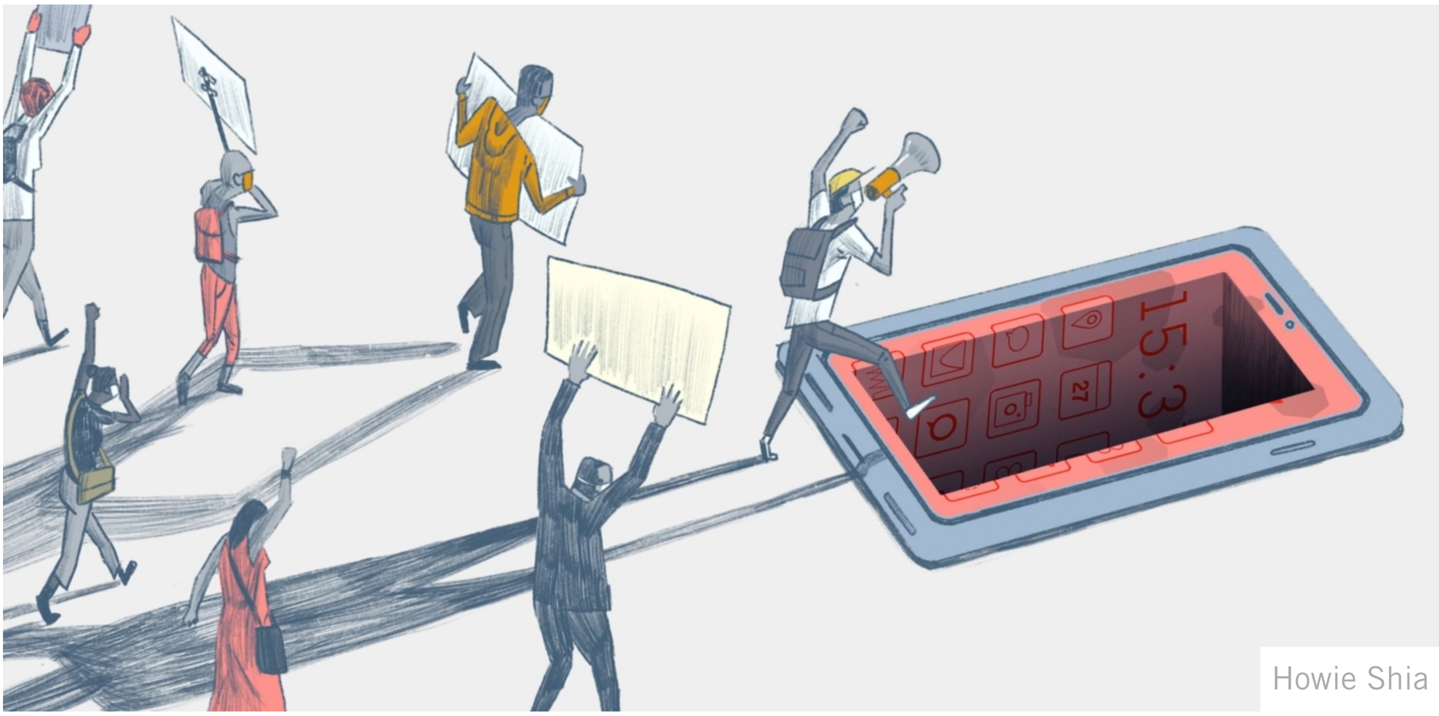
Which language would you like to use this site in? CLOSE

ENGLISH ESPAÑOL FRANÇAIS العربية



Howie Shia

August 6, 2021

Appendix E – Pegasus Forensic Traces per Target Identified in the Aftermath of the Pegasus Project Revelations

This document is an appendix to the research report "**Forensic Methodology Report: How to catch NSO Group's Pegasus**", published as part of the **Pegasus Project**. It contains forensic analysis conducted by Amnesty Tech's Security Lab of the mobile devices of individuals targeted with NSO Group's Pegasus spyware who were identified after the launch of the Pegasus Project on 18 July 2021.

The analysis in this appendix has been published with the informed consent of the individuals whose phones were targeted.

Forensic traces

Forensic traces for AZHRD1 – Anar Mammadli

Date (UTC)	Event
2021-01-15 13:14:54	Process: **payload**
2021-01-15 13:14:55	Process: **payload**
2021-01-15 13:14:55	Process: **bh** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 0.00 MB, WWAN OUT: 0.00 MB)
2021-01-15 13:14:57	Process: **payload**
2021-02-22 13:47:11	Process: **appccntd**

Forensic traces for AZJRN3 – Aziz Orujov

Date (UTC)	Event
2019-06-21 15:47:28	File Library/Preferences/**com.apple.CrashReporter.plist** created in RootDomain

2019-06-21 15:47:46
File Library/Preferences/**roleaccountd.plist** created in RootDomain
2019-06-21 15:47:56
Process: **roleaccountd** (WIFI IN: 0.03 MB, WIFI OUT: 0.01 MB, WWAN IN: 0.10 MB, WWAN OUT: 0.05 MB)
2019-06-21 15:47:56
Process: **stagingd** (WIFI IN: 7.32 MB, WIFI OUT: 0.39 MB, WWAN IN: 27.74 MB, WWAN OUT: 1.29 MB)
2019-06-21 15:48:27
Process record deleted from ZPROCESS (IN: 2.43 MB, OUT: 17.64 MB)
2019-06-24 05:50:44
Process record deleted from ZPROCESS (IN: 0.11 MB, OUT: 0.82 MB)
2019-06-25 06:42:14
Process record deleted from ZPROCESS (IN: 2.19 MB, OUT: 2.15 MB)
2019-06-26 07:19:46
Process record deleted from ZPROCESS (IN: 1.55 MB, OUT: 2.23 MB)
2019-07-09 06:11:57
Process record deleted from ZPROCESS (IN: 2.56 MB, OUT: 2.35 MB)
2019-07-16 13:01:37

