Smartphone et forensique : Comment attraper Pégasus for fun and non-profit

Etienne Maynier - Amnesty Tech

SSTIC 2022

AMNESTY INTERNATIONAL

La surveillance ciblée

AMNESTY INTERNATIONAL

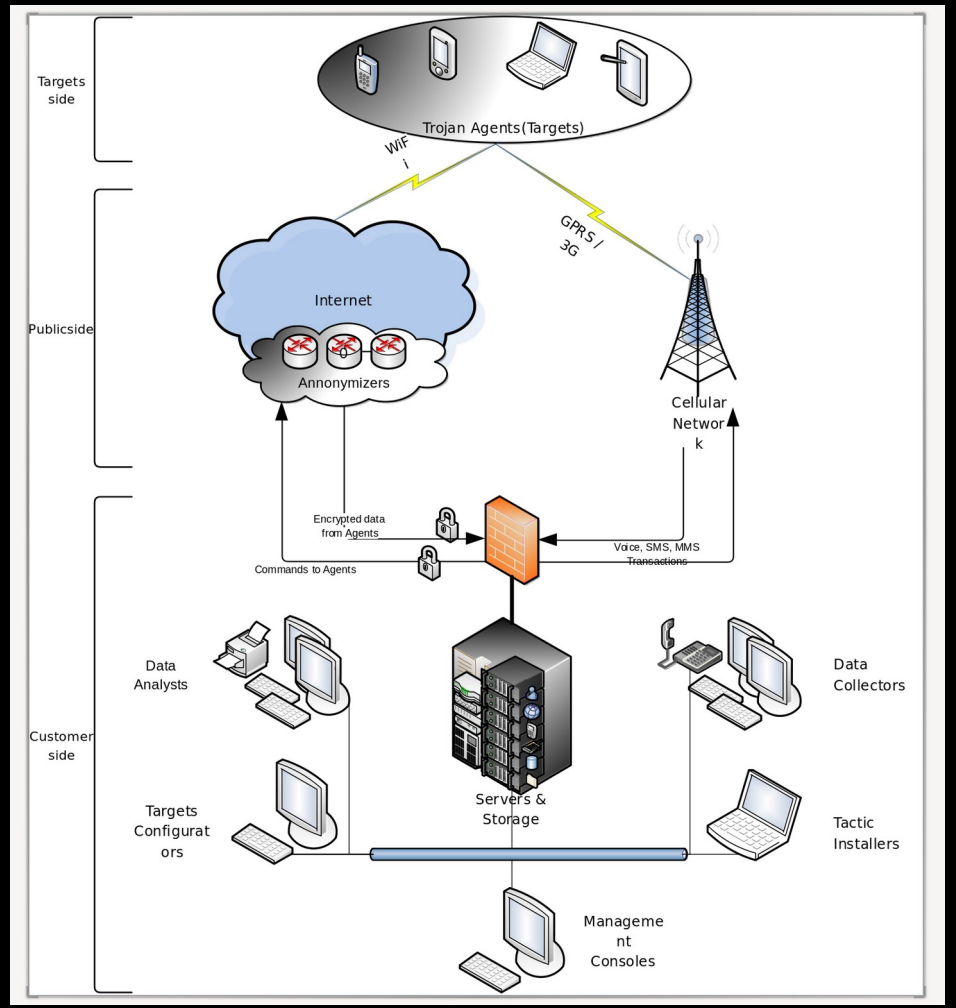
NSO GROUP

ABOUT US GOVERNANCE ECLIPSE NEWS CONFERENCES CONTACT US

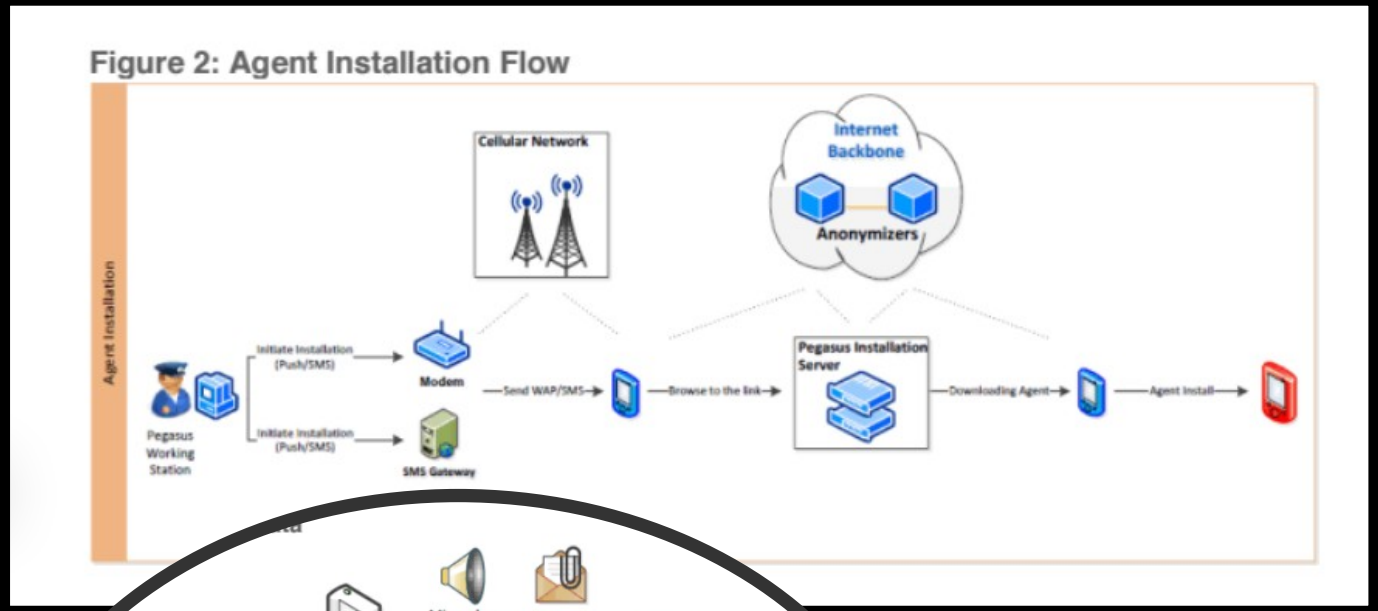
CYBER INTELLIGENCE FOR GLOBAL SECURITY AND STABILITY

NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.

