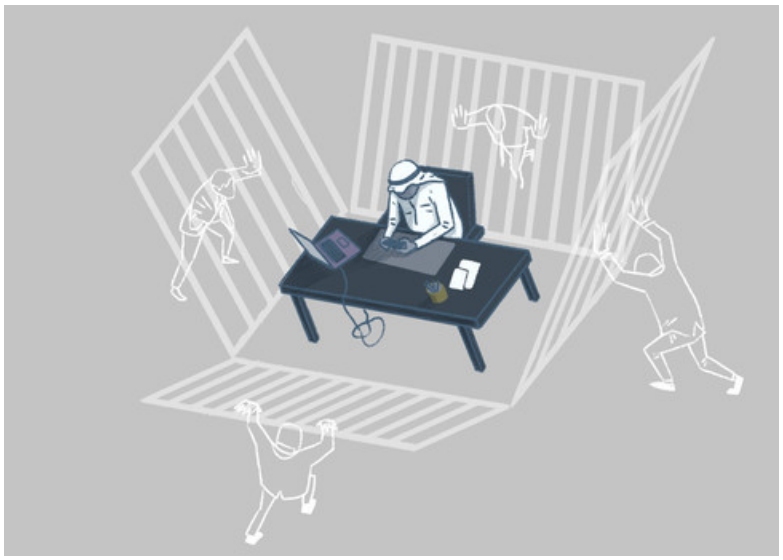
Forensic Methodology Report: Pegasus Forensic Traces per Target

amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/

July 18, 2021



July 18, 2021
Updated on: 27 July 2021

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.

This document may be updated over time as additional individuals become public.

Appendix D: Pegasus Forensic Traces per Target

All individuals have been assigned a code name for safety and privacy reasons. Only individuals who have given consent will be named publicly.

The occurrence of a known malicious iCloud account may be a result of actions made by a Pegasus customer against a potential target device. It does not by itself signify that an attack was attempted or succeeded.

Forensic traces for AZJRN1 – Khadija Ismayilova

Date (UTC)	Event
2019-03-28 07:44:14	Process: **roleaccountd**
2019-03-28 07:44:14	Process: **stagingd**

2019-03-28 07:44:15	File: Library/Preferences/***roleaccountd.plist***
2019-04-02 09:17:55	Process record deleted from ZPROCESS
2019-04-12 07:42:38	Process record deleted from ZPROCESS
2019-05-01 10:48:06	Process record deleted from ZPROCESS
2019-05-03 07:42:27	Process record deleted from ZPROCESS
2019-05-18 11:03:21	Process record deleted from ZPROCESS
2019-06-17 05:10:02	Process record deleted from ZPROCESS
2019-06-18 05:25:41	Process record deleted from ZPROCESS
2019-06-25 17:03:13	Process record deleted from ZPROCESS
2019-07-08 05:39:13	Process record deleted from ZPROCESS
2019-07-12 11:10:51	Process record deleted from ZPROCESS
2019-07-18 13:40:01	Process record deleted from ZPROCESS
2019-08-22 08:41:02	Process record deleted from ZPROCESS

2019-08-26 05:04:19	Process record deleted from ZPROCESS
2019-08-27 15:02:15	Process record deleted from ZPROCESS
2019-09-06 05:52:30	Process record deleted from ZPROCESS
2019-09-07 07:19:31	Process record deleted from ZPROCESS
2019-09-15 06:11:31	Process record deleted from ZPROCESS
2019-09-17 14:11:51	Process record deleted from ZPROCESS
2019-09-28 12:25:15	Process: **libtouchregd**
2019-10-01 19:42:17	Process record deleted from ZPROCESS
2019-10-14 05:11:06	Process record deleted from ZPROCESS
2019-10-14 16:08:43	Process: **libbmanaged**
2019-10-14 16:08:43	Process: **mobileargd**
2019-10-14 16:08:43	Process: **brstaged**
2019-10-14 16:08:43	Process: **libtouchregd**

2019-10-14 16:08:43	Process: **launchrexd**
2019-10-15 14:21:44	Process: **faskeepd**
2019-10-16 22:17:17	Process: **bundpwrd**
2019-10-22 15:42:40	Process: **seraccountd**
2019-10-22 15:42:40	Process: **comnetd**
2019-11-25 09:06:49	Process: **confinstalld**
2019-11-25 09:06:49	Process: **msgacntd**
2019-11-25 09:06:49	Process: **launchrexd**
2019-11-25 09:06:49	Process: **accountpfd**
2019-11-25 09:06:49	Process: **xpccfd**
2019-11-25 09:06:49	Process: **setframed**
2019-11-25 09:06:49	Process: **natgd**
2019-11-25 09:06:49	Process: **aggregatenotd**

2019-12-09 05:28:20	Process record deleted from ZPROCESS
2019-12-22 16:10:27	Process record deleted from ZPROCESS
2019-12-26 06:01:46	Process record deleted from ZPROCESS
2020-01-09 05:43:20	Process record deleted from ZPROCESS
2020-01-14 06:56:05	Process record deleted from ZPROCESS
2020-01-27 05:44:27	Process record deleted from ZPROCESS
2020-01-31 11:41:04	Process record deleted from ZPROCESS
2020-02-07 05:00:03	Process record deleted from ZPROCESS
2020-02-09 07:03:56	Process record deleted from ZPROCESS
2020-02-13 05:00:59	iMessage lookup for account **e\x00\x00aholm575[@]gmail.com** (emmaholm575[@]gmail.com)
2020-02-23 07:39:00	Process record deleted from ZPROCESS
2020-02-26 04:57:01	Process record deleted from ZPROCESS
2020-03-09 05:33:30	Process record deleted from ZPROCESS

2020-03-13 06:45:19	Process record deleted from ZPROCESS
2020-03-24 07:27:42	Process record deleted from ZPROCESS
2020-03-30 06:08:44	Process record deleted from ZPROCESS
2020-04-21 12:04:31	Process record deleted from ZPROCESS
2020-04-23 06:26:56	iMessage lookup for account **filip.bl82[@]gmail.\x00\x00m** (filip.bl82[@]gmail.com)
2020-04-23 07:24:11	Process record deleted from ZPROCESS
2020-04-29 07:31:57	Process record deleted from ZPROCESS
2020-04-30 07:58:32	Process record deleted from ZPROCESS
2020-05-11 14:25:28	Process record deleted from ZPROCESS
2020-05-15 11:31:09	Process record deleted from ZPROCESS
2020-05-17 07:03:29	Process record deleted from ZPROCESS
2020-05-20 21:10:16	Process: **logseld**
2020-05-20 21:10:16	Process: **brstaged**

2020-05-20 21:10:16	Process: **pstid**
2020-05-20 21:10:16	Process: **roleaboutd**
2020-05-20 21:10:16	Process: **libtouchregd**
2020-05-20 21:10:16	Process: **brstaged**
2020-05-29 07:11:37	Process record deleted from ZPROCESS
2020-05-31 07:32:56	Process record deleted from ZPROCESS
2020-05-31 15:28:11	Process: **bfrgbd**
2020-05-31 15:28:11	Process: **xpccfd**
2020-05-31 15:28:11	Process: **nehelprd**
2020-06-01 09:07:27	iMessage lookup for account **kleinleon1987[@]gma\x00\x00.com** (kleinleon1987[@]gmail.com)
2020-06-05 13:07:16	Process record deleted from ZPROCESS
2020-06-08 08:13:02	Process record deleted from ZPROCESS
2020-06-08 18:22:45	Process: **comnetd**

2020-06-08 18:22:45	Process: **fservernetd**
2020-06-08 18:22:45	Process: **rolexd**
2020-06-12 08:45:08	Process record deleted from ZPROCESS
2020-06-22 05:29:22	Process: **roleaccountd**
2020-06-22 05:29:23	Process: **stagingd**
2020-06-27 11:23:05	Process record deleted from ZPROCESS
2020-06-27 11:23:09	Process record deleted from ZPROCESS
2020-06-29 05:13:04	Process record deleted from ZPROCESS
2020-06-29 05:13:04	Process record deleted from ZPROCESS
2020-06-30 05:59:08	iMessage lookup for account **k\x00\x00inleon1987[@]gmail.com** (kleinleon1987[@]gmail.com)
2020-07-01 13:04:43	Process: **nehelprd**
2020-07-01 13:04:43	Process: **aggregatenotd**
2020-07-01 13:04:43	Process: **fservernetd**

2020-07-01 13:04:43	Process: **msgacntd**
2020-07-02 06:29:48	Process record deleted from ZPROCESS
2020-07-02 06:29:48	Process record deleted from ZPROCESS
2020-07-03 06:51:47	Process record deleted from ZPROCESS
2020-07-03 06:51:53	Process record deleted from ZPROCESS
2020-07-04 07:20:57	Process record deleted from ZPROCESS
2020-07-04 07:20:58	Process record deleted from ZPROCESS
2020-07-05 07:23:50	Process record deleted from ZPROCESS
2020-07-06 05:22:21	iMessage lookup for account **f\x00\x00ip.bl82[@]gmail.com** (filip.bl82[@]gmail.com)
2020-07-10 14:12:09	Cache file /private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache.db recorded visit to URL **hxxps://x1znqjo0x8b8j.php78mp9v.opposedarrangement[.]net:37271/afAVt89Wq/stadium/pop2.html?key=501_4&n=7**
2020-07-10 14:12:15	Cache file /private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache.db recorded visit to URL **hxxps://x1znqjo0x8b8j.php78mp9v.opposedarrangement[.]net:37271/afAVt89Wq/stadium/pop2.html?key=501_4&n=1**
2020-07-10 14:12:21	Process: **roleaccountd**
2020-07-10 14:12:26	Process: **stagingd**