Process record deleted from ZPROCESS (IN: 8.74 MB, OUT: 11.78 MB)
2019-07-17 06:43:31
Process record deleted from ZPROCESS (IN: 2.07 MB, OUT: 2.14 MB)
2019-07-18 07:54:36
Process record deleted from ZPROCESS (IN: 1.23 MB, OUT: 2.09 MB)
2019-07-21 09:20:44
Process record deleted from ZPROCESS (IN: 6.47 MB, OUT: 5.42 MB)
2019-07-30 10:24:29
Process record deleted from ZPROCESS (IN: 1.78 MB, OUT: 1.67 MB)
2019-08-07 14:15:58
Process record deleted from ZPROCESS (IN: 7.57 MB, OUT: 8.06 MB)
2019-08-10 07:15:39
Process record deleted from ZPROCESS (IN: 3.39 MB, OUT: 3.02 MB)
2019-08-16 06:44:29
Process record deleted from ZPROCESS (IN: 2.77 MB, OUT: 3.63 MB)
2019-08-21 08:27:51
Process record deleted from ZPROCESS (IN: 4.30 MB, OUT: 16.39 MB)
2019-08-24 13:46:43

Process record deleted from ZPROCESS (IN: 4.21 MB, OUT: 21.24 MB)
2019-08-26 07:53:08
Process record deleted from ZPROCESS (IN: 3.03 MB, OUT: 14.72 MB)
2019-08-27 15:00:03
Process: **roleaccountd** (IN: 0.10 MB, OUT: 0.06 MB)
2019-08-27 15:00:06
Process: **roleaccountd**
2019-08-27 15:00:16
Process: **stagingd** (IN: 27.75 MB, OUT: 1.30 MB)
019-08-27 15:00:23
Process: **stagingd**
2019-08-29 15:37:52
Process record deleted from ZPROCESS (IN: 0.27 MB, OUT: 0.81 MB)

Forensic traces for AZHRL1 – Asabali Mustafayev

Date (UTC)
Event
2019-04-29 06:08:05

iMessage lookup for account **f\x00\x00ip.bl82[@]gmail.com** (filip.bl82[@]gmail.com)
2019-04-29 06:11:50
File Library/Preferences/**com.apple.CrashReporter.plist** created in RootDomain
2020-06-18 10:33:59
iMessage lookup for account **filip.bl82[@]gmail.com**
2020-06-19 05:57:07
Process: **bh** (WIFI IN: 1.60 MB, WIFI OUT: 0.12 MB, WWAN IN: 0.00 MB, WWAN OUT: 0.00 MB)
2020-06-19 06:03:21
Process: **llmdwatchd** (WIFI IN: 15.82 MB, WIFI OUT: 32.86 MB, WWAN IN: 0.63 MB, WWAN OUT: 3.01 MB)
2020-06-19 08:33:26
Process: **llmdwatchd** (IN: 0.77 MB, OUT: 3.01 MB)
2020-06-19 12:57:13
Process: **llmdwatchd**
2020-07-16 07:15:03
iMessage lookup for account **kleinleon1987[@]gmail.com**

Forensic traces for BEJRN1 – Peter Verlinden, Journalist

Date (UTC)	Event
2020-09-22 06:32:38	Process **rlaccountd**
2020-09-29 09:53:57	Process: **rlaccountd** (IN: 11.77 MB, OUT: 148.72 MB)
2020-09-29 15:05:45	Process **rlaccountd**

Forensic traces for BHHRD – Ebtisam al Saegh

Date (UTC)	Event
2019-08-08 08:45:12	File Library/Preferences/**com.apple.CrashReporter.plist** created in RootDomain
2019-08-08 08:45:32	File Library/Preferences/**roleaccountd.plist** created in RootDomain
2019-08-08 08:45:35	Process: **roleaccountd** (WIFI IN: 0.03 MB, WIFI OUT: 0.01 MB, WWAN IN: 0.05 MB, WWAN OUT: 0.01 MB)

2019-08-08 08:45:37
File Library/Preferences/roleaccountd.plist modified in RootDomain
2019-08-08 08:45:41
Process: **stagingd** (WIFI IN: 8.62 MB, WIFI OUT: 0.56 MB, WWAN IN: 10.17 MB, WWAN OUT: 0.82 MB)
2019-08-08 08:46:07
Process: **xpccfd** (WIFI IN: 28.10 MB, WIFI OUT: 222.23 MB, WWAN IN: 9.72 MB, WWAN OUT: 127.68 MB)
2019-08-09 12:46:59
Process: **launchafd** (WIFI IN: 0.72 MB, WIFI OUT: 3.29 MB, WWAN IN: 2.31 MB, WWAN OUT: 30.34 MB)
2019-08-09 13:44:11
Process: **launchafd**
2019-08-12 09:04:46
Process: **logseld** (WIFI IN: 17.16 MB, WIFI OUT: 63.07 MB, WWAN IN: 4.00 MB, WWAN OUT: 36.22 MB)
2019-08-12 09:04:57
Process: **logseld**
2019-08-18 15:35:45
Process: **eventstorpd** (WIFI IN: 34.28 MB, WIFI OUT: 37.75 MB, WWAN IN: 21.03 MB, WWAN OUT: 38.25 MB)