AMNESTY INTERNATIONAL



Pégasus pour BlackBerry (~2010)



Brochure de Pégasus (~2014)

AMNESTY INTERNATIONAL

NSO Group & Pégasus

The Million Dollar Dissident

NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

By Bill Marczak and John Scott-Railton August 24, 2016

Download this report

This report was written with the assistance of the research team at Lookout Security.

Update (Sept 1, 2016): Today Apple released security updates for Desktop Safari and Mac OS X. These updates patch the Trident vulnerabilities that identified in this report for desktop users. The Trident vulnerabilities used by NSO could have been weaponized against users of non iOS devices, including OSX. **We encourage all Apple users to install the update as soon as possible**. Citizen Lab is not releasing samples of the attack at this time to protect the integrity of still-ongoing investigations.

This report describes how a government targeted an internationally recognized human rights defender, Ahmed Mansoor, with the Trident, a chain of zero-day exploits designed to infect his iPhone with sophisticated commercial spyware.

Source: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

AMNESTY INTERNATIONAL

NSO Group & Pégasus

Ahmed Mansoor

AMNESTY INTERNATIONAL

Amnesty & NSO

هل بالامكان عمل تغطية لاخوانك
المعتقلين في سجون السعودية امام
السفارة السعودية في واشنطن

انا اخوي معتقل في رمضان وانا مبتعثه
هناك فارجو ان لا يتم ارتباطي بالموضوع
https://akhbar-arabia.com/

تغطية للمظاهرات الان وستبدا بعد اقل من
ساعه

محتاجين دعمك لو سمحت

SHARE

< RESEARCH

August 1, 2018 1:19 pm

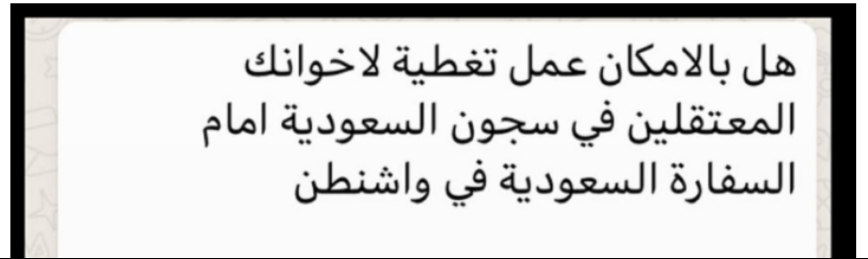
Amnesty International Among Targets of NSO-powered Campaign

Summary

In June 2018, an Amnesty International staff member received a malicious WhatsApp message with Saudi Arabia-related bait content and carrying links Amnesty International believes are used to distribute and deploy sophisticated mobile spyware. Through the course of our subsequent investigation we discovered that a Saudi activist based abroad had also received similar malicious messages. In its analysis of these messages, Amnesty International found connections with a network of over 600 domain names. Not only are these domain names suspicious, but they also overlap with infrastructure that had previously been identified as part of Pegasus, a sophisticated commercial exploitation and spyware platform sold by the Israel surveillance vendor, NSO Group.

Malicious Messages sent to Activists working on Human Rights in Saudi Arabia

In early June, an Amnesty International staff member received a suspicious message on their personal mobile device. The message, delivered through the WhatsApp messenger, carried a malicious link which Amnesty International believes belongs to infrastructure connected with NSO Group and previously documented attacks (see below for more information on these connections).



Recently added

- Qatar: Ensure fair trial for Abdullah Ibhais
- Write for Rights: Celebrating 20 years of change
- Write for Rights: World's biggest human rights campaign marks 20th birthday
- Iran: Release arbitrarily detained rights activist at imminent risk of flogging
- Pakistan: Legalization of forced chemical castration a cruel and retrograde step

AMNESTY INTERNATIONAL

Amnesty & NSO

AmnestyTech / **investigations** Public

Edit Pins | Unwatch 90 | Fork 162

Code | Issues 1 | Pull requests | Actions | Projects | Wiki | Security | Insights

master | **investigations** / 2018-08-01_nso / **indicators.csv** | Go to file | ...

