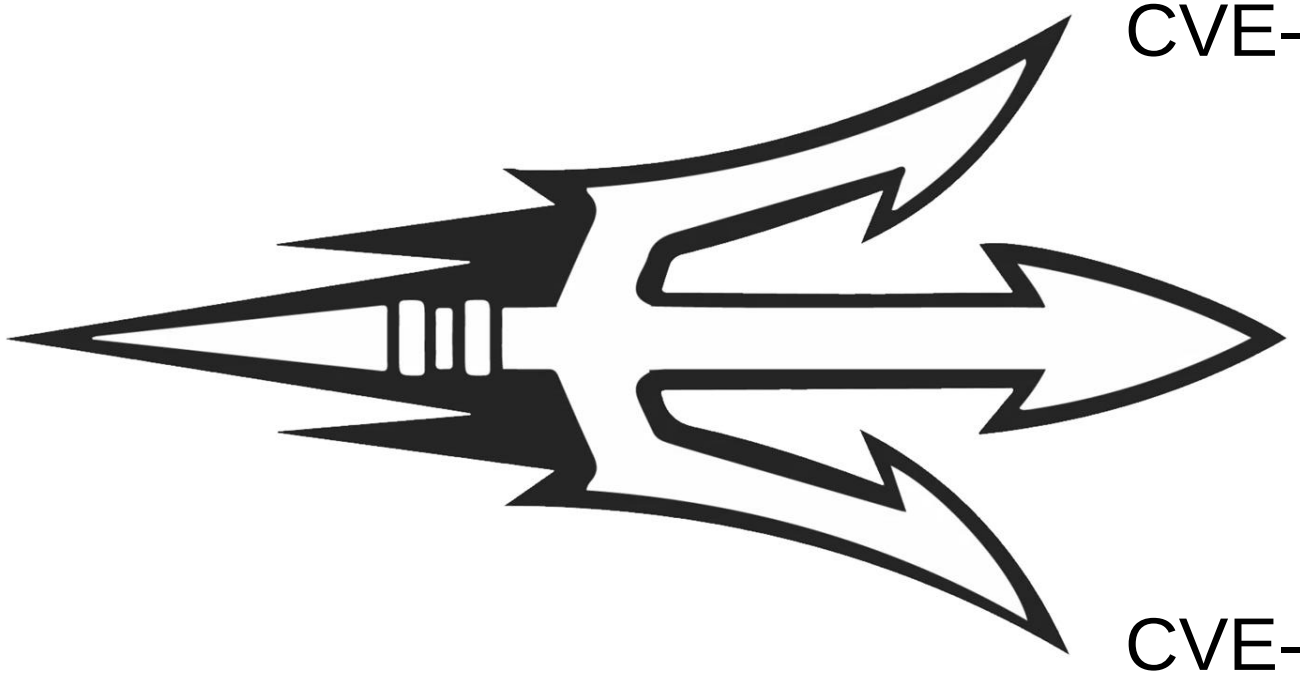
PEGASUS Nasıl Ortaya Çıktı ?

- PEGASUS ilk olarak 10 - 11 Ağustos 2016 yılında, Birleşik Arap Emirlikleri (BAE)' de bulunan Ahmet Mansoor hedef alındığında ortaya çıkmıştır.
- Ahmet Mansoor PEGASUS' tan önce de hedef alınmıştır.


FINFISHER
IT INTRUSION
2011
Vector: E-mail
Attack: Disguised EXE
]HackingTeam[
2012
Vector: E-mail
Attack: DOC • old exploit
NSO GROUP
2016
Vector: SMS
Attack: Link • zero-day

Saldırı Nasıl Gerçekleşti ?

Trident



CVE-2016-4657

CVE-2016-4655

CVE-2016-4656

AŞAMA - 0

- CVE-2016-4657 : WebKit (Safari) için bir exploit. İlk shellcode'un yürütülmesi işini yapıyor.

- CVE-2016-4655 : Temel Kernel adresini bulmak için, Kernel Address Space Layout Randomization (KASLR) bypass exploiti.

- CVE-2016-4656 : Telefonu jailbreaklemeyi, yazılım kurulumuna izin vermeyi ve kernelde kod çalıştırmayı sağlayan 32-bit ve 64-bit iOS kernel exploiti.