2019-08-18 17:29:56
Process: **eventstorpd**
2019-08-28 11:33:27
Process: **libtouchregd** (WIFI IN: 5.64 MB, WIFI OUT: 16.75 MB, WWAN IN: 5.45 MB, WWAN OUT: 9.35 MB)
2019-08-28 12:50:04
Process: **libtouchregd**
2019-08-31 14:53:14
Process: **frtipd** (WIFI IN: 14.49 MB, WIFI OUT: 10.70 MB, WWAN IN: 15.36 MB, WWAN OUT: 24.42 MB)
2019-08-31 14:53:25
Process: **frtipd**
2019-09-19 15:15:43
Process: **corecomnetd** (WIFI IN: 16.38 MB, WIFI OUT: 11.79 MB, WWAN IN: 26.91 MB, WWAN OUT: 41.67 MB)
2019-09-19 15:15:51
Process: **corecomnetd**
2019-11-22 16:08:19
Process: **bh** (WIFI IN: 3.03 MB, WIFI OUT: 0.16 MB, WWAN IN: 0.00 MB, WWAN OUT: 0.00 MB)

2019-11-22 16:08:49
Process: **boardframed** (WIFI IN: 13.16 MB, WIFI OUT: 7.23 MB, WWAN IN: 11.15 MB, WWAN OUT: 25.57 MB)
2019-11-22 16:21:04
Process: **boardframed**

Forensic traces for BHHRL1 – Mohammed al-Tajer

Date (UTC)
Event
2021-09-02 14:35:55
Traces related to Pegasus execution
2021-09-15 22:01:06
Traces related to Pegasus execution
2021-09-27 13:45:35
Traces related to Pegasus execution

Forensic traces for BHPOI1 – Sharifa Siwar

Date (UTC)
Event

2021-06-10 22:41:53
Process: **fservernetd**

Forensic traces for BHJRN1

Date (UTC)
Event
Approx. 2021-09-20
Traces related to Pegasus execution

Forensic traces for FRPOI6 – Arnaud Montebourg

Date (UTC)
Event
2019-09-01 20:04:00
iMessage lookup for account **b\x00\x00gers.o79[@]gmail.com** (bergers.o79[@]gmail.com)
2019-09-01 20:24:41
File Library/Preferences/**com.apple.CrashReporter.plist** created in RootDomain
2019-09-01 20:25:03
File Library/Preferences/**roleaccountd.plist** created in RootDomain

2019-09-01 20:25:05
Process: **roleaccountd** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 0.02 MB, WWAN OUT: 0.01 MB)
2019-09-01 20:25:07
Process: **stagingd**
2019-09-01 20:25:08
File Library/Preferences/**roleaccountd.plist** modified in RootDomain
2019-09-01 20:25:09
Process: **stagingd** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 4.39 MB, WWAN OUT: 0.23 MB)
2019-09-01 20:25:57
Process: **actmanaged** (WIFI IN: 13.13 MB, WIFI OUT: 79.11 MB, WWAN IN: 6.01 MB, WWAN OUT: 41.19 MB)
2019-09-01 20:26:07
Process: **actmanaged** (IN: 6.01 MB, OUT: 41.23 MB)
2019-09-02 12:37:19
Process: **actmanaged**
2019-09-06 10:20:27
Process: **roleaccountd** (IN: 0.02 MB, OUT: 0.01 MB)
2019-09-06 10:20:53

Process: **confinstalld** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 5.01 MB, WWAN OUT: 32.13 MB)

2019-09-06 10:21:04
Process: **confinstalld** (IN: 5.01 MB, OUT: 32.16 MB)
2019-09-06 10:21:05
Process: **confinstalld**
2019-09-06 14:11:53
Process: **confinstalld**
2019-09-06 10:21:05
iMessage lookup for account **bergers.o79[@]gmail.com**
2019-09-07 19:33:59
Process: **roleaccountd**
2019-09-07 19:34:02
Process: **stagingd** (IN: 4.39 MB, OUT: 0.23 MB)
2019-09-07 19:34:10
Process: **stagingd**
2019-09-07 19:34:45
Process: **eventstorpd** (WIFI IN: 0.01 MB, WIFI OUT: 0.01 MB, WWAN IN: 1.50 MB, WWAN OUT: 9.09 MB)

MB, WWAN OUT: 9.09 MB)
2019-09-07 19:34:55

Process: **eventstorpd** (IN: 1.50 MB, OUT: 9.09 MB)
2019-09-07 20:27:28
Process: **eventstorpd**
2019-09-08 05:08:10
iMessage lookup for account **naomiwerff772[@]gmail.com**

Forensic traces for HUJRN3 – Brigitta Csikász, Hungarian journalist

Date (UTC)
Event
2019-04-05 11:06:39
File *Library/Preferences/com.apple.CrashReporter.plist* created in RootDomain
2019-04-05 11:06:41
File Library/Preferences/com.apple.CrashReporter.plist modified in RootDomain
2019-04-05 11:06:57
File Library/Preferences/roleaccountd.plist created in RootDomain
2019-04-05 11:07:01

File Library/Preferences/roleaccountd.plist modified in RootDomain
2019-04-05 17:57:29

Process: **logseld**
2019-04-07 06:32:00
Process: **logseld** (IN: 0.71 MB, OUT: 0.40 MB)
2019-04-07 14:31:02
Process: **logseld**
2019-06-18 14:04:18
Process: **roleaccountd** (IN: 0.03 MB, OUT: 0.01 MB)
2019-06-18 14:04:22
Process: **stagingd** (IN: 8.55 MB, OUT: 0.41 MB)
2019-06-18 14:04:46
Process: **bundpwrd**
2019-06-21 05:14:41
Process: **bundpwrd** (IN: 4.37 MB, OUT: 2.24 MB)
2019-06-21 14:21:19
Process: **bundpwrd**
2019-07-12 14:10:39

iMessage lookup for account e\x00\x00adavies8266[@]gmail.com (emmadavies8266[@]gmail.com)

2019-07-12 14:13:11
Process: **roleaccountd**
2019-07-12 14:13:39
Process: **boardframed**
2019-07-12 14:14:25
Process: **stagingd**
2019-07-13 10:09:47
iMessage lookup for account **emmadavies8266[@]gmail.com**
2019-07-31 13:33:30
Process: **boardframed** (IN: 21.00 MB, OUT: 13.58 MB)
2019-08-04 07:01:15
Process: **boardframed**
2019-11-18 08:16:31
Photostream lookup for account **ameliehaggart[@]gmail.com**
2019-11-18 08:18:50
Process: **bh** (IN: 4.43 MB, OUT: 0.16 MB)

2019-11-18 08:19:01	Process: **bh**
2019-11-18 08:20:44	Process: **rolexd** (IN: 8.96 MB, OUT: 23.01 MB)
2019-11-19 15:24:55	Process: **rolexd**

Forensic traces for HUJRN4 – Dániel Németh, Hungarian journalist

This data was peer reviewed **from Citizen Lab analysis**.