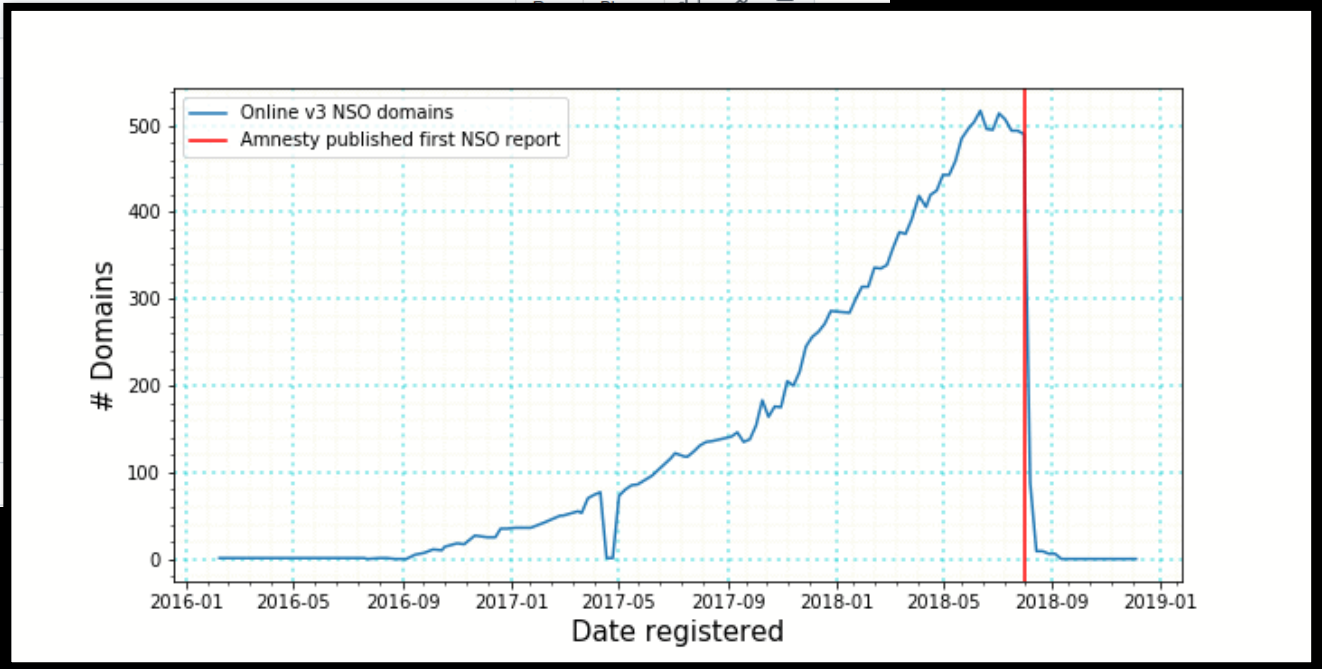
botherder First commit — Latest commit `50bfc1f` on Oct 1, 2018 — **History**

1 contributor

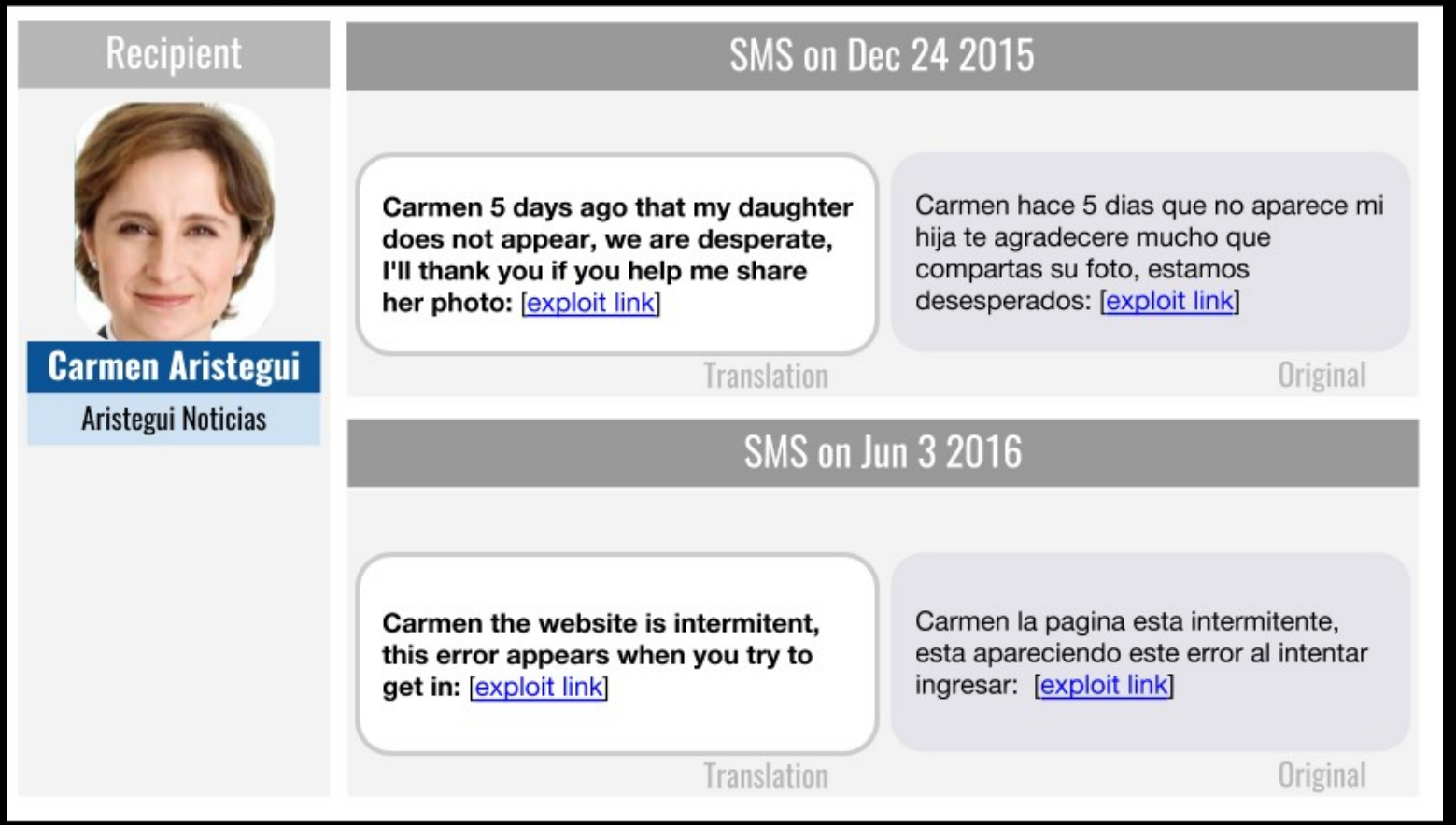
605 lines (605 sloc) | 21.3 KB

Search this file...

	domain_name
1	**domain_name**
2	14-tracking.com
3	1minto-start.com
4	24-7clinic.com
5	3driving.com
6	456h612i458g.com
7	7style.org
8	800health.net
9	access.dynamic-dns.net
10	accountnotify.com