2020-07-11 19:34:04	Process: **confinstalld**
2020-07-11 19:34:04	Process: **roleaboutd**
2020-07-11 19:34:04	Process: **lobbrogd**
2020-07-11 19:34:04	Process: **fservernetd**
2020-07-11 19:34:04	Process: **launchafd**
2020-07-13 05:05:17	Cache file /private/var/mobile/Containers/Data/Application/D6A69566-55F7-4757-96DE-EBA612685272/Library/Caches/com.apple.Music/Cache.db recorded visit to URL **hxxps://4n3d9ca2st.php78mp9v.opposedarrangement[.]net:37891/w58Xp5Z/stadium/pop2.html?key=501_4&n=7**
2020-12-07 07:23:23	iMessage lookup for account **kleinleon1987[@]gmail.com**
2021-04-20 17:53:51	iMessage lookup for account **filip.bl82[@]gmail.com**
2021-05-06 08:34:43	iMessage lookup for account **emmaholm575[@]gmail.com**

Forensic traces for AZJRN2 – Sevinc Vaqifqizi

Date (UTC)	Event
2019-04-17 10:53:04	File created: **Library/Preferences/com.apple.CrashReporter.plist** from RootDomain
2019-04-17 10:53:45	Process: **roleaccountd**
2019-04-17 10:53:45	File created: **Library/Preferences/roleaccountd.plist** from RootDomain
2019-04-24 12:13:29	Process: **roleaccountd**
2019-04-24 12:13:31	Process: **stagingd**

2019-07-18 09:35:17	Process: **rolexd**
2019-08-02 11:45:12	Process: **actmanaged**
2019-10-08 15:22:29	Process: **libbmanaged**
2019-10-12 08:17:28	Process: **xpccfd**
2019-10-14 05:05:09	Process: **setframed**
2019-10-18 06:16:16	Process: **natgd**
2019-10-21 05:23:50	Process: **libtouchregd**
2019-10-29 05:28:54	Process: **frtipd**
2019-11-08 07:01:25	Process: **brstaged**
2019-11-11 10:46:47	Process: **boardframed**
2019-11-17 07:15:36	Process: **ckkeyrollfd**
2019-11-19 11:50:37	Process: **mptbd**
2019-12-02 05:18:49	Process: **mobileargd**
2019-12-03 13:15:03	Process: **nehelprd**
2019-12-12 14:38:31	Process: **corecomnetd**
2020-02-10 05:15:54	Process: **pstid**
2020-02-12 10:10:30	Process: **stagingd** (IN: 63.17 MB, OUT: 2.76 MB)
2020-02-13 15:32:49	Process: **roleaccountd** (IN: 0.25 MB, OUT: 0.13 MB)
2020-03-02 08:57:41	Process: **roleaccountd**
2020-03-02 08:57:48	Process: **stagingd**
2020-03-02 08:58:07	Process: **seraccountd**
2020-12-15 10:55:58	Process: **comsercvd**
2020-12-24 08:45:03	Process: **comsercvd** (IN: 17.63 MB, OUT: 64.19 MB)

2020-12-24 16:47:45	Process: **comsercvd**
2021-02-09 09:42:00	Attack related push notifications over iMessage
2021-02-09 10:06:50	Process: **ctrlfs**
2021-02-09 10:06:50	Process: **ctrlfs**
2021-05-20 05:46:42	Process: **com.apple.rapports.events**

Forensic traces for FRHRD1 – Claude Mangin

Phone 1

Date (UTC)	Event
2020-10-08 08:40:42	File created: Library/Preferences/**com.apple.softwareupdateservicesd.plist** from HomeDomain
2020-10-08 10:25:29	Process record deleted from ZPROCESS (IN: 5.46 MB, OUT: 45.62 MB)
2020-10-09 16:17:22	Process record deleted from ZPROCESS (IN: 0.71 MB, OUT: 1.33 MB)
2020-10-10 16:17:24	Process record deleted from ZPROCESS (IN: 0.30 MB, OUT: 0.82 MB)
2020-10-11 16:17:32	Process record deleted from ZPROCESS (IN: 2.25 MB, OUT: 4.88 MB)
2020-10-12 16:51:34	Process record deleted from ZPROCESS (IN: 0.98 MB, OUT: 1.31 MB)
2020-10-13 17:55:23	Process record deleted from ZPROCESS (IN: 1.20 MB, OUT: 5.40 MB)
2020-10-15 17:30:29	Process record deleted from ZPROCESS (IN: 1.56 MB, OUT: 1.92 MB)
2020-10-17 17:08:00	Process record deleted from ZPROCESS (IN: 1.80 MB, OUT: 0.23 MB)
2020-11-18 13:32:24	Process record deleted from ZPROCESS (IN: 1.83 MB, OUT: 0.21 MB)
2020-12-14 15:29:59	Process record deleted from ZPROCESS (IN: 1.83 MB, OUT: 0.25 MB)

2020-12-14 15:31:13	Process record deleted from ZPROCESS (IN: 0.02 MB, OUT: 0.05 MB)
2020-12-15 14:36:59	Process record deleted from ZPROCESS (IN: 1.83 MB, OUT: 0.25 MB)
2021-01-12 14:33:11	Process record deleted from ZPROCESS (IN: 6.99 MB, OUT: 22.26 MB)
2021-01-15 13:39:12	Process record deleted from ZPROCESS (IN: 0.06 MB, OUT: 0.07 MB)
2021-01-16 13:43:10	Process record deleted from ZPROCESS (IN: 2.00 MB, OUT: 1.88 MB)
2021-01-17 15:48:01	Process record deleted from ZPROCESS (IN: 1.25 MB, OUT: 4.43 MB)
2021-01-19 13:58:33	Process record deleted from ZPROCESS (IN: 2.94 MB, OUT: 3.59 MB)
2021-01-21 08:40:52	Process record deleted from ZPROCESS (IN: 1.69 MB, OUT: 1.64 MB)
2021-01-22 08:41:08	Process record deleted from ZPROCESS (IN: 2.50 MB, OUT: 4.70 MB)
2021-03-16 12:33:20	Process record deleted from ZPROCESS (IN: 292.83 MB, OUT: 353.60 MB)
2021-03-17 12:40:45	Process record deleted from ZPROCESS (IN: 0.63 MB, OUT: 0.37 MB)
2021-03-19 10:55:06	Process record deleted from ZPROCESS (IN: 2.74 MB, OUT: 1.72 MB)
2021-03-20 10:57:33	Process record deleted from ZPROCESS (IN: 9.34 MB, OUT: 8.15 MB)
2021-03-21 10:59:08	Process record deleted from ZPROCESS (IN: 12.38 MB, OUT: 19.65 MB)
2021-03-22 11:02:54	Process record deleted from ZPROCESS (IN: 2.54 MB, OUT: 5.11 MB)
2021-03-23 11:34:43	Process record deleted from ZPROCESS (IN: 0.35 MB, OUT: 0.21 MB)
2021-03-24 11:51:11	Process record deleted from ZPROCESS (IN: 2.69 MB, OUT: 1.72 MB)

2021-03-25 12:44:15	Process record deleted from ZPROCESS (IN: 3.74 MB, OUT: 3.94 MB)
2021-03-27 14:43:42	Process record deleted from ZPROCESS (IN: 1.72 MB, OUT: 1.06 MB)
2021-03-27 22:52:14	Process: **brstaged**
2021-03-31 14:18:42	Process record deleted from ZPROCESS (IN: 0.02 MB, OUT: 0.01 MB)
2021-03-31 14:19:03	Process record deleted from ZPROCESS (IN: 1.87 MB, OUT: 0.28 MB)
2021-04-01 05:50:40	Process: **accountpfd**
2021-04-30 12:25:15	Process record deleted from ZPROCESS (IN: 77.19 MB, OUT: 49.49 MB)
2021-05-01 16:35:25	Process record deleted from ZPROCESS (IN: 5.86 MB, OUT: 3.63 MB)
2021-05-03 07:27:01	Process record deleted from ZPROCESS (IN: 1.70 MB, OUT: 0.97 MB)
2021-05-04 07:59:24	Process record deleted from ZPROCESS (IN: 2.66 MB, OUT: 1.77 MB)
2021-05-05 09:09:40	Process record deleted from ZPROCESS (IN: 11.23 MB, OUT: 7.73 MB)
2021-05-07 13:13:51	Process record deleted from ZPROCESS (IN: 5.51 MB, OUT: 3.57 MB)
2021-05-08 13:15:26	Process record deleted from ZPROCESS (IN: 13.65 MB, OUT: 9.88 MB)
2021-05-09 13:18:40	Process record deleted from ZPROCESS (IN: 15.42 MB, OUT: 9.87 MB)
2021-05-10 13:20:46	Process record deleted from ZPROCESS (IN: 0.31 MB, OUT: 0.19 MB)
2021-05-12 09:25:23	Process record deleted from ZPROCESS (IN: 3.87 MB, OUT: 2.33 MB)
2021-05-13 09:26:19	Process record deleted from ZPROCESS (IN: 1.79 MB, OUT: 1.15 MB)

2021-05-14 00:32:59	Process: **comsercvd**
2021-05-15 12:51:46	Process: **com.apple.Mappit.SnapshotService** (IN: 0.03 MB, OUT: 0.01 MB)
2021-05-15 12:56:04	Process record deleted from ZPROCESS (IN: 1.87 MB, OUT: 0.28 MB)
2021-05-15 13:04:10	Process: **roleaboutd**
2021-05-15 13:04:10	Process: **confinstalld**
2021-05-15 13:04:10	Process: **gssdp**
2021-05-15 20:58:34	Process: **roleaboutd**
2021-05-15 20:58:34	Process: **confinstalld**
2021-05-15 20:58:34	Process: **gssdp**
2021-05-16 21:46:58	Process: **roleaboutd**
2021-05-16 21:46:58	Process: **confinstalld**
2021-05-16 21:46:58	Process: **gssdp**
2021-05-17 21:46:13	Process: **roleaboutd**
2021-05-17 21:46:13	Process: **confinstalld**
2021-05-17 21:46:13	Process: **gssdp**
2021-05-18 21:47:13	Process: **roleaboutd**
2021-05-18 21:47:13	Process: **confinstalld**

