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 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 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 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)
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 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 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
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

2020-07-24 11:45:09
Process: **otpgrefd** (IN: 1.15 MB, OUT: 3.96 MB)
2020-07-24 18:45:05
Process: **otpgrefd**
2021-02-10 12:15:38
Process: **tisppd**
2021-02-12 10:30:5
Process: **launchrexd**
2021-02-12 10:30:52
Process: **boardframed**
2021-04-13 20:39:16
Process: **accountpfd**
2021-04-15 16:59:11
Process: **xpccfd**
2021-04-26 23:52:27
Process: **xpccfd**
2021-05-02 20:22:15
Process: **faskeepd**
2021-05-09 12:51:05
Process: **corecomnetd**

2021-05-23 00:00:13
Process: **roleaboutd**
2021-07-05 15:11:44
Process: **neagentd**
2021-07-05 15:11:44
Process: **smmsgingd**

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)