Pégasus au Mexique



RECKLESS EXPLOIT: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware

Scott-Railton J, Marczak B, Abdulrazzak B, Crete-Nishihata M & Deibert R

CITIZEN LAB 2017

AMNESTY INTERNATIONAL

Pégasus au Maroc

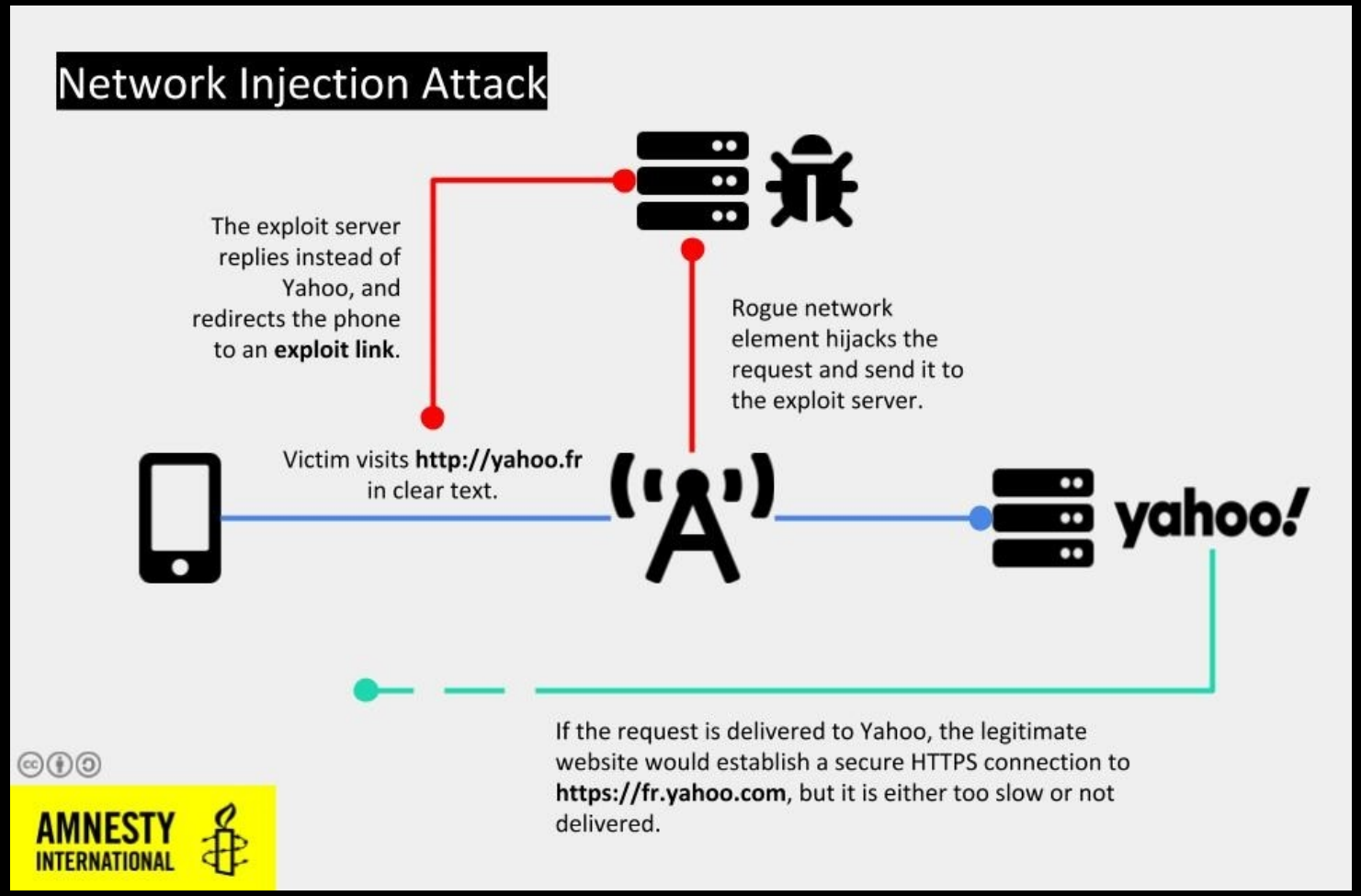
Maati Monjib

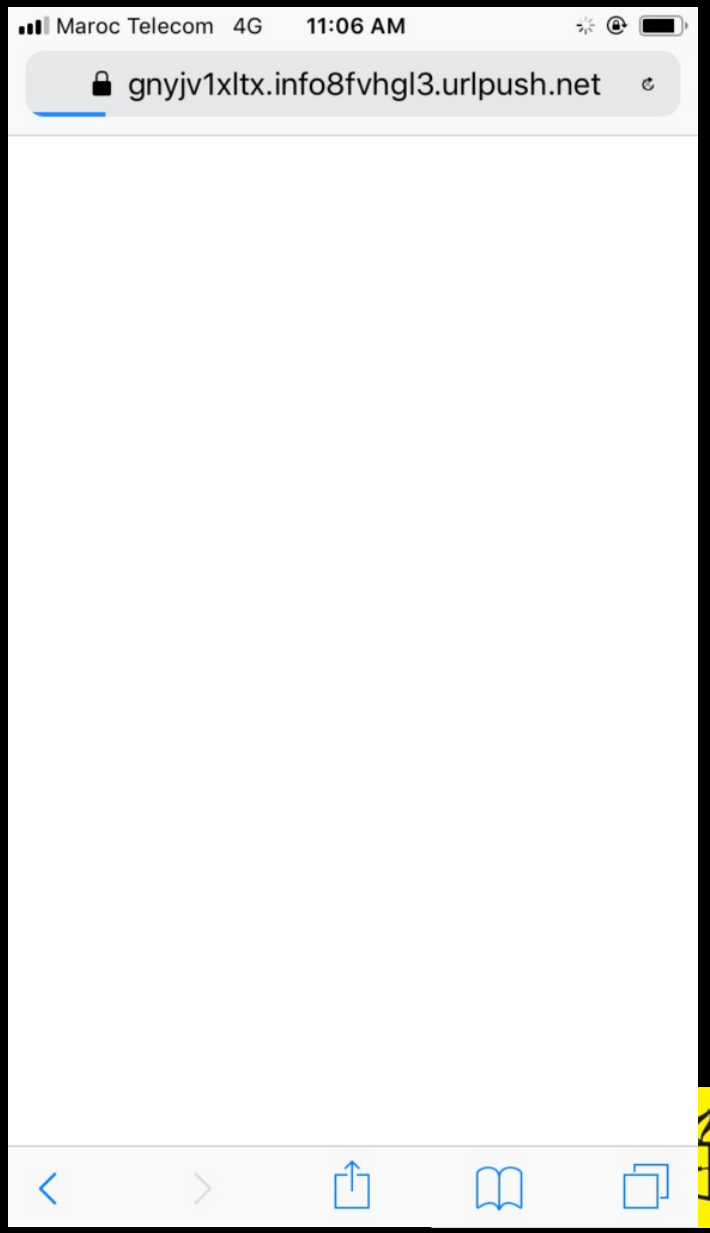
Human Rights Defender

		Translation
2 Nov 2017 at 12:29	Truecaller à le plaisir de vous annoncer l'ajout d'une nouvelle functionnalité, consulter le noms des personnes qui ont cherché votre numéro durant une semaine http://tinyurl.com/redacted	Truecaller has the pleasure to announce the addition of a new functionality, check the name of the people who searched your number in the last week. [exploit link]
15 Nov 2017 at 17:05	فضيحة أخلاقية داخل مقهى بورتز في حي أكدال بالرباطلمشاهدة الفيديو الذي يوثق الفضيحةhttps://videosdownload.co/redacted	A moral scandal inside Portz Café in the Agdal district in Rabat. To see the video documenting the scandal. [exploit link]
7 Dec 2017 at 18:21	ALQODS RESTERA TOUJOURS LA CAPITALE DE LA PALESTINE SAUVEZ LA VILLE SAINTE EN SIGNANT CETTE PETITION http://tinyurl.com/redacted	Jerusalem will remain the capital of Palestine Save the holy city by signing this petition. [exploit link]
8 Jan 2018 at 12:58	Urgent le livre sur Donald Trump s est arrache dans toutes les libraires une version arabe est disponible gratuitement sur le lien http://tinyurl.com/redacted	Urgent the book on Donald Trump is selling fast in all book shops an arabic version is available for free at the following link. [exploit link]

AMNESTY INTERNATIONAL

Pégasus au Maroc





http://yahoo[.]fr redirected to
hxxps://bun54l2b67.get1tn0w.free247downloads[.]com:30495/szev4hz

WhatsApp

PIXELS · WHATSAPP

Partage

WhatsApp dépose une plainte contre l'entreprise israélienne NSO Group, accusée d'espionnage

NSO Groupe aurait directement contribué à une série d'appels « infectés », qui ont ciblé des militants des droits de l'homme et des journalistes en exploitant une faille de l'application, dénonce le dirigeant de WhatsApp.

Par Michaël Szadkowski (avec AFP)

Publié le 30 octobre 2019 à 15h39 - Mis à jour le 30 octobre 2019 à 16h48 · Lecture 3 min.

Ils ont ciblé, avant mai 2019, *« 100 défenseurs des droits humains, journalistes et autres membres de la société civile dans le monde »*, précise Will Cathcart. En tout, 1 400 appareils ont été infectés du 29 avril au 10 mai dans différents pays, dont le royaume de Bahreïn, les Emirats arabes unis et le Mexique, d'après la plainte déposée par WhatsApp devant une cour fédérale, lisible en intégralité sur le *Washington Post*.