2021-05-18 21:47:13	Process: **gssdp**
2021-05-19 22:30:36	Process: **roleaboutd**
2021-05-19 22:30:36	Process: **confinstalld**
2021-05-19 22:30:36	Process: **gssdp**
2021-05-21 21:09:59	Process: **roleaboutd**
2021-05-21 21:09:59	Process: **confinstalld**
2021-05-21 21:09:59	Process: **gssdp**
2021-05-22 21:12:51	Process: **roleaboutd**
2021-05-22 21:12:51	Process: **confinstalld**
2021-05-22 21:12:51	Process: **gssdp**
2021-05-23 21:13:37	Process: **roleaboutd**
2021-05-23 21:13:37	Process: **confinstalld**
2021-05-23 21:13:37	Process: **gssdp**
2021-05-23 21:14:55	Process: **roleaboutd**
2021-05-23 21:14:55	Process: **confinstalld**
2021-05-23 21:14:55	Process: **gssdp**
2021-05-25 10:51:16	Process: **roleaboutd**

2021-05-25 10:51:16	Process: **confinstalld**
2021-05-25 10:51:16	Process: **gssdp**
2021-05-26 19:31:58	Process: **roleaboutd**
2021-05-26 19:31:58	Process: **confinstalld**
2021-05-26 19:31:58	Process: **gssdp**
2021-05-27 19:35:21	Process: **roleaboutd**
2021-05-27 19:35:21	Process: **confinstalld**
2021-05-27 19:35:21	Process: **gssdp**
2021-05-28 19:50:06	Process: **roleaboutd**
2021-05-28 19:50:06	Process: **confinstalld**
2021-05-28 19:50:06	Process: **gssdp**
2021-05-29 19:51:18	Process: **roleaboutd**
2021-05-29 19:51:18	Process: **confinstalld**
2021-05-29 19:51:18	Process: **gssdp**
2021-05-31 04:52:47	Process: **roleaboutd**
2021-05-31 04:52:47	Process: **confinstalld**
2021-05-31 04:52:47	Process: **gssdp**

2021-05-31 04:53:49	Process: **roleaboutd**
2021-05-31 04:53:49	Process: **confinstalld**
2021-05-31 04:53:49	Process: **gssdp**
2021-06-01 05:13:25	Process: **roleaboutd**
2021-06-01 05:13:25	Process: **confinstalld**
2021-06-01 05:13:25	Process: **gssdp**
2021-06-01 14:12:05	Process: **PDPDialogs**
2021-06-02 05:14:44	Process: **roleaboutd**
2021-06-02 05:14:44	Process: **confinstalld**
2021-06-02 05:14:44	Process: **gssdp**
2021-06-03 05:23:42	Process: **roleaboutd**
2021-06-03 05:23:42	Process: **confinstalld**
2021-06-03 05:23:42	Process: **gssdp**
2021-06-04 14:38:54	Process: **roleaboutd**
2021-06-04 14:38:54	Process: **confinstalld**
2021-06-04 14:38:54	Process: **gssdp**
2021-06-05 20:26:58	Process: **confinstalld**

2021-06-06 20:33:20	Process: **confinstalld**
2021-06-07 20:31:57	Process: **confinstalld**
2021-06-09 14:42:29	Process: **confinstalld**
2021-06-10 20:09:26	Process: **confinstalld**
2021-06-11 09:34:00	Attack related push notifications over iMessage
2021-06-11 09:35:00	Attack related push notifications over iMessage
2021-06-11 09:36:00	Attack related push notifications over iMessage
2021-06-11 09:37:00	Attack related push notifications over iMessage
2021-06-11 09:37:52	iMessage lookup for account linakeller2203[@]gmail.com
2021-06-11 09:38:00	Attack related push notifications over iMessage
2021-06-11 09:40:00	Attack related push notifications over iMessage
2021-06-11 09:41:00	Attack related push notifications over iMessage
2021-06-11 09:43:00	Attack related push notifications over iMessage
2021-06-11 09:48:37	Process: **com.apple.Mappit.SnapshotService** (IN: 0.02 MB, OUT: 0.01 MB)
2021-06-11 09:48:49	Process: **com.apple.Mappit.SnapshotService**
2021-06-11 09:51:28	Process: **cfprefssd**
2021-06-11 20:25:58	Process: **confinstalld**

2021-06-12 19:30:30	Process: **confinstalld**

Phone 2

Date (UTC)	Event
2021-07-06 12:39:42	iMessage lookup for account **linakeller2203[@]gmail.com**
2021-07-06 12:40:30	Traces from zero-click attack attempt over iMessage

Forensic traces for FRHRD2

Date (UTC)	Event
2019-01-03 11:32	Suspicious SMS with fake Facebook link: **https://web-facebook[.]com/[REDACTED]**

Forensic traces for FRHRL1 – Joseph Breham

Date (UTC)	Event
2019-09-20 10:27:41	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-09-20 10:29:47	iMessage lookup for account **naomiwerff772[@]gmail.com**
2019-10-29 09:04:58	Process: **bh** (IN: 2.86 MB, OUT: 0.21 MB)
2019-10-29 09:05:08	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-10-29 09:05:52	Process: **mptbd** (IN: 18.31 MB, OUT: 106.70 MB)
2019-11-01 12:09:05	Process: **mptbd**
2019-11-01 19:03:23	Process: **mptbd**
2019-11-04 09:35:34	Process: **corecomnetd** (IN: 62.45 MB, OUT: 157.21 MB)
2019-11-07 11:53:06	Process: **corecomnetd**
2019-11-07 19:41:45	Process: **corecomnetd**
2019-11-08 15:27:30	Process: **actmanaged** (IN: 90.27 MB, OUT: 139.34 MB)
2019-11-13 19:09:16	Process: **actmanaged**

2019-11-15 17:07:06	Process: **actmanaged**
2019-11-20 11:15:13	Process: **pstid** (IN: 13.85 MB, WWAN OUT: 1.83 MB)
2019-11-20 11:17:40	Process: **pstid**
2019-11-22 09:17:27	Process: **bh**
2019-11-22 09:22:00	Process: **logseld** (IN: 0.01 MB, WWAN OUT: 0.01 MB)
2019-11-26 09:23:57	Process: **ckeblld** (IN: 0.02 MB, WWAN OUT: 0.01 MB)
2019-11-29 09:38:05	Process: **libbmanaged** (IN: 77.70 MB, OUT: 128.32 MB)
2019-12-05 10:45:44	Process: **libbmanaged**
2019-12-06 08:25:23	Process: **libbmanaged**
2019-12-06 12:02:25	Process: **natgd**
2019-12-09 10:44:59	Process: **launchrexd** (IN: 22.50 MB, OUT: 86.92 MB)
2019-12-15 17:17:59	Process: **launchrexd**
2019-12-16 01:37:31	Process: **launchrexd**
2019-12-18 08:13:29	Process: **bh**
2019-12-18 08:14:05	Process: **ckeblld**
2019-12-18 11:50:15	Process: **ckeblld**
2019-12-22 15:13:04	Process: **natgd** (IN: 5.39 MB, OUT: 35.72 MB)
2019-12-25 08:57:28	iMessage lookup for account **bogaardlisa803[@]gmail.com**

Forensic traces for FRHRL2

Date (UTC)	Event
2019-06-13 14:03:23	File created: Library/Preferences/**com.apple.CrashReporter.plist** from RootDomain
2019-06-13 14:03:42	File created: Library/Preferences/**roleaccountd.plist** from RootDomain

2019-06-13 14:04:00	Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2019-06-13 14:04:00	Process: **stagingd** (IN: 1.47 MB, OUT: 0.08 MB)
2019-06-13 14:04:30	Process: **launchafd** (IN: 0.01 MB, OUT: 0.01 MB)
2019-06-13 14:04:31	Process: **launchafd**
2019-06-13 16:03:43	Process: **roleaccountd**
2019-06-17 17:22:00	Process: **corecomnetd**
2019-06-24 08:58:25	Process: **corecomnetd** (IN: 0.51 MB, OUT: 0.88 MB)
2019-07-01 14:44:29	iMessage lookup for account **b\x00\x00gers.o79[@]gmail.com** (bergers.o79[@]gmail.com)
2019-07-04 09:01:19	Process: **fdlibframed**
2019-07-08 10:14:53	Process: **fdlibframed** (IN: 25.19 MB, OUT: 209.25 MB)
2019-07-10 08:44:54	Process: **fdlibframed**
2019-07-12 13:58:16	iMessage lookup for account **bergers.o79[@]gmail\x00\x00om** (bergers.o79[@]gmail.com)
2019-07-18 18:22:47	Process: **corecomnetd** (IN: 64.69 MB, OUT: 401.88 MB)
2019-07-18 19:53:44	Process: **corecomnetd**
2019-07-22 15:13:11	Process: **roleaboutd**
2019-07-25 18:29:47	Process: **roleaboutd** (IN: 4.62 MB, OUT: 10.40 MB)
2019-07-28 20:24:31	Process: **roleaboutd** (IN: 27.80 MB, OUT: 261.17 MB)
2019-07-29 04:02:57	Process: **roleaboutd**
2019-08-02 15:34:08	Process: **roleaccountd** (IN: 0.02 MB, OUT: 0.01 MB)
2019-08-02 15:34:11	Process: **stagingd** (IN: 2.95 MB, OUT: 0.12 MB)
2019-08-02 15:34:19	Process: **stagingd**
2019-08-02 15:34:36	Process: **pstid** (IN: 10.20 MB, OUT: 68.77 MB)
2019-08-03 13:58:01	Process: **pstid**

2019-08-07 10:40:04	iMessage lookup for account **bergers.o79[@]gmail.com**
2020-02-06 14:52:22	Photostream lookup for account **bogaardlisa803[@]gmail.com**
2021-02-08 10:42:40	iMessage lookup for account **linakeller2203[@]gmail.com**
2021-02-08 11:27:23	Process: **gatekeeperd** (IN: 0.01 MB, OUT: 0.00 MB)
2021-02-08 11:27:25	Process: **bluetoothfs**
2021-02-08 12:27:21	Process: **gatekeeperd**