Phone 1:

Date (UTC)	Event
2021-07-01 07:57:02	iMessage lookup for account **meliastahl[@]gmail.com**
2021-07-01 08:34:24	Process: **com.apple.Mappit.SnapshotService** (IN: 1.93 MB, OUT: 0.27 MB)
2021-07-09 01:25:12	Process: **roleaboutd**

Phone 2:

Date (UTC)	Event
2021-07-05 07:30:55	iMessage lookup for account **meliastahl[@]gmail.com**
2021-07-07 15:52:03	Process: **keybrd** (IN: 5.30 MB, OUT: 3.26 MB)
2021-07-09 06:59:15	Process: **keybrd** (IN: 0.00 MB, OUT: 0.03 MB)
2021-07-09 07:00:40	Process: **keybrd**
2021-07-09 07:01:35	Process **keybrd**

Forensic traces for INHRD2 – Rona Wilson

This data is an independent analysis of Rona Wilson’s iPhone backups identified by Arsenal in their forensic analysis of Rona Wilson’s hard drive.

Date (UTC)	Event

2017-07-05 14:24:46
File Library/Preferences/**com.apple.CrashReporter.plist** created in RootDomain
2017-07-05 14:24:48
Process **GoldenGate** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 0.91 MB, WWAN OUT: 0.01 MB)
2017-07-05 14:28:59
Process **pcsd** (WIFI IN: 0.92 MB, WIFI OUT: 7.48 MB, WWAN IN: 57.50 MB, WWAN OUT: 293.37 MB)
2017-07-05 17:11:35
Process: **pcsd**
2017-07-11 10:12:02
Process: **pcsd** (IN: 14.68 MB, OUT: 55.46 MB)
2017-07-11 17:35:42
Process: **pcsd**
2017-08-03 13:14:45
iMessage lookup for account **martin.vdm78[@]gmail.com**
2017-08-07 13:02:07
SMS: “Maoists gun down 2 cops in encounter in Rajnandgaon, Chhattisgarh http://bit[.]ly/2vHMLw2” (**https://myfreecharge[.]online/TPy8paiO**)
2017-08-09 09:28:00

2017-08-09 09:28:00
SMS: “Gujrat ATS arrests Nagpur activist for ‘seditious activities’. http://bit[.]ly/2wGGc9x” (**https://myfreecharge[.]online/e2sM1ryy**)

2017-08-10 10:12:22
SMS: “Free Dr Saibaba and Oppose the suppression of Dissent in India. Please sign the petition here clicking http://bit[.]ly/2vRBs3V” (**https://myfreecharge[.]online/aMtsfCb**)
2017-08-31 10:01:45
SMS: “Missing Najeeb, seat cuts to dictate JNUSU elections. Read more at http://bit[.]ly/2wV87ab” (**https://myfreecharge[.]online/gTLGJUVG**)
2017-09-01 12:48:09
SMS: “Dear valued customer, UNLOCK exclusive offers designed JUST FOR YOU at : http://bit[.]ly/2gp2ztM” (**https://myfreecharge[.]online/muWMKiV**)
2017-09-04 08:26:56
SMS: “Justice to Dalit victims of Una-Gujarat. Ban Cow protection groups in India. Express solidarity & sign: http://bit[.]ly/2gwYwf1” (**https://myfreecharge[.]online/OQ7vweIrL**)
2017-09-04 13:06:46
SMS: “Investigate the Human Rights emergency and attacks on Religious Minorities and Dalits in India.Pls sign http://bit[.]ly/2wAUb29” (**https://myfreecharge[.]online/WU7HJGVQ**)
2017-09-05 02:45:36
SMS: “Jabong Clearance Sale: Flat 50% off+Extra 25% off on Top Brands. Use Code VISA25 at: http://bit[.]ly/2vH3gJs” (**https://myfreecharge[.]online/awBn8TI**)

2017-09-06 10:38:30

SMS: “The India Post spreads malicious propaganda of right wingers in Punjab University. Read the article : http://bit[.]ly/2xO56W9” (**https://myfreecharge[.]online/ljdyQkie**)
2017-09-15 03:02:34
SMS: “UNHRC slams India on Rohingya, Gauri Lankesh murder and Cow lynching. Click here for details: http://bit[.]ly/2wdKJEW” (**https://myfreecharge[.]online/KvFw9qa**)
2017-09-26 11:15:10
SMS: “Amazon to step-up FMCG discount. Flat 35% to 50%. To avail visit here: http://bit[.]ly/2winuWf” (**https://myfreecharge[.]online/fx9zM94**)
2017-10-25 12:08:13
iMessage lookup for account **martin.vdm78[@]gmail.com**
2018-01-15 15:14:16
Thumper lookup for account **yvonne.wechsler61[@]gmail.com**
2018-01-31 10:58:20
SMS: “JNU Chronicles: Real-life tales of love jihad from JNU, the citadel of Indian Marxism. Read details here: http://bit[.]ly/2BFYvOl” (**https://news-alert[.]org/u6GjGDqZ**)
2018-02-02 08:41:53
SMS: “19 Indian Nazi Tweets that will turn you into a hardliner Right Winger right now. Read here: http://bit[.]ly/2nuLxvN” (**https://news-**