AMNESTY INTERNATIONAL

Projet Pégasus

Investigation mondiale sur les abus permis par NSO Group

Coordonné par Forbidden Stories avec la participation de 17 Média, Amnesty International étant le partenaire technique du projet

Investigation basée sur 50000 numéros de téléphones de cibles potentielles de clients de NSO Group

Analyse de 67 téléphones pendant le projet, 37 avec des traces de Pégasus (ciblage ou infection)

De Rabat à Paris, le Maroc ne lâche pas les journalistes

Par Damien Leloup

En Hongrie, le pouvoir vise les journalistes et les patrons de presse

Par Jean-Baptiste Chastand (Budapest, envoyé spécial)

Affaire Khashoggi : deux femmes proches du journaliste assassiné ont été surveillées par Pegasus

Par Arthur Bouvart (Forbidden Stories) et Dana Priest (The Washington Post)

Méthodologie forensique

SHARE

< RESEARCH

July 18, 2021 5:00 pm

Forensic Methodology Report: How to catch NSO Group's Pegasus

A copy of this report is available for download here.

Introduction

NSO Group claims that its Pegasus spyware is only used to "investigate terrorism and crime" and "leaves no traces whatsoever". This Forensic Methodology Report shows that neither of these statements are true. This report accompanies the release of the Pegasus Project, a collaborative investigation that involves more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories with technical support of Amnesty International's Security Lab.[1]

Amnesty International's Security Lab has performed in-depth forensic analysis of numerous mobile devices from human rights defenders (HRDs) and journalists around the world. This research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using NSO Group's Pegasus spyware.

As laid out in the UN Guiding Principles on Business and Human Rights, NSO Group should urgently take pro-active steps to ensure that it does not cause or contribute to human rights abuses within its global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs and journalists do not continue to become targets of unlawful surveillance.

In this Forensic Methodology Report, Amnesty International is sharing its methodology and publishing an open-source mobile forensics tool and detailed technical indicators, in order to assist information security researchers and civil society with detecting and responding to these serious threats.

This report documents the forensic traces left on iOS and Android devices following targeting with the Pegasus spyware. This includes forensic records linking recent Pegasus infections back to the 2016 Pegasus payload used to target the HRD Ahmed Mansoor.