Forensic traces for FRJRN1 – Lenaig Bredoux

Date (UTC)	Event
2019-07-08 05:22:05	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-10-10 12:39:17	File: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2020-03-12 15:06:23	Process: **frtipd** (IN: 0.05 MB, OUT: 0.43 MB)
2020-03-13 02:20:34	Process: **frtipd**
2020-03-16 10:46:55	Process: **comnetd** (IN: 0.58 MB, OUT: 4.92 MB)
2020-03-20 09:48:10	Process: **comnetd**
2020-03-21 20:09:49	Process: **comnetd**
2020-03-23 13:57:42	Process: **netservcomd** (IN: 0.01 MB, OUT: 0.06 MB)
2020-03-23 21:10:16	Process: **netservcomd**
2020-04-19 12:25:41	Process: **setframed** (IN: 0.23 MB, OUT: 2.00 MB)
2020-04-20 21:32:18	Process: **setframed**
2020-04-22 16:43:22	Process: **launchrexd** (IN: 0.50 MB, OUT: 4.14 MB)
2020-04-27 20:01:46	Process: **launchrexd**
2020-05-01 14:18:15	Process: **nehelprd** (IN: 4.24 MB, OUT: 52.75 MB)

2020-05-03 00:57:11	Process: **nehelprd**
2020-05-04 11:39:47	Process: **msgacntd** (IN: 3.21 MB, OUT: 34.59 MB)
2020-05-06 12:52:13	Process: **msgacntd**
2020-05-06 20:29:07	Process: **msgacntd**
2020-07-07 15:04:34	Process: **aggregatenotd** (IN: 1.10 MB, OUT: 10.69 MB)
2020-05-08 17:56:58	Process: **aggregatenotd**
2020-05-09 10:21:18	Process: **bundpwrd** (IN: 1.37 MB, OUT: 9.63 MB)
2020-05-09 16:52:05	Process: **bundpwrd**
2020-05-12 05:27:20	Process: **seraccountd** (IN: 0.06 MB, OUT: 0.42 MB)
2020-05-12 19:29:17	Process: **seraccountd**
2020-05-13 16:06:41	Process: **otpgrefd** (IN: 1.28 MB, OUT: 13.78 MB)
2020-05-13 17:19:07	Process: **otpgrefd**
2020-05-15 12:23:30	Process: **eventstorpd** (IN: 0.01 MB, OUT: 0.06 MB)
2020-05-16 18:00:50	Process: **eventstorpd**
2020-05-16 18:12:29	Process: **eventstorpd**
2020-05-17 14:42:23	Process: **roleaboutd** (IN: 6.54 MB, OUT: 69.61 MB)
2020-05-20 11:38:45	Process: **roleaboutd**
2020-05-20 21:01:24	Process: **roleaboutd**
2020-05-21 14:54:20	Process: **mptbd** (IN: 0.70 MB, OUT: 8.14 MB)
2020-05-23 16:05:30	Process: **mptbd**
2020-05-23 22:58:10	Process: **bh** (IN: 4.93 MB, OUT: 0.61 MB)
2020-05-24 15:44:39	Process: **bh**
2020-05-24 15:46:51	Process: **fservernetd** (IN: 0.00 MB, OUT: 0.04 MB)

2020-05-24 17:36:36	Process: **fservernetd**
2020-05-26 12:28:34	Process: **brstaged** (IN: 2.56 MB, OUT: 22.61 MB)
2020-05-27 04:33:50	Process: **brstaged**
2020-05-27 14:55:06	Process: **ckkeyrollfd** (IN: 0.01 MB, OUT: 0.09 MB)
2020-05-27 16:58:52	Process: **bh**
2020-05-27 18:00:50	Process: **ckkeyrollfd**
2020-07-10 11:12:35	iMessage account lookup: **bogaardlisa803[@]gmail.com**

Forensic traces for FRJRN2

Date (UTC)	Event
2019-08-16 12:08:44	iMessage lookup for account **bergers.o79[@]gmail.com**
2019-08-16 12:33:52	iMessage lookup for account **bergers.o79[@]gmail\x00\x00om**
2019-08-16 12:37:55	File created: **Library/Preferences/com.apple.CrashReporter.plist** from RootDomain
2019-08-16 12:41:25	File created: **Library/Preferences/roleaccountd.plist** from RootDomain
2019-08-16 12:41:36	Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.01 MB)
2019-08-16 12:41:52	Process: **stagingd** (IN: 1.46 MB, OUT: 0.09 MB)
2019-08-16 12:49:21	Process: **aggregatenotd**
2019-08-20 13:35:23	Process: **aggregatenotd** (IN: 11.07 MB, OUT: 45.52 MB)
2019-08-21 14:10:48	Process: **aggregatenotd**

Forensic traces for FRJRN3 – Edwy Plenel

Date (UTC)	Event
2019-07-05 11:23:29	File: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-07-05 11:23:45	File created: *Library/Preferences/**roleaccountd.plist*** from RootDomain

2019-07-05 11:23:51	Process: **stagingd**
2019-07-05 11:24:19	Process: **eventfssd**
2019-07-07 11:28:15	Process: **eventfssd**
2019-07-09 10:39:41	Process: **fservernetd**
2019-07-09 11:49:48	Process: **fservernetd**
2019-07-12 11:12:24	Process: **nehelprd**
2019-07-14 14:01:26	Process: **nehelprd**
2019-07-20 12:18:30	Process: **libbmanaged**
2019-08-11 14:03:11	Process: **rlaccountd**
2019-08-13 17:34:40	Process: **rlaccountd**
2019-08-19 13:21:02	Process: **libbmanaged**
2019-08-19 14:48:42	Process: **libbmanaged**
2019-08-19 21:51:00	Process: **libbmanaged**
2019-08-28 09:12:33	Process: **roleaccountd**
2019-08-28 09:12:34	Process: **stagingd**
2019-08-28 09:12:49	Process: **stagingd**
2019-08-28 09:13:10	Process: **boardframed**
2019-08-29 09:15:05	Process: **boardframed**
2019-08-31 09:04:17	Process: **boardframed**
2019-08-31 09:49:33	Process: **boardframed**
2019-09-03 10:59:31	Process: **launchafd**
2019-09-05 11:02:43	Process: **launchafd**
2019-09-05 20:32:02	Process: **launchafd**

Forensic traces for FRJRN4 – Bruno Delport

Date (UTC)	Event
2019-07-05 13:21:47	File created *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-07-05 13:21:53	File modified *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain

Forensic traces for FRJRN5

2019-08-16 12:19:54	iMessage lookup for account **b\x00\x00gers.o79[@]gmail.com**
2019-08-19 09:20:01	File created: Library/Preferences/c**om.apple.CrashReporter.plist** from RootDomain
2019-08-19 09:20:30	File created: Library/Preferences/**roleaccountd.plist** from RootDomain
2019-08-19 09:20:45	Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.00 MB)
2019-08-19 09:20:45	Process: **stagingd** (IN: 1.46 MB, OUT: 0.06 MB)
2019-08-19 09:20:50	Process: **stagingd**
2019-08-19 09:21:13	Process: **bundpwrd** (IN: 28.50 MB, OUT: 198.12 MB)
2019-08-21 05:36:00	Process: **bundpwrd**
2019-08-21 07:39:34	iMessage lookup for account **bergers.o79[@]gmail.com**

Forensic traces for FRPOI1

Date (UTC)	Event
2019-03-16 10:42:56	iMessage lookup for account **bergers.o79[@]gmail.com**
2020-08-02 20:03:19	iMessage lookup for account **naomiwerff772[@]gmail.com**

Forensic traces for FRPOI2 – François de Rugy

Date (UTC)	Event
2019-07-XX	iMessage lookup for account **bergers.o79[@]gmail.com**

Forensic traces for FRPOI3 – Philippe Bouyssou

Date (UTC)	Event
2021-07-06 12:20:01	iMessage lookup for account **linakeller2203[@]gmail.com**

Forensic traces for FRPOI4

Date (UTC)	Event
2021-XX-XX	iMessage lookup for account **linakeller2203[@]gmail.com**

Forensic traces for FRPOI5 – Oubi Buchraya Bachir

Date (UTC)	Event
2021-03-15 12:08:27	iMessage lookup for account **linakeller2203[@]gmail.com**
2021-03-15 12:12:49	Traces related to iMessage exploitation
2021-03-15 12:16:02c	File modified: *Library/Caches* from RootDomain

Forensic traces for HUJRN1 – András Szabó

Date (UTC)	Event
2019-06-13 11:15:40	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-06-13 11:15:53	File created: *Library/Preferences/**roleaccountd.plist*** from RootDomain
2019-06-13 12:39:40	Process record deleted from ZPROCESS (IN: 3.69 MB, OUT: 27.39 MB)
2019-06-15 08:06:27	Process record deleted from ZPROCESS (IN: 0.32 MB, OUT: 0.56 MB)
2019-07-25 09:31:09	Process record deleted from ZPROCESS (IN: 7.80 MB, OUT: 6.43 MB)
2019-08-16 10:13:19	Process record deleted from ZPROCESS (IN: 18 MB, OUT: 29.81 MB)
2019-09-15 15:30:44	Process record deleted from ZPROCESS (IN: 1.27 MB, OUT: 3.34 MB)
2019-09-17 06:33:24	Process record deleted from ZPROCESS (IN: 2.00 MB, OUT: 5.57 MB)
2019-09-24 13:26:15	iMessage lookup for account **jessicadavies1345[@]outlook.com**
2019-09-24 13:26:51	iMessage lookup for account **emmadavies8266[@]gmail.com**

2019-09-24 13:32:10	Process: **roleaccountd** (IN: 0.02 MB, OUT: 0.003 MB)
2019-09-24 13:32:11	Process: **roleaccountd**
2019-09-24 13:32:13	Process: **stagingd** (IN: 4.03 MB, OUT: 0.19 MB)
2019-09-24 13:32:23	Process: **stagingd**
2019-09-26 14:32:25	Process record deleted from ZPROCESS (IN: 1.16 MB, OUT: 2.81 MB)
2019-10-24 05:40:33	Process record deleted from ZPROCESS (IN: 12.81 MB, OUT: 46 MB)