AŞAMA - 1

- 10 - 11 Ağustos 2016
- Mansoor iPhone 6 (iOS 9.3.3)
- CitizenLab iPhone 5 (iOS 9.3.3)
- Lookout Security (iOS 9.3.4)
- StealthFalcon
- Pegasus v1 - One Click
- Pegasus v2 - Zero Click


etisalat
10:16 AM
Back (6) +45 609910233
Text Message
Today 9:38 AM
أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
3589003s/


etisalat
2:41 PM
Messages (6) InfoSMS
Text Message
Today 1:44 PM
أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

AŞAMA - 2

- final111
  - CVE-2016-4657
    - WebKit Memory Corruption 0-day
    - Obfuscated JavaScript
    - XMLHttpRequest
    - iPhone 5 <= 32-bit binary
    - iPhone 5s >= 64-bit binary
  - CVE-2016-4655
    - KASLR bypass 0-day
  - CVE-2016-4656
    - Kernel Memory Corruption 0-day
- test111.tar
  - Payload

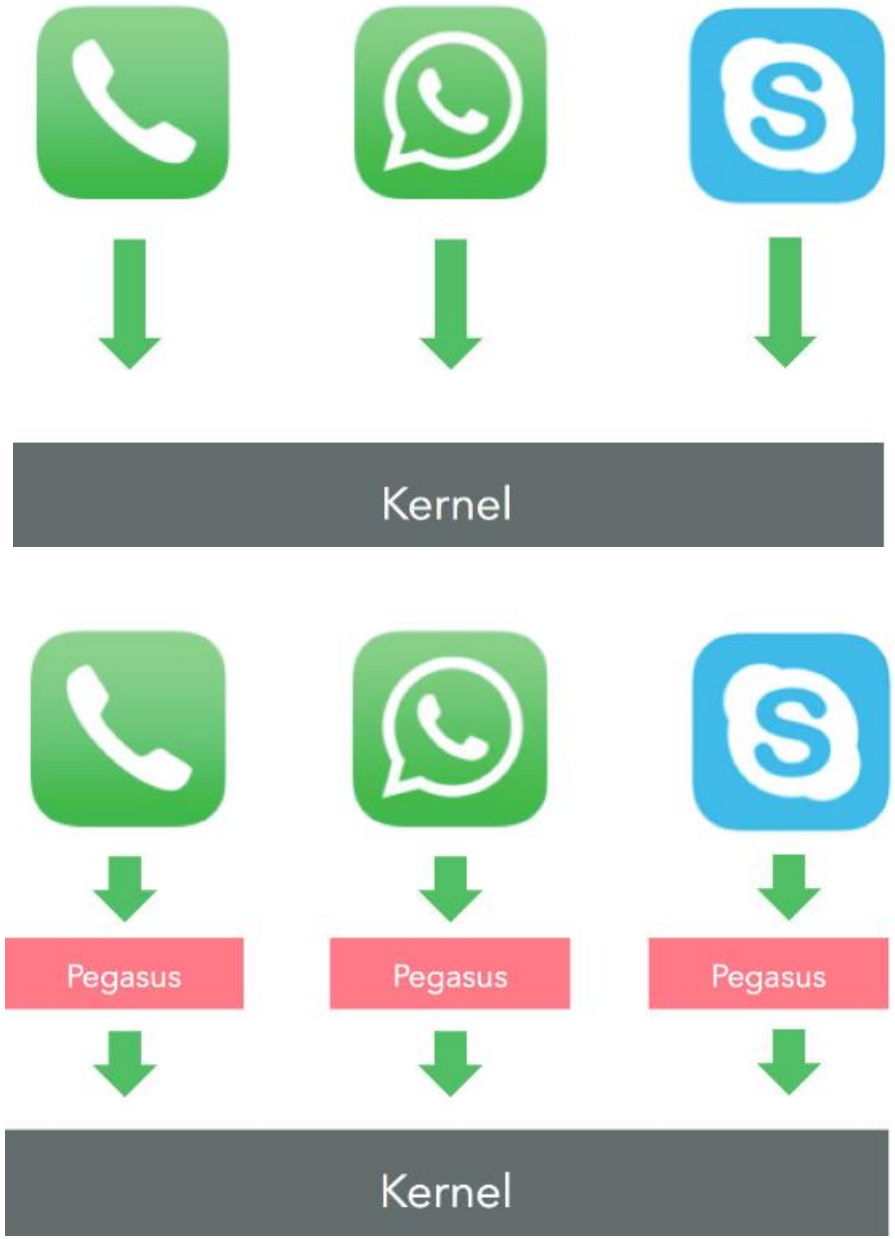
```
GET /[redacted]/ HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /[redacted]/ntf_xps.html&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=1&nocache=[redacted] HTTP/1.1
GET /[redacted]//final111?&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=2&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=[redacted]&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK  (application/octet-stream)
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=3&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
HTTP/1.1 200 OK
GET /[redacted]/ntf_gog.html?a=568_320_2_SGX543&b=4&nocache=[redacted] HTTP/1.1
GET /[redacted]/ntf_xpe.html&nocache=[redacted] HTTP/1.1
HTTP/1.1 200 OK
HTTP/1.1 200 OK
GET /[redacted]/ntf_bed.html?s=[redacted]&d= HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_brc.html?m=0 HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/ntf_bed.html?s=[redacted]&d=Tring%20to%20download%20bundle%28try%3A0%29 HTTP/1.1
HTTP/1.1 200 OK
GET /[redacted]/test111.tar HTTP/1.1
```

AŞAMA - 2

- Kalıcılık (Persistence)
  - JavaScriptCore Binary
  - Reboot - Restart
  - Apple Updates
  - Jailbreak