Recently added

- Qatar: Ensure fair trial for Abdullah Ibhais
- Write for Rights: Celebrating 20 years of change
- Write for Rights: World's biggest human rights campaign marks 20th birthday
- Iran: Release arbitrarily detained rights activist at imminent risk of flogging
- Pakistan: Legalization of forced chemical castration a cruel and retrograde step

AMNESTY INTERNATIONAL

Méthodologie Forensique

Comment accéder aux données ?

Quels artefacts forensiques ?

Spécificités iPhone / Android

AMNESTY INTERNATIONAL

Accès aux données

Dans la vraie vie :

- Jailbreak / root : très compliqué
- Sous iPhone : backups
- Sous Android : ?

AMNESTY INTERNATIONAL

Méthodologie

Plusieurs défis :

- Pas de sample récent de Pégasus
- Peu d'analyses de malware type Pégasus
- Communauté forensique très orientée sur du travail policier

AMNESTY INTERNATIONAL

Méthodologie

Sous iPhone :

- Récupération de backups chiffrés
- Déchiffrement et analyse des backups

AMNESTY INTERNATIONAL

Mobile Verification Toolkit (MVT)

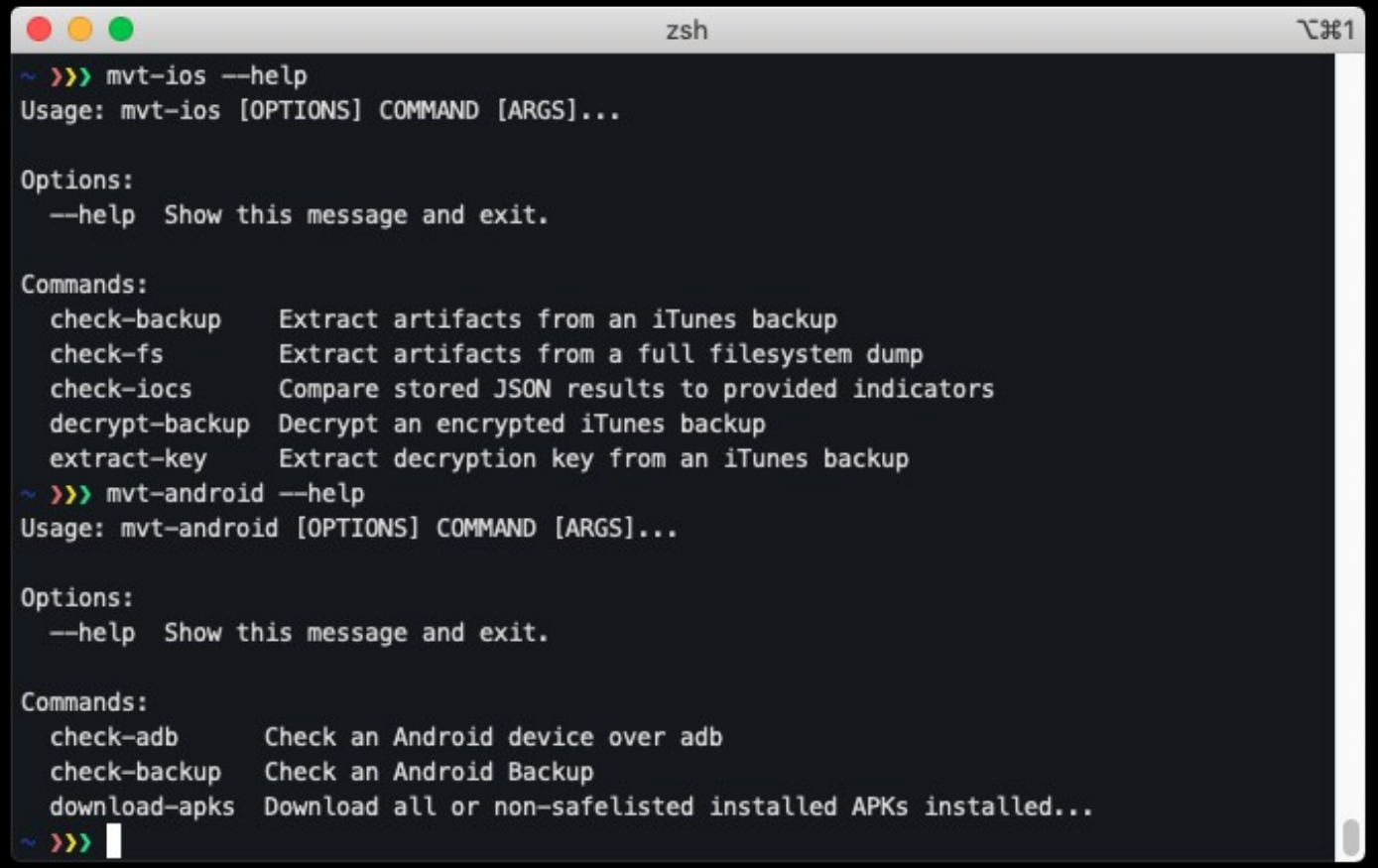
- MVT est un outil open-source pour simplifier l'analyse de smartphones à la recherche de traces de spyware

https://github.com/mvt-project/mvt

- Licence demandant le consentement du/de la propriétaire du téléphone

- Et des indicateurs

Mobile Verification Toolkit (MVT)



En Python :

pip3 install mvt

Usage:

$ mvt-ios check-backup –i iocs.stix2 –o ./results ./backup

AMNESTY INTERNATIONAL

MVT: liens malveillants dans les SMS

- Liens malveillants envoyés par SMS menant à une exploitation du navigateur
- **Surtout utilisé entre 2016 et 2018**
- Des liens trouvés de 2014 à 2020

```
14:28:53 INFO     [mvt.ios.modules.mixed.sms] Found SMS database at path: ./private/var/mobile/Library/SMS/sms.db
         INFO     [mvt.ios.modules.mixed.sms] Extracted a total of 193 SMS messages containing links
14:28:55 WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Maybe found a known suspicious domain: Https://stopsms.biz/vi78ELI
14:29:01 WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain https://revolution-news.co/ikXFZ34ca shortened as http://tinyurl.com/y73qr7mb
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain: https://stopsms.biz/vi78ELI
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain: https://videosdownload.co/nBBJBIP
14:29:02 WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain https://business-today.info/k8mc8FJpz shortened as http://tinyurl.com/y93yg2sc
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain: https://stopsms.biz/2Kj2ik6
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain: https://hmizat.co/ronEKDVaf
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain https://infospress.com/Ln3HYK4C shortened as http://tinyurl.com/y7wdcd8z
14:29:03 WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain: https://infospress.com/LQoHgMCEE
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain https://hmizat.co/JaCTkfEp shortened as http://tinyurl.com/y9hbdqm5
14:29:04 WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain https://infospress.com/asjmXqiS shortened as http://tinyurl.com/y87hnl3o
         WARNING  [mvt.ios.modules.mixed.sms] Found a known suspicious domain: https://stopsms.biz/yTnWt1Ct
```

MVT: Historique de navigation

- L'historique de navigation est inclus dans les backups chiffrés d'iPhones
- Utile pour identifier de l'injection de trafic réseau ou un clic sur un lien

```
INFO     [mvt.ios.modules.mixed.safari_history] Found HTTP redirect to different domain: "yahoo.fr" ->
         "bun54l2b67.get1tn0w.free247downloads.com:30495"
WARNING  [mvt.ios.modules.mixed.safari_history] Redirect took less than a second! (2 milliseconds)
INFO     [mvt.ios.modules.mixed.safari_history] Found HTTP redirect to different domain: "yahoo.fr" -> "fr.yahoo.com"
WARNING  [mvt.ios.modules.mixed.safari_history] Redirect took less than a second! (1 milliseconds)
WARNING  [mvt.ios.modules.mixed.safari_history] Found a sub-domain matching a known suspicious top level:
         https://bun54l2b67.get1tn0w.free247downloads.com:30495/szev4hz
WARNING  [mvt.ios.modules.mixed.safari_history] Found a sub-domain matching a known suspicious top level:
         https://bun54l2b67.get1tn0w.free247downloads.com:30495/szev4hz#048634787343287485982474853012724998054718494423286
```

AMNESTY INTERNATIONAL

MVT: logs réseaux

Plusieurs fichiers enregistrent les processus communiquant avec le réseau

Datausage.sqlite

Com.apple.osanalytics.addaily.plist

Netusage.sqlite (absent des backups)


```
"first_isodate": "2019-04-02 04:51:45.699098",
"isodate": "2019-10-23 03:48:40.716171",
"proc_name": "roleaccountd",
"bundle_id": "",
"proc_id": 351,
"wifi_in": 0.0,
"wifi_out": 0.0,
"wwan_in": 35466.0,
"wwan_out": 16210.0,
"live_id": 88539,
"live_proc_id": 351,
"live_isodate": "2019-07-12 09:07:18.507282"
```


```
Found a known suspicious process name "roleaccountd"
Found a known suspicious process name "roleaccountd"
Found a known suspicious process name "stagingd"
Found a known suspicious process name "stagingd"
Found a known suspicious process name "fdlibframed"
Found a known suspicious process name "xpccfd"
```

AMNESTY INTERNATIONAL

MVT: ID Status Cache

- Contiens des traces de comptes iCloud qui ont interagi avec le téléphone via différents services (iMessage, AirDrop etc.)
- Inclus dans les backups jusqu'à iOS 14.7
- Comptes malveillants propres à chaque client, peut indiquer quelles personnes ont été ciblés par le même client

linakeller2203[@]gmail.com	• FRHRD1 – Claude Mangin • FRPOI3 – Philippe Bouyssou • FRPOI4 • FRPOI5 – Oubi Buchraya Bachir • MOJRN1 – Hicham Mansouri
jessicadavies1345[@]outlook.com	• HUJRN1 – András Szabó • HUJRN2 – Szabolcs Panyi
emmadavies8266[@]gmail.com	• HUJRN1 – András Szabó • HUJRN2 – Szabolcs Panyi
k.williams.enny74[@]gmail.com	• HUPOI1 • HUPOI2 – Adrien Beauduin • HUPOI3

AMNESTY INTERNATIONAL

MVT: Timeline

Permet de voir les liens entre des artefacts sur un téléphone.

Utile pour identifier des traces d'exploits

2019-06-16 12:08:44	Lookup of **bergers.o79@gmail.com** by com.apple.madrid (iMessage)
2019-08-16 12:33:52	Lookup of bergers.o79@gmail**\x00\x00**om by com.apple.madrid (iMessage)
2019-08-16 12:37:55	The file *Library/Preferences/com.apple.CrashReporter.plist* is created within RootDomain
2019-08-16 12:41:25	The file *Library/Preferences/roleaccountd.plist* is created within RootDomain
2019-08-16 12:41:36	Process: **roleaccountd**
2019-08-16 12:41:52	Process: **stagingd**
2019-08-16 12:49:21	Process: **aggregatenotd**