Forensic traces for HUJRN2 – Szabolcs Panyi

Date (UTC)	Event
2019-04-04 05:33:02	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-04-04 05:33:12	File created: *Library/Preferences/**roleaccountd.plist*** from RootDomain
2019-04-04 06:02:26	Process: **libbmanaged** (IN: 23.29 MB, OUT: 21.39 MB)
2019-04-06 21:47:45	Process: **libbmanaged**
2019-07-05 08:35:28	Process: **ckeblld** (IN: 45.44 MB, OUT: 118.06 MB)
2019-07-12 20:49:11	Process: **ckeblld**
2019-07-13 20:32:28	Process: **ckeblld**
2019-07-15 12:02:37	iMessage lookup for account **e\x00\x00adavies8266[@]gmail.com** (emmadavies8266[@]gmail.com)
2019-07-15 14:21:40	Process: **accountpfd** (IN: 0.88 MB, OUT: 1.77 MB)
2019-07-16 14:25:11	Process: **accountpfd**
2019-08-29 10:57:43	Process: **roleaccountd** (IN: 0.01 MB, OUT: 0.003 MB)

2019-08-29 10:57:44	Process: **stagingd** (IN: 4.05 MB, OUT: 0.20 MB)
2019-08-29 10:58:35	Process: **launchrexd** (IN: 0.03 MB, OUT: 0.01 MB)
2019-09-03 07:54:26	Process: **roleaccountd**
2019-09-03 07:54:28	Process: **stagingd**
2019-09-03 07:54:51	Process: **seraccountd** (IN: 20.94 MB, OUT: 7.52 MB)
2019-09-05 08:00:15	Process: **seraccountd**
2019-09-05 13:26:38	Process: **seraccountd**
2019-09-05 13:26:55	Process: **misbrigd** (IN: 10.12 MB, OUT: 8.13 MB)
2019-09-06 13:27:04	Process: **misbrigd**
2019-09-06 22:04:12	Process: **misbrigd**
2019-09-10 06:09:04	iMessage lookup for account **emmadavies8266[@]gmail.com**
2019-09-10 06:09:49	iMessage lookup for account **jessicadavies1345[@]outlook.com**
2019-10-30 14:09:51	Process: **nehelprd** (IN: 23.45 MB, OUT: 8.64 MB)
2019-11-04 14:27:48	Process: **nehelprd**
2019-11-07 01:58:52	Process: **nehelprd**

Forensic traces for HUPOI1

Date (UTC)	Event

2018-06-01 12:33:08	Process: **stagingd**
2018-06-01 12:33:08	Process: **roleaccountd**
2018-06-01 12:35:55	Process: **fmld**
2018-06-05 18:21:35	Process: **stagingd** (IN: 7.17 MB, OUT: 0.01 MB)
2018-06-08 14:42:05	Process: **fmld** (IN: 3.52 MB, OUT: 0.07 MB)
2018-06-21 07:02:55	File created: Library/Preferences/**com.apple.CrashReporter.plist** from RootDomain
2018-06-21 07:03:19	Process: **roleaccountd** (IN: 0.05 MB, OUT: 0.00 MB)
2018-06-21 07:03:31	Process: **stagingd**
2018-06-27 05:04:19	Thumper lookup for account **k.williams.enny74[@]gmail.com**
2018-06-27 08:09:04	Process: **bh** (IN: 4.42 MB, OUT: 0.29 MB)
2018-07-09 08:30:34	Process: **bh**
2018-07-10 08:31:19	Process: **fmld** (IN: 22.54 MB, OUT: 64.62 MB)
2018-07-10 09:40:37	Process: **fmld**

Forensic traces for HUPOI2 – Adrien Beauduin

Date (UTC)	Event
2018-12-19 09:13:48	File created: Library/Preferences/**com.apple.CrashReporter.plist** from RootDomain
2018-12-19 09:15:57	File modified: **Library/Caches** from RootDomain
2018-12-20 11:06:49	Thumper lookup for account **k.williams.enny74[@]gmail.com**

Forensic traces for HUPOI3

Date (UTC)	Event
2018-06-01 10:12:49	IMessage lookup for **k.williams.enny74[@]gmail.com**

Forensic traces for INHRD1 – SAR Geelani

Date (UTC)	Event
2017-07-05 15:01:28	Process: **pcsd**
2017-11-30 09:26:33	Process: **pcsd** (IN: 24.09 MB, OUT: 211.43 MB)
2017-12-19 06:48:00	Process: **pcsd**
2018-02-13 12:46:10	SMS from +447797801009: United Nations launches online portal for the independence of Kashmir. To cast your online vote click here **http://bit[.]ly/2o487h1** (**https://signpetition[.]co/vU1zwaqFh**)
2018-02-15 12:06:01	SMS from +447797801009: BJP hatches conspiracy for a muslim free Jammu region through medical poisoning of muslims. **http://bit[.]ly/2o95TNh** (**https://news-alert[.]org/TfteZB6wK**)
2018-02-16 09:44:46	SMS from +447797801009: Another incident showing Indian army beating librandu Kashmiri youth mercilessly to chant Pakistan Murdabad. **http://bit[.]ly/2ob9QkO** (**https://news-alert[.]org/K9pAkFk3R**)
2018-04-12 14:10:57	SMS from +447797801009: Organization of Islamic countries(OIC) launches online portal for the independence of Kashmir from India. For the detailed article, click here **http://bit[.]ly/2Hk1UJE (https://news-alert[.]org/WW7G1EW2)**
2018-04-13 13:13:30	SMS from +447797801009: Global powers urge Indian leadership to concede the entire Jammu & Kashmir to Pakistan for regional peace and stability. For the detailed article, click here. **https://news-alert[.]org/T1q4YjltT**
2018-04-16 10:52:26	SMS from +447797801009: Hot & sexy male & female escorts available at 60% discount. To avail the service, please click on **https://my-privacy[.]co/Ooboe7u**
2018-04-17 12:39:36	SMS from +447797801009: European Union leads its unconditional support to India over the issue of Kashmir during the current visit of PM Modi. For more details, click **https://my-privacy[.]co/j2xgK558**
2018-04-20 13:36:02	SMS from +447797801009: India & America strategically conspiring for the failure of China Pakistan Economic Corridor(CPEC). For the detailed article, click here. **https://my-privacy[.]co/ZOubFbXW**
2018-04-23 12:58:31	SMS from +447797801009: Syed Ali Shah Geelani comes out with 5 point proposal for India, Pak. **http://bit[.]ly/2HkhW2L (https://news-alert[.]org/1M2VbKPeB)**

2018-04-27 08:17:38	SMS from +447797801009: Pakistan always stood like a rock guarding Kashmir cause says Geelani. **http://bit[.]ly/2FI7Dtq (https://news-alert.org/xdwWVvCP)**
2018-04-27 12:02:13	SMS from +447797801009: Yasin Malik to address press conference at UN.For detail news click at **http://bit[.]ly/2FlNjlC (https://news-alert[.]org/CyCX97BO)**
2018-05-01 11:57:38	SMS from +447797801009: Pakistan strategically preparing to put the issue of Kashmir in International Court of Justice. Read full storey here **http://bit[.]ly/2Fwg2dH (https://news-alert[.]org/AXJ1n6e)**
2018-05-02 12:36:16	SMS from +447797801009: Pakistan in all probability will become the next province of China through China Pakistan Economic Corridor (CPEC). For the detailed article, click here. **https://news-alert[.]org/KYz4FG6**
2018-05-18 04:37:42	Process: **fmld**
2018-05-24 04:18:31	Process: **roleaccountd**
2018-05-24 04:18:41	Process: **stagingd**
2018-07-20 14:05:14	Thumper lookup for account **taylorjade0303[@]gmail.com**
2018-10-24 08:48:04	Process: **fmld** (IN: 208.63 MB, OUT: 3591.56 MB)
2018-10-27 07:05:42	Process: **roleaccountd** (IN: 0.28 MB, OUT: 0.04 MB)
2018-10-27 07:05:50	Process: **stagingd** (IN: 53.02 MB, OUT: 0.15 MB)
2018-10-28 07:09:14	Process: **fmld** (IN: 1.84 MB, OUT: 110.30 MB)
2018-10-29 07:16:51	Process: **fmld** (IN: 1.70 MB, OUT: 69.41 MB)

2018-10-30 07:25:43	Process: **fmld** (IN: 1.25 MB, OUT: 4.15 MB)
2018-10-31 07:29:37	Process: **fmld** (IN: 0.63 MB, OUT: 19.51 MB)
2018-12-08 07:24:18	Process: **fmld** (IN: 9.88 MB, OUT: 150.38 MB)
2018-12-10 06:23:11	Process: **fmld**
2018-12-27 09:44:30	Process: **otpgrefd** (IN: 1.66 MB, OUT: 20.07 MB)
2018-12-28 09:08:32	Process: **otpgrefd**
2018-12-31 06:37:59	Process: **bfrgbd**
2019-01-02 06:45:14	Process: **bfrgbd** (IN: 3.02 MB, OUT: 59.12 MB)
2019-01-02 15:34:37	Process: **bfrgbd**
2019-01-03 07:13:41	Process: **stagingd** (IN: 12.96 MB, OUT: 0.05 MB)
2019-01-03 07:20:50	Process: **fservernetd** (IN: 0.58 MB, OUT: 15.90 MB)
2019-01-03 08:35:44	Process: **fservernetd**
2019-01-05 05:28:58	Process: **libtouchregd** (IN: 1.04 MB, OUT: 41.43 MB)