alert[.]org/l0xz0K9G)
2018-02-02 12:52:21

SMS: “This controversial website is targeting Radical’ left-wing academics. Read details here: http://bit[.]ly/2nw1wwi” (**https://news-alert[.]org/sJHra27pL**)
2018-02-05 13:19:05
SMS: “Padmaavat has Deepika as the hero, Ranveer as the villain, and BJP as the joker. Read full review here: http://bit[.]ly/2E1Jexw” (**https://news-alert.[o]rg/ipvK2G6eC**)
2018-02-06 10:07:21
Process: **roleaccountd** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 0.11 MB, WWAN OUT: 0.03 MB)
2018-02-06 10:07:27
Process **stagingd** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 25.02 MB, WWAN OUT: 0.08 MB)
2018-02-06 10:08:42
Process: **pcsd** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 25.02 MB, WWAN OUT: 0.08 MB)
2018-02-13 04:44:56
Thumper lookup for account **sylianosliatsos84[@]gmail.com**
2018-03-11 09:25:50
Process: **stagingd** (IN: 16.47 MB, OUT: 0.06 MB)

2018-03-14 12:15:46
Process: **roleaccountd** (IN: 0.07 MB, OUT: 0.02 MB)

2018-03-14 12:18:02
Process: **pcsd** (IN: 6.12 MB, OUT: 70.55 MB)
2018-03-16 03:49:04
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-17 03:56:04
Process: **pcsd** (IN: 0.57 MB, OUT: 14.47 MB)
2018-03-19 04:27:23
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-19 04:27:26
Process: **stagingd** (IN: 1.23 MB, OUT: 0.00 MB)
2018-03-19 04:28:08
Process: **pcsd** (IN: 0.36 MB, OUT: 4.65 MB)
2018-03-20 05:18:40
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-20 05:18:44
Process: **stagingd** (IN: 1.22 MB, OUT: 0.00 MB)

2018-03-20 05:28:58
Process: **pcsd** (IN: 0.64 MB, OUT: 6.52 MB)

2018-03-22 13:38:21
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-22 13:38:24
Process: **stagingd** (IN: 1.23 MB, OUT: 0.01 MB)
2018-03-22 13:39:08
Process: **pcsd** (IN: 0.18 MB, OUT: 4.27 MB)
2018-03-24 04:33:48
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-24 04:33:52
Process: **stagingd** (IN: 1.22 MB, OUT: 0.00 MB)
2018-03-24 04:34:30
Process: **pcsd** (IN: 1.18 MB, OUT: 23.78 MB)
2018-03-25 04:34:46
Process: **pcsd** (IN: 1.31 MB, OUT: 27.42 MB)
2018-03-26 04:44:28
Process: **pcsd** (IN: 1.75 MB, OUT: 37.15 MB)

2018-03-27 04:55:04
Process: **pcsd** (IN: 1.90 MB, OUT: 43.49 MB)

2018-03-28 04:23:32
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-28 04:23:33
Process: **stagingd** (IN: 1.22 MB, OUT: 0.00 MB)
2018-03-29 06:19:54
File Library/Preferences/**com.apple.CrashReporter.plist** updated in RootDomain
2018-03-29 06:20:23
Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2018-03-29 06:20:31
Process: **stagingd** (IN: 1.22 MB, OUT: 0.00 MB)
2018-03-29 06:21:13
Process: **stagingd**
2018-03-29 06:21:43
Process: **pcsd** (IN: 0.28 MB, OUT: 3.80 MB)
2018-03-29 12:32:57
Process: **pcsd**

2018-04-01 06:26:09
Thumper lookup for account **taylorjade0303[@]gmail.com**
2018-04-10 05:24:09
Thumper lookup for account **lee.85.holland[@]gmail.com**

Forensic cases for INHRL1 – Jagdeep Singh, Human Rights Lawyer

Date (UTC)
Event
2019-07-07 07:33:51
File Library/Preferences/com.apple.CrashReporter.plist created in RootDomain
2019-07-07 07:41:06
File Library/Preferences/roleaccountd.plist created in RootDomain
2019-07-07 10:18:55
Process: **lobbrogd**
2019-07-08 10:20:32
Process: **lobbrogd** (IN: 14.06 MB, OUT: 122.39 MB)
2019-07-08 16:46:06
Process: **lobbrogd**

2019-07-10 06:14:53
Process: **roleaccountd**

2019-07-10 06:14:57
Process: **stagingd**
2019-07-10 06:15:39
Process: **misbrigd**
2019-07-11 06:16:24
Process: **misbrigd** (IN: 5.34 MB, OUT: 23.78 MB)
2019-07-11 14:54:34
Process: **misbrigd**
2019-07-12 04:27:20
Process: **bfrgbd** (IN: 3.46 MB, OUT: 16.15 MB)
2019-07-12 16:28:56
Process: **bfrgbd**
2019-07-15 04:34:36
Process: **setframed** (IN: 4.14 MB, OUT: 28.88 MB)
2019-07-15 04:34:37
Process: **setframed**

2019-07-15 16:35:11
Process: **setframed**

2019-07-17 08:42:21
Process: **fnotifyd** (IN: 2.19 MB, OUT: 27.52 MB)
2019-07-17 11:10:09
Process: **fnotifyd**
2019-07-19 04:30:49
Process: **keybrd** (IN: 3.01 MB, OUT: 17.09 MB)
2019-07-19 13:01:01
Process: **keybrd**
2019-07-22 04:41:28
Process: **seraccountd**
2019-07-24 04:43:04
Process: **seraccountd** (IN: 8.85 MB, OUT: 24.74 MB)
2019-07-25 01:33:36
Process: **seraccountd**
2019-08-01 03:40:15
Process: **roleaccountd** (IN: 0.05 MB, OUT: 0.03 MB)