AMNESTY INTERNATIONAL

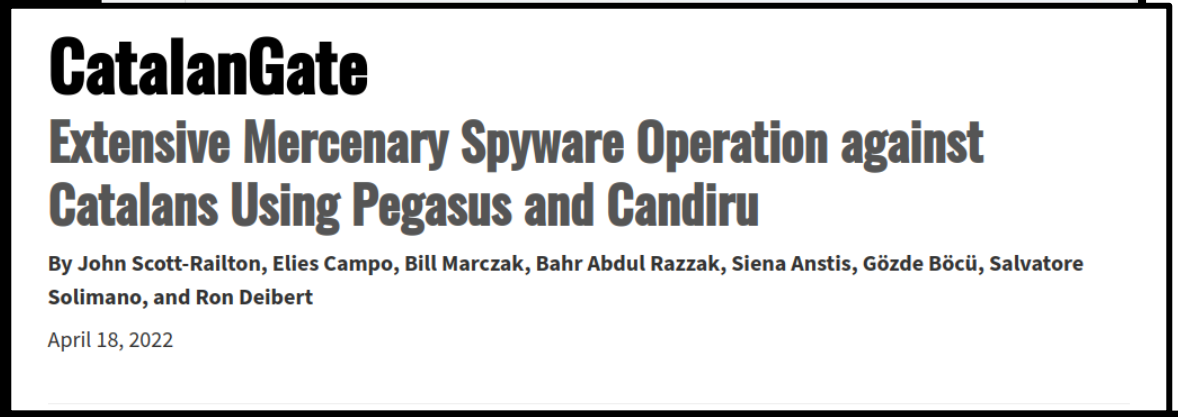
MVT: Mégalodon / FORCEDENTRY

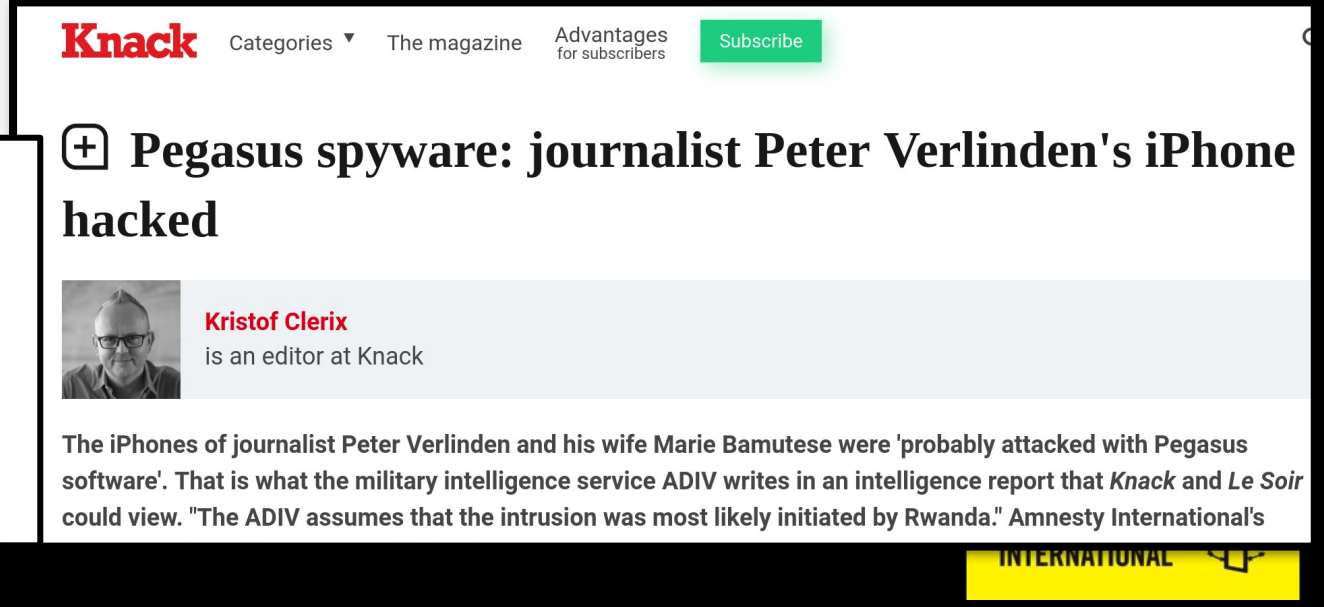
Exploit dans iMessage en 2021.
Fichiers identifiés
par Citizen Lab et corrigé
par Apple en septembre 2021

CVE-2021-30860 (iOS 14.8)

Date (UTC)	Event
2021-05-17 13:39:16	Lookup for iCloud account **benjiburns8[@]gmail.com** (iMessage)
2021-05-17 13:40:12	File: /private/var/mobile/Library/SMS/Attachments/dc/12/DEAE6789-0AC4-41A9-A91C-5A9086E406A5/.eBDOuIN1wq.gif-2hN9
2021-05-17 13:40:21	File: /private/var/mobile/Library/SMS/Attachments/41/01/D146B32E-CA53-41C5-BF61-55E0FA6F5FF3/.TJi3fIbHYN.gif-bMJq
…	…
2021-05-17 13:44:19	File: /private/var/mobile/Library/SMS/Attachments/42/02/45F922B7-E819-4B88-B79A-0FEE289701EE/.v74ViRNkCG.gif-V678

Suite au projet Pégasus






U.S. Department of Commerce
Bureaus and offices • Contact us
Search
Search
BOUT
ISSUES
NEWS
DATA AND REPORTS
WORK WITH US
Home » News » Press Releases
releases
Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities


PRESS RELEASE
November 23, 2021
Apple sues NSO Group to curb the abuse of state-sponsored spyware
Apple also announced a $10 million contribution to support cybersurveillance researchers and advocates


Menu
Search
Bloomberg
Sign In
Technology
Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop
Davide Scigliuzzo
November 22, 2021, 9:31 PM UTC
Moody's cuts company's credit rating by two notches to Caa2
NSO at risk of covenant breach on about $500 million of debt
LIVE ON BLOOMBERG
Watch Live TV
Listen to Live Radio
LISTEN TO ARTICLE
1:47
SHARE THIS ARTICLE
NSO Group is facing a growing risk of default on around $500 million of debt amid a cash burn that's expected to continue this year after new export restrictions from the U.S., according to Moody's Investors Service.


MNESTY
INTERNATIONAL

Une entreprise parmi d'autres

Candiru

Et maintenant ?

- Trop d'abus depuis trop longtemps
- Besoin de plus de collaboration entre ONG, la communauté technique et les grandes plateformes
- On ne règlera pas ce problème uniquement avec de la technologie

AMNESTY INTERNATIONAL

Merci !

Etienne Maynier

etienne.maynier@amnesty.org

@tenacioustek

Samples et infos à

share@amnesty.tech

AMNESTY INTERNATIONAL