2019-01-05 05:33:02	Process: **libtouchregd** (IN: 0.00 MB, OUT: 0.38 MB)
2019-01-07 06:06:22	Process: **roleaccountd** (IN: 0.05 MB, OUT: 0.01 MB)
2019-01-07 06:09:43	Process: **stagingd**
2019-01-07 06:11:34	Process: **accountpfd** (IN: 1.41 MB, OUT: 9.05 MB)
2019-01-07 18:13:34	Process: **accountpfd**
2019-01-25 07:26:52	Thumper lookup for account **lee.85.holland[@]gmail.com**
2019-01-25 07:33:59	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-01-25 07:34:08	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-01-26 14:16:19	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-09-22 05:14:27	iMessage lookup for account **bekkerfredi[@]gmail.com**
2019-09-27 09:20:58	SMS from +9159039000: Trump to mediate between India and Pakistan on Kashmir **https://bit[.]ly/eclCPjk**
2019-09-27 09:32:59	Process: **bh** (IN: 1.47 MB, OUT: 0.09 MB)
2019-09-27 09:33:49	Process: **natgd** (IN: 19.95 MB, OUT: 171.65 MB)

2019-09-28 13:49:07	Process: **natgd**
2019-10-15 08:40:38	SMS from +9156161940: Get Rs 100 off on recharge of your Tata Sky Id 1093453759 **https://todaysdeals4u[.]com/n7V7uA4X5**
2019-10-18 10:34:49	SMS from +9156161940: Avail extra benefits on recharge of your Tata Sky Id 1093453759 **https://todaysdeals4u[.]com/KjtvDBA**
2019-10-23 17:07:15	Process: **frtipd** (IN: 2.24 MB, OUT: 2.87 MB)
2019-10-24 19:27:51	Process: **frtipd**

Forensic traces for INJRN1 – Mangalam Kesavan Venu

Date (UTC)	Event
2021-02-16 18:40:27	Process: **frtipd**
2021-02-22 21:34:35	Process: **otpgrefd**
2021-03-25 08:11:28	Process: **boardframed**
2021-03-25 08:11:28	Process: **comsercvd**
2021-05-15 05:06:16	Process: **llmdwatchd**
2021-05-15 05:06:16	Process: **aggregatenotd**
2021-05-21 19:17:37	Process: **setframed**
2021-06-03 19:15:52	Process: **seraccountd**
2021-06-07 07:09:16	Upgrade from iOS 14.4.2 to 14.6
2021-06-11 14:02:14	Process: **comsercvd**
2021-06-11 14:02:14	Process: **Diagnostics-2543**
2021-06-16 05:53:28	Process: **actmanaged**

2021-06-16 05:53:28	Process: **nehelprd**
2021-06-16 05:53:29	Process: **cfprefssd**
2021-06-16 05:58:43	Process: **actmanaged**
2021-06-16 06:18:04	Process: **actmanaged**
2021-06-16 07:01:03	Process: **actmanaged**
2021-06-16 07:16:45	Process: **cfprefssd**
2021-06-16 07:16:45	Process: **nehelprd**
2021-06-23 13:39:51	Process record deleted from ZPROCESS (IN: 0.20 MB, OUT: 2.04 MB)
2021-06-27 03:27:12	iMessage lookup for account **herbruud2[@]gmail.com**
2021-06-27 03:49:51	Process: **corecomnetd** (IN: 1.25 MB, OUT: 13.20 MB)
2021-06-28 11:11:36	Process: **corecomnetd** (IN: 0.03, OUT: 0.04 MB)
2021-06-29 07:26:55	Process: **corecomnetd**

Forensic traces for INJRN2 – Sushant Singh

Date (UTC)	Event
2021-03-31 13:45:32	Process: **CommsCenterRootHelper** (IN: 0.01 MB, OUT: 4.41 KB)
2021-03-31 13:45:46	Process: **CommsCenterRootHelper**
2021-04-07 09:34:40	Process: **eventfssd**
2021-04-07 09:34:40	Process: **locserviced**
2021-04-13 08:52:18	Process: **accountpfd**
2021-04-13 08:52:18	Process: **fservernetd**
2021-04-19 15:49:38	Process: **otpgrefd**
2021-04-19 15:49:38	Process: **ckeblld**

2021-04-26 13:54:30	Process record deleted from ZPROCESS (IN: 4.24 MB, OUT: 2.19 MB)
2021-04-27 03:34:16	Process: **comsercvd**
2021-06-05 13:36:54	Process record deleted from ZPROCESS (IN: 0.11 MB, OUT:
2021-06-06 13:38:51	Process record deleted from ZPROCESS (IN: 0.10 MB, OUT: 0.11 MB)
2021-06-07 13:41:51	Process record deleted from ZPROCESS (IN: 0.16 MB, OUT: 0.17 MB)
2021-06-08 13:42:25	Process record deleted from ZPROCESS (IN: 0.11MB, OUT: 0.13 MB)
2021-06-10 13:42:35	Process record deleted from ZPROCESS (IN: 0.10 MB, OUT: 0.11 MB)
2021-06-12 19:09:37	Process: **faskeepd**
2021-06-12 19:09:37	Process: **logseld**
2021-06-18 09:40:45	Process record deleted from ZPROCESS (IN: 0.20 MB, OUT: 0.23 MB)
2021-06-19 14:25:16	Process record deleted from ZPROCESS (IN: 0.04 MB, OUT:
2021-06-19 17:05:21	Process: **xpccfd**
2021-06-19 17:05:21	Process: **pstid**
2021-06-21 05:29:38	iMessage lookup for account **herbruud2[@]gmail.com**
2021-06-21 05:56:55	Process: **bfrgbd**
2021-06-21 05:56:55	Process: **msgacntd**
2021-06-21 05:56:55	Process: **CommsCenterRootHelper**
2021-06-21 06:29:13	Process: **bfrgbd**
2021-06-21 06:59:25	Process: **bfrgbd**
2021-06-21 08:22:27	Process: **bfrgbd** (IN: 1.02 MB, OUT: 2.25 MB)
2021-06-21 13:33:03	Process: **bfrgbd**
2021-06-21 13:33:03	Process: **msgacntd**
2021-06-21 13:33:03	Process: **CommsCenterRootHelper**

2021-06-21 13:34:01	Process: **bfrgbd**
2021-06-21 13:34:01	Process: **msgacntd**
2021-06-21 13:34:01	Process: **CommsCenterRootHelper**
2021-06-22 09:47:01	Process: **bfrgbd** (IN: 0.50 MB, OUT: 0.65 MB)
2021-06-22 14:06:24	Process: **bfrgbd**
2021-06-22 14:06:24	Process: **msgacntd**
2021-06-22 14:06:24	Process: **CommsCenterRootHelper**
2021-06-23 09:50:46	Process: **bfrgbd** (IN: 0.86 MB, OUT: 1.05 MB)
2021-06-23 15:02:35	Process: **bfrgbd**
2021-06-23 15:02:35	Process: **msgacntd**
2021-06-23 15:02:35	Process: **CommsCenterRootHelper**
2021-06-24 09:50:51	Process: **bfrgbd** (IN: 0.44 MB, OUT: 60.72 MB)
2021-06-24 15:02:23	Process: **bfrgbd**
2021-06-24 15:02:23	Process: **msgacntd**
2021-06-24 15:02:23	Process: **CommsCenterRootHelper**
2021-06-25 09:59:00	Process: **bfrgbd** (IN: 0.74 MN, OUT: 5.53 MB)
2021-06-25 15:03:09	Process: **bfrgbd**
2021-06-25 15:03:09	Process: **msgacntd**
2021-06-25 15:03:09	Process: **CommsCenterRootHelper**
2021-06-26 13:04:37	Process: **bfrgbd** (IN: 0.08 MB, OUT: 0.09 MB)
2021-06-26 16:18:41	Process: **bfrgbd**
2021-06-26 16:18:41	Process: **msgacntd**
2021-06-26 16:18:41	Process: **CommsCenterRootHelper**

2021-06-26 16:22:12	Process: **bfrgbd**
2021-06-26 16:22:12	Process: **msgacntd**
2021-06-26 16:22:12	Process: **CommsCenterRootHelper**
2021-06-27 13:34:07	Process: **bfrgbd** (IN: 0.91 MB, OUT: 1.29 MB)
2021-06-28 00:04:15	Process: **bfrgbd**
2021-06-28 00:04:15	Process: **msgacntd**
2021-06-28 00:04:15	Process: **CommsCenterRootHelper**
2021-06-28 13:37:38	Process: **bfrgbd** (IN: 0.43 MB, OUT: 0.60 MB)
2021-06-29 06:39:31	Process: **bfrgbd**
2021-06-29 06:39:31	Process: **msgacntd**
2021-06-29 06:39:31	Process: **CommsCenterRootHelper**
2021-06-29 06:40:42	Process: **bfrgbd**
2021-06-29 06:40:42	Process: **msgacntd**
2021-06-29 06:40:42	Process: **CommsCenterRootHelper**
2021-06-29 14:12:36	Process: **bfrgbd** (IN: 0.14 MB, OUT: 0.17 MB)
2021-06-30 07:15:33	Process: **bfrgbd**
2021-06-30 07:15:33	Process: **msgacntd**
2021-06-30 07:15:33	Process: **CommsCenterRootHelper**
2021-06-30 14:15:33	Process: **bfrgbd** (IN: 0.61 MB, OUT: 1.90 MB)
2021-07-01 14:19:26	Process: **bfrgbd** (IN: 0.30 MB, OUT: 0.46 MB)
2021-07-01 14:33:08	Process: **bfrgbd**
2021-07-01 14:33:08	Process: **msgacntd**
2021-07-01 14:33:08	Process: **CommsCenterRootHelper**

2021-07-02 14:20:32	Process: **bfrgbd** (IN: 0.43 MB, OUT: 0.50 MB)
2021-07-03 04:14:29	Process: **bfrgbd**
2021-07-03 04:14:29	Process: **msgacntd**
2021-07-03 04:14:29	Process: **CommsCenterRootHelper**
2021-07-03 14:27:24	Process: **bfrgbd** (IN: 0.03 MB, OUT: 0.02 MB)
2021-07-04 05:34:57	Process: **bfrgbd**
2021-07-04 05:34:57	Process: **msgacntd**
2021-07-04 05:34:57	Process: **CommsCenterRootHelper**
2021-07-04 14:39:00	Process: **bfrgbd** (IN: 0.77 MB, OUT: 0.91 MB)
2021-07-05 09:40:02	Process: **bfrgbd**
2021-07-05 12:12:01	Process: **bfrgbd**
2021-07-05 12:12:01	Process: **msgacntd**
2021-07-05 12:12:01	Process: **CommsCenterRootHelper**
2021-07-05 12:13:31	Process: **bfrgbd**
2021-07-05 12:13:31	Process: **msgacntd**
2021-07-05 12:13:31	Process: **CommsCenterRootHelper**
2021-07-05 12:50:32	Process: **msgacntd**
2021-07-05 12:50:32	Process: **bfrgbd**