AŞAMA - 3

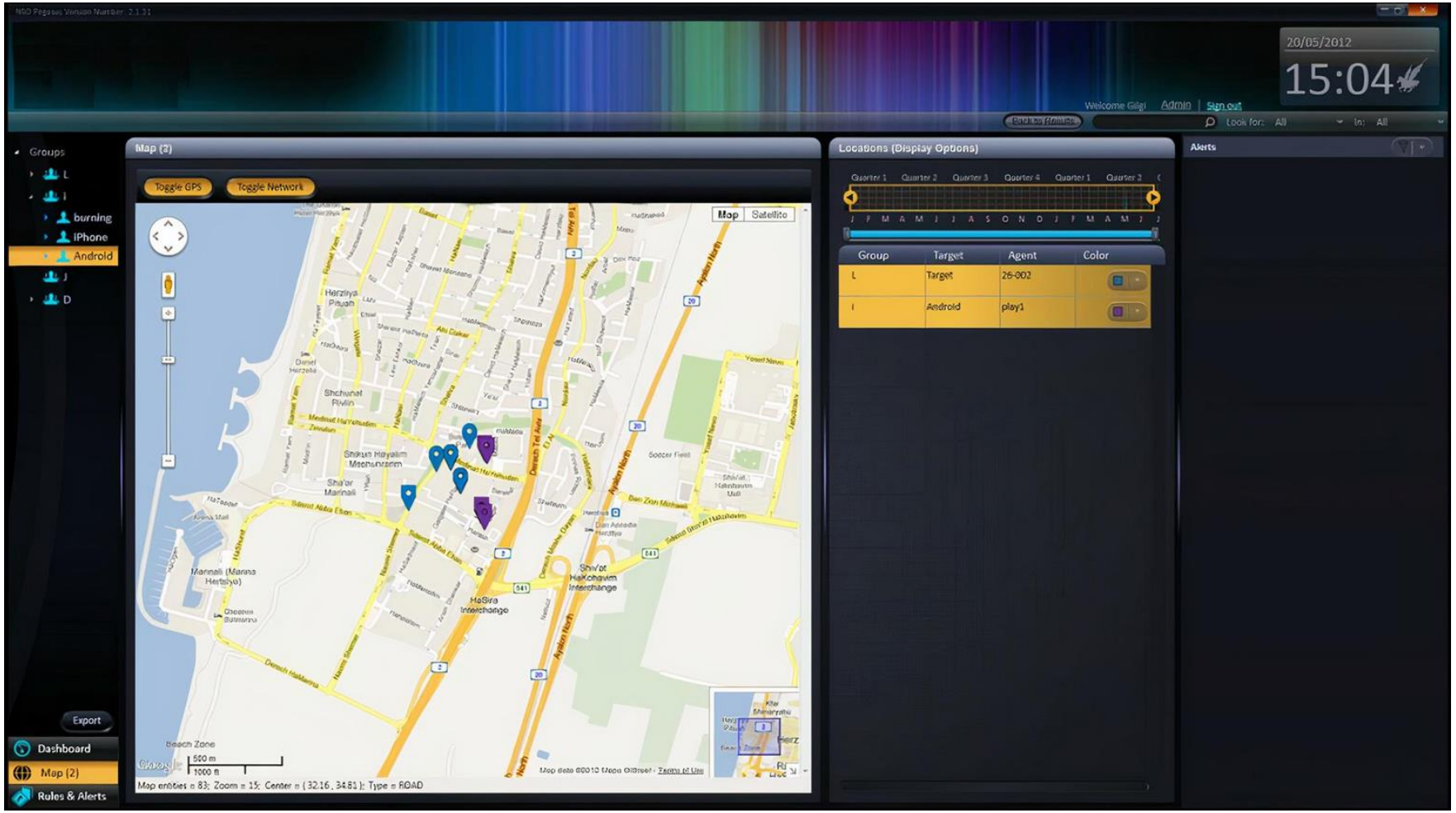
- iOS Uygulama İzinleri
- Hooking Tekniği
- Dynamic Library Injection
- Cydia Substrate Framework



Sızıntı Boyutu Ne Kadar ?

- iMessage
- Facetime
- Gmail
- Viber
- Facebook
- WhatsApp
- Telegram
- Skype
- Line
- KakaoTalk
- WeChat
- Surespot
- Imo.im
- Mail.Ru
- Tango
- VK
- Ok.ru
- Takvim
- GPS
- SMS
- Ağ ve WI-FI dahil kaydedilmiş tüm parolalar
- Telefon aramaları
- Arama Kayıtları
- Ses ve video kaydı
- Kişiler
- Galeri
- Dahili depolama

Komuta & Kontrol Merkezi



- Pegasus Anonymizing Transmission Network (PATN)
- UI
- C&C
- HackingTeam Leakage

Kurtuluşumuz Nedir ?

Referanslar

- https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
- https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

Thank you!
Any Questions?