2019-08-01 03:41:02
Process: **otpgrefd** (IN: 2.13 MB, OUT: 21.51 MB)

2019-08-01 04:37:31
Process: **otpgrefd**
2019-08-08 09:33:37
Process: **roleaccountd**
2019-08-08 09:33:43
Process: **stagingd** (IN: 11.87 MB, OUT: 0.62 MB)
2019-08-08 09:34:09
Process: **stagingd**
2019-08-08 09:34:27
Process: **natgd**
2019-08-09 09:35:39
Process: **natgd** (IN: 7.87 MB, OUT: 44.54 MB)
2019-08-09 22:56:13
Process: **natgd**
2019-08-21 09:09:02
iMessage lookup for account **b\x00\x00kerfredi[@]gmail.com** (bekkerfredi[@]gmail.com)

(bekkerfredi[@]gmail.com)
2019-11-30 04:51:07

iMessage lookup for account **bekkerfredi[@]gmail.com**

Forensic traces for INHRL2 – Joseph Aljo, Lawyer

Date (UTC)
Event
2019-03-30 05:00:32
iMessage lookup for account **bekkerfredi[@]gmail.com**

Forensic traces for INPOI1 – Karma D Namgyal, Secretary and Legal officer, Office of Karmapa

Date (UTC)
Event
2017-12-08 12:12:31
SMS: “To know: Why American actor Gere got “”Knocked Out”” by American lawmakers during a Congress hearing? http://bit[.]ly/2AIiVJR” (**https://news-alert[.]org/Tdcs3jLF**)
2017-12-11 12:37:17
SMS: “To find as to how setting up of Tibet group in Lithuania’s parliament would impact its relation with China? http://bit[.]ly/2iTb4Px” (**https://news-**

would impact its relation with China: http://bit[.]ly/2Irb4Fx" (**https://news-alert[.]org/PSIwgEF**)
2018-01-24 08:21:50

SMS: "Open Airtel Payment Bank A/C and earn 7.25% interest on your deposit. To open A/C click: **https://myfreecharge[.]online/ORzJIfp**"

Forensic traces for JOHRL – Hala Deeb

Date (UTC)	Event
2021-03-16 14:58:48	Process **bluetoothfs** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 0.02 MB, WWAN OUT: 0.00 MB)
2021-03-16 14:58:57	Process: **JarvisPluginMgr** (WIFI IN: 0.00 MB, WIFI OUT: 0.00 MB, WWAN IN: 1.70 MB, WWAN OUT: 0.24 MB)
2021-03-16 14:59:32	Process: **launchafd** (WIFI IN: 0.07 MB, WIFI OUT: 0.87 MB, WWAN IN: 0.03 MB, WWAN OUT: 0.01 MB)
2021-03-16 17:56:19	Process **launchafd**

Forensic traces for KZHRD1 – Tamina Ospanova

Date (UTC)	**Event**
2021-06-05 06:51:41	Process: **ctrlfs**
2021-06-05 06:51:45	Process: **ABSCarryLog**
2021-06-05 06:52:19	Process: **fdlibframed**
2021-06-05 08:12:09	Process: **xpccfd**

Forensic traces for KZHRD2 – Dimash Alzhanov

Date (UTC)	**Event**
2021-06-03 06:34:32	Process: **cfprefssd** (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-03 06:34:37	Process: **com.apple.rapports.events** (IN: 1.70 MB, OUT: 0.20 MB)

2021-06-03 06:35:13
Process: **boardframed** (IN: 6.37 MB, OUT: 12.52 MB)
2021-06-06 05:48:44
Process: **faskeepd**
2021-06-26 02:56:51
Process: **ABSCarryLog** (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-26 02:56:58
Process: **Diagnosticd** (IN: 1.78 MB, OUT: 0.22 MB)
2021-06-26 02:59:15
Process: **seraccountd** (IN: 14.57 MB, OUT: 17.90 MB)
2021-07-02 12:19:31
Process: **passsd** (IN: 0.01 MB, OUT: 0.00 MB)
2021-07-02 12:19:37
Process: **ctrlfs** (IN: 1.83 MB, OUT: 0.34 MB)
2021-07-02 12:25:03
Process: **fservernetd** (IN: 10.04 MB, OUT: 15.32 MB)
2021-07-03 06:18:06
Process: **fservernetd**

2021-07-04 11:30:40	Process: **vm_stats** (IN: 0.01 MB, OUT: 0.00 MB)
2021-07-04 11:30:46	Process: **wifip2ppd** (IN: 1.78 MB, OUT: 0.22 MB)
2021-07-04 11:32:09	Process: **rlaccountd** (IN: 23.27 MB, OUT: 22.86 MB)
2021-07-06 20:35:32	Process: **rlaccountd**

Forensic traces for KZHRD3 – Aizat Abilseit

Date (UTC)	**Event**
2021-06-05 06:15:49	Process: **gatekeeperd** (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-05 06:15:53	Process: **ABSCarryLog** (IN: 1.78 MB, OUT: 0.14 MB)
2021-06-05 06:18:26	Process: **smmsgingd** (IN: 13.54 MB, OUT: 15.44 MB)

2021-06-07 07:05:46
Process: **smmsgingd**

2021-06-09 03:29:18
Process: **Diagnosticd** (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-09 03:30:05
Process: **ReminderIntentsUIExtension** (IN: 0.00 MB, OUT: 0.00 MB)
2021-06-09 03:30:18
Process: **nehelprd** (IN: 0.35 MB, OUT: 0.29 MB)
2021-06-09 09:42:04
Process: **nehelprd**
2021-06-12 06:21:59
Process: **JarvisPluginMgr** (IN: 1.78 MB, OUT: 0.16 MB)
2021-06-12 06:22:28
Process: **frtipd** (IN: 14.94 MB, OUT: 16.21 MB)
2021-06-15 18:02:27
Process: frtipd
2021-06-15 22:37:54
Process: **frtipd**