Forensic traces for INJRN3 – SNM Abdi

Date (UTC)	Event
2019-04-02 04:51:19	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2019-04-02 04:51:40	File created *Library/Preferences/**roleaccountd.plist*** from RootDomain

2019-04-02 04:51:45	Process: **roleaccountd**
2019-04-02 04:51:50	Process: **stagingd**
2019-04-26 03:27:40	Process: **fdlibframed**
2019-04-28 04:00:46	Process: **fdlibframed** (IN: 7.90 MB, OUT: 25.36 MB)
2019-04-29 12:56:34	Process: **fdlibframed**
2019-05-27 04:46:07	Process: **xpccfd**
2019-05-28 04:48:01	Process: **xpccfd** (IN: 5.24 MB, OUT: 15.32 MB)
2019-07-04 03:33:11	Process: **ckeblld** (IN: 7.91 MB, OUT: 33.05 MB)
2019-07-05 01:22:18	Process: **ckeblld**
2019-07-05 09:22:54	Process: **lobbrogd** (IN: 3.76 MB, OUT: 15.59 MB)
2019-07-06 03:20:03	Process: **lobbrogd**
2019-07-08 05:56:52	Process: **xpccfd** (IN: 5.69 MB, OUT: 16.14 MB)
2019-07-10 01:24:04	Process: **xpccfd**
2019-07-11 06:46:37	Process: **pstid** (IN: 3.59 MN, OUT: 12.08 MB)
2019-07-11 13:41:50	Process: **pstid**
2019-07-12 09:07:18	Process: **roleaccountd** (IN: 0.03 MB, OUT: 0.02 MB)
2019-07-12 09:08:07	Process: **boardframed** (IN: 6.24 MB, OUT: 32.14 MB)
2019-07-12 14:15:01	Process: **boardframed**
2019-07-15 06:07:28	Process: **stagingd** (IN: 8.49 MB, OUT: 0.5 MB)
2019-07-15 18:08:57	Process: **ckkeyrollfd**
2019-10-19 04:32:33	Process: **roleaccountd** (IN: 0.04 MB, OUT: 0.02 MB)
2019-10-19 04:33:46	Process: **launchafd** (IN: 1.28 MB, OUT: 6.48 MB)
2019-10-19 06:10:04	Process: **launchafd**

2019-10-21 07:07:16	Process: **netservcomd** (IN: 0.22 MB, OUT: 1.26 MB)
2019-10-21 07:31:16	Process: **netservcomd**
2019-10-23 03:48:40	Process: **roleaccountd**
2019-10-23 03:48:47	Process: **stagingd** (IN: 7.03 MB, OUT: 0.41 MB)
2019-10-23 03:49:02	Process: **stagingd**
2019-10-23 03:49:24	Process: **misbrigd**
2019-10-24 03:50:28	Process: **misbrigd** (IN: 15.79 MB, OUT: 99.28 MB)
2019-12-22 11:15:30	Process: **netservcomd**
2019-12-22 11:15:30	Process: **launchafd**
2019-12-22 11:15:30	Process: **misbrigd**

Forensic traces for INJRN4 – Siddharth Varadarajan

Date (UTC)	Event
2018-04-06 08:17:14	Process: **roleaccountd** (IN: 0.03 MB, OUT: 0.01 MB)
2018-04-06 08:17:22	Process: **stagingd**
2018-04-06 08:18:47	Process: **pcsd**
2018-04-24 07:57:53	Process: **stagingd** (IN: 4.15 MB, OUT: 0.02 MB)
2018-04-24 07:57:56	Process: **roleaccountd**
2018-04-24 07:58:16	Process: **stagingd**
2018-04-26 05:35:12	Process: **pcsd** (IN: 16.30 MB, OUT: 329.17 MB)
2018-04-26 12:24:42	Process: **pcsd**
2018-04-27 04:41:37	File created Library/Preferences/**com.apple.CrashReporter.plist** in RootDomain

Forensic traces for INJRN5 – Paranjoy Guha Thakurta

Date (UTC)	Event
2018-04-04 05:33:47	Process: **roleaccountd**
2018-04-04 05:33:49	Process: **stagingd**
2018-05-15 07:46:30	Process: **pcsd**
2018-05-22 04:17:46	Process: **roleaccountd** (IN: 0.04 MB, OUT: 0.01 MB)
2018-05-22 04:17:59	Process: **stagingd** (IN: 5.18 MB, OUT: 0.02 MB)
2018-05-22 04:18:08	Process: **pcsd** (IN: 3.25 MB, OUT: 20.54 MB)
2018-05-22 04:18:17	Process: **pcsd**
2018-05-22 04:18:48	Process: **fmld**
2018-06-20 10:44:14	Process: **roleaccountd**
2018-06-20 10:44:31	Process: **stagingd**
2018-07-25 03:58:42	File created Library/Preferences/**com.apple.CrashReporter.plist** from RootDomain
2018-07-29 13:07:51	Process: **fmld** (IN: 55.21 MB, OUT: 417.58 MB)
2018-07-30 11:07:56	Process: **fmld**

Forensic traces for INJRN6 – Smita Sharma

Date (UTC)	Event
2018-06-25 17:31:37	iMessage lookup for **taylorjade0303[@]gmail.com**
2018-07-20 11:11:49	iMessage lookup for **lee.85.holland[@]gmail.com**

Forensic traces for INJRN7

Date (UTC)	Event
2019-06-12 08:48:04	SMS “R&AW and IB chief to get three months extension. Read full story **https://globalnews247[.]net/3BMw9Zj**”

Forensic traces for INPOI1 – Prashant Kishor

Date (UTC)	Event
2018-06-21 13:23:30	Thumper lookup for account **taylorjade0303[@]gmail.com**
2018-09-06 09:11:49	Thumper lookup for account **lee.85.holland[@]gmail.com**
2021-04-28 03:31:39	Process: **ReminderIntentsUIExtension** (IN: 0.01 MB, OUT: 0.00 MB)
2021-04-28 03:31:39	Process: **ReminderIntentsUIExtension**
2021-04-28 03:31:45	Process: **ReminderIntentsUIExtension**
2021-06-11 12:45:48	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-11 12:46:22	Process record deleted from ZPROCESS (IN: 1.79 MB, OUT: 0.31 MB)
2021-06-11 12:46:47	Process record deleted from ZPROCESS (IN: 12.94 MB, OUT: 145.88 MB)
2021-06-14 06:17:10	Process record deleted from ZPROCESS (IN: 2.36 MB, OUT: 2.76 MB)
2021-06-15 06:21:28	Process record deleted from ZPROCESS (IN: 1.05 MB, OUT: 1.29 MB)
2021-06-16 13:47:51	Process record deleted from ZPROCESS (IN: 0.16 MB, OUT: 0.16 MB)
2021-06-18 13:52:14	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-06-18 13:53:37	Process record deleted from ZPROCESS (IN: 1.79 MB, OUT: 0.31 MB)
2021-06-18 13:58:41	Process record deleted from ZPROCESS (IN: 13.63 MB, OUT: 172.99 MB)
2021-06-19 14:16:20	Process record deleted from ZPROCESS (IN: 0.87 MB, OUT: 1.02 MB)
2021-06-21 05:44:29	Process record deleted from ZPROCESS (IN: 1.81 MB, OUT: 2.58 MB)
2021-06-22 05:45:29	Process record deleted from ZPROCESS (IN: 1.19 MB, OUT: 1.38 MB)
2021-06-23 05:49:37	Process record deleted from ZPROCESS (IN: 0.98 MB, OUT: 1.19 MB)
2021-06-24 05:57:02	Process record deleted from ZPROCESS (IN: 2.66 MB, OUT: 24.15 MB)
2021-06-25 05:57:03	Process record deleted from ZPROCESS (IN: 1.98 MB, OUT: 2.77 MB)
2021-06-26 06:01:26	Process record deleted from ZPROCESS (IN: 0.35 MB, OUT: 0.47 MB)
2021-06-27 06:06:59	Process record deleted from ZPROCESS (IN: 0.42 MB, OUT: 0.49 MB)

2021-06-28 13:19:57	Process record deleted from ZPROCESS (IN: 1.12 MB, OUT: 7.33 MB)
2021-06-30 04:50:04	Process record deleted from ZPROCESS (IN: 1.51 MB, OUT: 6.50 MB)
2021-07-01 04:50:49	Process record deleted from ZPROCESS (IN: 0.52 MB, OUT: 0.60 MB)
2021-07-02 05:08:42	Process record deleted from ZPROCESS (IN: 1.48 MB, OUT: 1.73 MB)
2021-07-03 05:33:23	Process record deleted from ZPROCESS (IN: 1.00 MB, OUT: 2.03 MB)
2021-07-05 11:44:29	Traces related to iMessage attack
2021-07-05 11:48:34	File created: **Library/Caches** from RootDomain
2021-07-05 11:48:35	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-07-05 11:49:27	Process: **CommsCenterRootHelper** (IN: 1.88 MB, OUT: 0.31 MB)
2021-07-05 11:49:27	Process: **CommsCenterRootHelper**
2021-07-05 11:50:19	Process record deleted from ZPROCESS (IN: 7.57 MB, OUT: 90.71 MB)
2021-07-07 04:11:55	Process record deleted from ZPROCESS (IN: 0.62 MB, OUT: 0.77 MB)
2021-07-08 12:21:05	iMessage lookup for account **herbruud2[@]gmail.com**
2021-07-08 12:27:04	Process record deleted from ZPROCESS (IN: 0.01 MB, OUT: 0.00 MB)
2021-07-08 12:27:18	Process record deleted from ZPROCESS (IN: 1.88 MB, OUT: 0.23 MB)
2021-07-08 12:28:14	Process: **smmsgingd** (IN: 6.94 MB, OUT: 82.77 MB)
2021-07-09 12:59:49	Process: **smmsgingd** (IN: 0.45 MB, OUT: 0.51 MB)
2021-07-12 08:45:26	Process: **smmsgingd** (IN: 2.69 MB, OUT: 7.99 MB)
2021-07-13 08:47:45	Process: **smmsgingd** (IN: 1.23 MB, OUT: 8.63 MB)
2021-07-14 09:26:50	Process: **smmsgingd** (IN: 0.77 MB, OUT: 2.28 MB)
2021-07-14 13:17:15	Process: **smmsgingd**