Forensic traces for KZHRD4 – Darkhan Sharipov

Date (UTC)	Event
2021-06-05 05:57:10	Process: **CommsCenterRootHelper** (IN: 0.02 MB, OUT: 0.01 MB)
2021-06-05 05:57:20	Process: **neagentd** (IN: 1.70 MB, OUT: 0.17 MB)
2021-06-05 05:58:59	Process: **brfstagingd** (IN: 0.13 MB, OUT: 0.22 MB)
2021-06-09 03:27:39	Process: **vm_stats**
2021-06-09 03:27:58	Process: **com.apple.Mappit.SnapshotService**
2021-06-09 03:28:52	Process: **jlmvskrd**
2021-06-10 04:18:09	Process: **wifip2ppd**

2021-06-10 04:31:22
Process: **cfprefssd**

2021-06-24 06:52:51
Process: **JarvisPluginMgr** (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-24 06:52:53
Process: **Diagnosticd** (IN: 1.70 MB, OUT: 0.11 MB)
2021-06-24 06:53:28
Process: **corecomnetd** (IN: 2.98 MB, OUT: 21.72 MB)
2021-06-26 03:17:58
Process: **ABSCarryLog**
2021-06-26 03:25:41
Process: **eventfssd** (IN: 5.10 MB, OUT: 4.13 MB)
2021-07-02 12:12:15
Process: **dhcp4d** (IN: 1.78 MB, OUT: 0.10 MB)
2021-07-02 12:12:20
Process: **CommsCenterRootHelper**
2021-07-02 12:12:50
Process: **tisppd** (IN: 3.22 MB, OUT: 23.07 MB)

Forensic traces for PLPOI1 – Magdalena Łośko

Date (UTC)	Event
2019-04-17 12:42:55	SMS from **Klub51015**: Zakupy z klubem 5.10.15! Sezonowa wyprzedaż -50% online i w sklepach stacjonarnych. Sprawdź: **https://sale-2019[.]com/2CaJGuQ**
2019-04-18 14:13:26	SMS from **SklepyCCC:** Przeceny do 50% na obuwie, a dla klubowiczów dodatkowe 10% rabatu na wszystkie produkty! Oferta do 20-04-2019. Sprawdź online! **http://bit[.]ly/lPl1jEU**
2019-04-19 10:40:51	SMS from **Playpl**: Pobierz fakturę nr: F/20087153/04/19 na kwotę 125.00 zł. Jej termin płatności mija 2019/04/26. Zaloguj się online **http://bit.ly/nEFmH03**
2019-04-23 07:12:47	SMS from **Infor**: Mobbing w miejscu pracy to pojęcie szersze niż powszechnie się wydaje. Czytaj więcej: **http://bit.ly/PpF97sS**

Forensic traces for PLPOI2 – Ryszard Brejza

Date (UTC)	Event

2019-07-11 12:15:35

SMS from **BramkaSMS**: Panie Prezydencie, widział Pan komentarze na portalu “ino” na temat skoszonej łąki? Proszę wejść i poczytać. Podsyłam link do artykułu: **http://tinyurl[.]com/y69p3pyk (https://newsportal24[.]online/mtM8dy6cz)**
2019-07-12 07:18:19
SMS from **PlatformaKO**: Już 12-13 lipca spotkajmy się na Forum Programowym Koalicji Obywatelskiej, by porozmawiać o Polsce! **http://tinyurl[.]com/y3cnsgzl (https://loginverify[.]net/EWSRfbj)**
2019-07-12 16:23:51
SMS from **HTC-Polska**: Zapisz sie do klubu HTC! Jako klubowicz będziesz otrzymywać niedostępne dla innych informacje o nowych produktach, akcesoriach i usługach. Korzystaj w pełni z możliwości swojego telefonu! **https://oneadjump[.]com/SQY8jBX**
2019-07-16 08:38:32
SMS from **WCZK-A1**: AmberGO – nowy system płatności na autostradzie A1! System automatycznego poboru opłat bez biletów i bez dokonywania płatności na bramkach. **https://loginverify[.]net/6Egzh2F** Wypróbuj już teraz!
2019-07-24 06:56:35
SMS from **KtoMaLek.pl**: Kryzys lekowy trwa! Sprawdź, w której aptece w okolicy dostaniesz potrzebny lek! **https://sale-2019[.]com/8QCAqcU8**
2019-07-29 12:23:42
SMS from **Energa**: Drogi kliencie, przypominamy o ostatecznym terminie składania oświadczeń ws. zamrożenia cen energii. Pełną informację o uprawnieniu do rozliczeń według niższych cen i stawek znajdziesz na naszej stronie:

	mu do rozliczeń według niższych cen i stawek znajdziesz na naszej stronie. **https://loginverify[.]net/sj5zsue**
2019-07-31 13:24:43	SMS from **BramkaSMS**: Ryszard zagłosuj w sondażu dotyczącym naszej kandydatki do senatu. To już ostatnie chwile! **https://newsportal24[.]online/kcUU9pshh**
2019-08-06 12:05:56	SMS from **e-nadmorzem**: Hotele na Wybrzeżu Bałtyku do 50% zniżki. Zobacz ofertę. **https://holiday-sun[.]net/eXppP19S**
2019-08-14 11:53:11	SMS from **Bytom**: Dzień dobry, informujemy, że Pańska przesyłka jest do odebrania w salonie firmowym Bytom C.H. Złote Tarasy. Prosimy o przygotowanie numeru zamówienia. Przejdź do Twojego zamówienia: **https://awizo[.]info/7AvsrqNYR**
2019-08-20 12:06:19	SMS from **newsportal**: Znamy już pełne listy wyborcze! Czeka nas kilka ciekawych starć. Zobacz listę kandydatów z Twojego okręgu wyborczego **https://newsportal24[.]online/8ZedQvG**

Forensic traces for TRJRN1 – Ragip Soylu, Turkey Bureau Chief for Middle East Eye

Date (UTC)	**Event**
2021-02-09 07:26:27	

Traces related to iMessage exploitation
2021-02-10 12:15:38

Process: **tisppd**
2021-02-12 07:25:17
Traces related to iMessage exploitation
2021-02-12 07:30:51
Process: **CommsCenterRootHelper** (IN: 1.74 MB, OUT: 0.23 MB)
2021-02-12 07:31:12
Process: **CommsCenterRootHelper**
2021-02-12 10:30:52
Process: **launchrexd**
2021-02-12 10:30:52
Process: **boardframed**
2021-02-19 05:26:06
Traces related to iMessage exploitation
2021-02-21 07:58:44
Traces related to iMessage exploitation
2021-03-22 05:39:06

Traces related to iMessage exploitation
2021-04-10 08:09:32

Traces related to iMessage exploitation
2021-04-13 20:39:16
Process: **accountpfd**
2021-04-14 04:41:05
Traces related to iMessage exploitation
2021-04-15 16:59:11
Process: **xpccfd**
2021-04-25 04:59:32
Traces related to iMessage exploitation
2021-04-26 23:52:27
Process: **xpccfd**
2021-05-02 07:12:23
Traces related to iMessage exploitation
2021-05-02 20:22:15
Process: **faskeepd**
2021-05-08 20:28:06

Traces related to iMessage exploitation
2021-05-09 12:51:05
Process: **corecomnetd**
2021-05-16 04:27:48
Traces related to iMessage exploitation
2021-05-19 11:04:07
Traces related to iMessage exploitation
2021-05-23 00:00:13
Process: **roleaboutd**
2021-07-05 12:41:48
Traces related to iMessage exploitation
2021-07-05 12:56:59
Process: **ReminderIntentsUIExtension** (IN: 1.89 MB, OUT: 0.22 MB)
2021-07-05 12:57:11
Process: **ReminderIntentsUIExtension**
2021-07-05 15:11:44
Process: **neagentd**
2021-07-05 15:11:44

Date (UTC)	Event
	Process: **smmsgingd**

Forensic traces for UKHRL1 – David Haigh, human rights lawyer

Date (UTC)	Event
2020-08-03 04:01:01	iMessage lookup for account **arvidamelia1[@]gmail.com**
2020-08-03 07:37:49	Process: **netservcomd** (IN: 5.27 MB, OUT: 79.44 MB)
2020-08-04 15:27:47	Process: **netservcomd**

Forensic traces for UKPOI1 – Anas Altikriti, CEO and Founder of The Cordoba Foundation

Date (UTC)	Event
2020-07-04 12:10:47	iMessage lookup for account **weertlaura1[@]outlook.com**
2020-07-17 16:09:05	

iMessage lookup for account **mitchkremer14[@]outlook.com**
2020-07-24 11:45:09
Process: **otpgrefd** (IN: 1.15 MB, OUT: 3.96 MB)
2020-07-24 18:45:05
Process: **otpgrefd**

Forensic traces for WSHRD1 – Mahjoub Mleiha, Western Sahara HRD

Date (UTC)
Event
2021-01-29 13:17:06
Process: **Diagnosticd** (IN: 6.43 KB, OUT: 2.06 KB)
2021-03-20 01:53:44
Process: **vm_stats**
2021-03-20 01:53:44
Process: **ReminderIntentsUIExtension**
2021-03-20 01:53:44
Process: **neagentd**
2021-03-20 01:53:44

	Process: **updaterd**
2021-04-22 23:10:51	Process: **wifip2ppd**
2021-05-12 12:46:12	Process: **MobileSMSd**
2021-05-12 12:46:12	Process: **ABSCarryLog**
2021-06-03 08:22:06	Process: **dhcp4d** (IN: 1.8 MB, OUT: 0.26 MB)
2021-06-03 08:22:06	Process: **bluetoothfs** (IN: 9.27 KB, OUT: 2.9 KB)

Forensic traces for WSHRD2 – Aminatou Haidar, Western Sahara HRD

Phone 1

Date (UTC)	Event
2021-10-28 20:39:02	Traces related to Pegasus execution

2021-11-05 17:17:08	Traces related to Pegasus execution

Phone 2

Date (UTC)	**Event**
2018-09-21 10:30:16	Thumper lookup for account **krystynajasinska86[@]gmail.com**

Update history

This document was first published on 6 August 2021 with forensic traces for HUJRN3, UKHRL1, UKPOI1, and TRJRN1.

It was subsequently updated:

- On 23 November 2021 to include forensic traces for WSHRD1;
- On 29 November 2021 to include forensic traces for BEJRN1, INHRL1 and INHRL2;
- On 3 December 2021 to include forensic traces for HUJRN4;
- On 9 December 2021 to include forensic traces for KZHRD1, KZHRD2, KZHRD3 and KZHRD4;
- On 17 December 2021 to include forensic traces for INHRD2;
- On 17 January 2022 to include forensic traces for BHHRD and JOHRL;
- On 27 January 2022 to include forensic traces for INPOI1;
- On 7 February 2022 to include forensic traces for FRPOI6;
- On 8 February 2022 to update table UKPOI1 to fix transcription errors in the table and add additional indicators;
- On 9 February 2022 to include forensic traces for AZHRD1, AZJRN2 and AZHRL1;
- On 17 February 2022 to include forensic traces for PLPOI1 and PLPOI2;
- On 17 February 2022 to update the code AZJRN2 to AZJRN3;

- On 18 February 2022 to include forensic traces for BHHRL1, BHPOI1, and BHJRN1;
- On 10 March 2022 to include forensic traces for WSHRD2;

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

Forensic Methodology Report: Pegasus Forensic Traces per Target

Topics

RESEARCH