Forensic traces for INPOI2

Date (UTC)	Event
2019-10-18 03:59:01	iMessage lookup for **bekkerfredi[@]gmail.com**

Forensic traces for KASH01 – Hatice Cengiz

Date (UTC)	Event
2018-10-06 00:33:28	File created: *Library/Preferences/**com.apple.CrashReporter.plist*** from RootDomain
2018-10-06 07:30:13	Process: **fmld** (IN: 33.27 MB, OUT: 324.72 MB)
2018-10-09 07:12:39	Process: **bh** (IN: 1.49 MB, OUT: 0.95 MB)
2018-10-09 07:13:07	Process: **bh**
2018-10-12 08:30:33	Process: **fmld**
2018-10-12 21:23:23	Process: **fmld**
2019-06-02 16:05:23	iMessage lookup for account **vincent.dahl76[@]gmail.com**

Forensic traces for KASH02 – Rodney Dixon

Date (UTC)	Event
2019-04-29 10:50:44	iMessage lookup for account **vincent.dahl76[@]gmail.com**

Forensic traces for KASH03 – Wadah Khanfar

Phone 1:

Date (UTC)	Event
2019-11-02 17:19:22	Process record deleted from ZPROCESS
2019-11-02 17:19:29	File created *Library/Preferences/**com.apple.CrashReporter.plist*** by RootDomain
2019-11-02 17:20:23	Process record deleted from ZPROCESS
2021-04-11 08:35:25	Process: **ReminderIntentsUIExtension** (IN: 0.01 MB, OUT: 0.00 MB)
2021-04-11 08:35:33	Process: **ReminderIntentsUIExtension**

2021-06-30 08:58:04	iMessage lookup for account **oskarschalcher[@]outlook.com**
2021-06-30 09:34:34	Process: **com.apple.Mappit.SnapshotService** (IN: 0.02 MB, OUT: 0.01 MB)
2021-06-30 09:34:40	Process: **com.apple.Mappit.SnapshotService**

Phone 2:

Date (UTC)	Event
2021-04-02 10:43:27	iMessage lookup for **oskarschalcher[@]outlook.com**

Forensic traces for KASH04 – Hanan El Atr

Date (UTC)	Event
2017-11-08 10:22	Malicious SMS from VERIFY: WhatsApp Web for [REDACTED] is now active on CHROME in ABU DHABI. Not you? Click here: **hxxps://noonstore[.]sale/tkYHFbE**
2017-11-15 09:01	Malicious SMS from VERIFY: Emirates AIrline changing the game in first class travel: **hxxp://bit[.]ly/2A00El7**
2017-11-19	Malicious SMS from VERIFY: Dear Hanan Elatr, Nada shared a photo with you on Photobucket! Click here to view it and download our app. **hxxp://bit[.]ly/AbzvEMS**
2018-11-26 17:16:48	Malicious link in browsing history: **https://done[.]events/TajbxOGh5**
2017-11-27 08:48	Malicious SMS: Dear HANA you have a package from CAIRO via Aramex, enter PIN 3483 and choose delivery location on our map: **https://bit[.]ly/2zxnwOF**
2018-04-15 09:33	Malicious SMS from SMSINFO: MONA ELATR shared a photo with you on Photobucket! Click here to view it and download our app: **https://myfiles[.]photo/sVIKHJE**

Forensic traces for MOJRN1 – Hicham Mansouri

Date (UTC)	Event
2021-02-04 10:31:36	Process: **CommsCenterRootHelper** (IN: 0.01 MB, OUT: 0.00 MB)
2021-02-11 13:45:07	Process: **CommsCenterRootHelper**
2021-04-02 10:15:38	iMessage lookup for account **linakeller2203[@]gmail.com**

Forensic traces for MXJRN1

Date (UTC)	Event
2016-08-03 21:52:00	SMS: Hola Alvaro unicamente paso a saludarte y enviarte esta nota de the guardian que parece importante retomar: **http://bit[.]ly/2ayGnMm (https://smsmensaje[.]mx/5901888s/)**

Forensic traces for MXJRN2 – Carmen Aristegui

These Pegasus attack messages were original discovered and published as part of collaborative investigation between Citizen Lab, R3D, SocialTic and Article 19.

Date (UTC)	Event
2014-11-20 03:10:04	SMS from +525536438524: El siguiente mensaje esta marcado como urgente y no se recibio correctamente. **http://smsmensaje[.]mx/5103285s/**
2014-12-17 19:32:13	SMS from +525511393977: El siguiente mensaje no ha sido enviado **http://smscentro[.]com/7984947s/**
2015-01-06 18:29:53	SMS from +525512350872: El siguiente mensaje no ha sido enviado **http://smscentro[.]com/4064303s/**
2015-01-09 19:45:57	SMS from +525512350872: El siguiente mensaje no ha sido enviado **http://tinyurl[.]com/l8cwcc5 (http://smscentro[.]com/1097486s/)**
2015-01-13 01:59:19	SMS from +525511393877: El siguiente mensaje no ha sido enviado **http://bit[.]ly/1z2NQdh (http://smscentro[.]com/9480260s/)**
2015-03-26 18:15:59	SMS from +525585292665: El numero 5535606234 le ha enviado un mensaje de texto que no se recibio. Entre a **http://iusacell-movil[.]com[.]mx/6731340s/** para ver el sms
2015-04-12 22:41:24	SMS from +525525715066: Notificacion de compra con tarjeta **** monto $3,500.00 M.N, ver detalles en: **http://smsmensaje[.]mx/1493024s/**
2015-05-08 19:49:23	SMS from +525525715066: Aviso de vencimiento de pago asociado a tu servicio con cargo a tu tarjeta ****, ver mas detalles: **http://smsmensaje[.]mx/6445761s/**
2015-05-08 23:19:14	SMS from +525585292665: El siguiente mensaje esta marcado como urgente y no se recibio correctamente, recuperalo en .. **http://smsmensaje[.]mx/3863925s/**

2015-05-09 01:24:29	SMS from +525525715066: Haz realizado un Retiro/Compra en tienda departamental **** monto $2,500.00 M.N, ver detalles **http://smsmensaje[.]mx/9936510s/**
2015-05-09 02:42:26	SMS from +525585292665: Haz realizado un Retiro/Compra en tienda departamental **** monto $2,500.00 M.N, ver detalles **http://smsmensaje[.]mx/1796758s/**
2015-05-10 00:09:55	SMS from +525585292665: UNOTV[.]com/ AUDI ENTRE LOS PRINCIPALES AUTOS CON PROBLEMAS EN LA TRANSMICION VERIFICA LA LISTA DE ELLOS: **http://unonoticias[.]net/1291412s/**
2015-05-11 20:19:20	SMS from +525585292665: El siguiente mensaje esta marcado como urgente y no se recibio correctamente, recuperalo en .. **http://smsmensaje[.]mx/6713776s/**
2015-05-12 02:05:06	SMS from +525585292665: El siguiente mensaje esta marcado como urgente y no se recibio correctamente, recuperalo en .. **http://smsmensaje[.]mx/6318147s/**
2015-05-12 04:03:33	SMS from +525525715066: Estimado cliente informamos que presentas un problema de pago asociado a tu servicio, ver detalles.. **http://smsmensaje[.]mx/8884678s/**
2015-05-12 22:42:53	SMS from +525585292665: Alcanzaste la tarifa premium de IUSACELL $0.30 Min a Celular y $0.10 Nacional, codigo 2207 y activalo ya… **http://smsmensaje[.]mx/3432773s/**
2015-05-14 00:37:27	SMS from +525585292665: Alcanzaste la tarifa premium de IUSACELL $0.30 Min a Celular y $0.10 Nacional, codigo 2207 activalo ya… **http://smsmensaje[.]mx/7534402s/**
2015-05-14 02:55:35	SMS from +525525715066: UNONOTICIAS. En encuesta revelan las 3 posiciones sexuales favoritas de las mujeres, ver nota en: **http://unonoticias[.]net/6218095s/**
2015-05-14 03:24:41	SMS from +525585292665: Retiro/Compra en tienda departamental $4,000.00 M.N 13/05/2015 20:10 hrs ,ver detalles en: **http://smsmensaje[.]mx/9550014s/**
2015-05-14 19:56:23	SMS from +525585292665: El numero +525541337879 le ha mandado un mensaje de texto que ser ecibio incompleto. Ver mensaje en: **http://smsmensaje[.]mx/5670989s/**
2015-05-15 01:18:30	SMS from +525585292665: UNOTV. Detectan irregularidades en caso Aristegui, ver nota completa.. **http://unonoticias[.]net/4347580s/**
2015-06-05 01:56:27	SMS from +525585292665: UNOTV. Que depara el futuro para MVS y cual es el camino de Carmen Aristegui? ver nota completa.. **http://unonoticias[.]net/9275690s/**

2015-07-26 03:05:05	SMS from +525585292665: TELCEL[.]com/ RECIBISTE CORRECTAMENTE TU FACTURA ELECTRONICA VERIFICA DETALLES DE TU COMPRA: **http://ideas-telcel.com[.]mx/9872742s/**
2015-07-26 12:34:59	SMS from +525525715066: has realizado un Retiro/Compra Tarjeta**** M.N monto $3,500.00 verifica detalles de operacion: **http://smsmensaje[.]mx/6156234s/**
2015-07-26 15:23:35	SMS from +525525715066: UNOTV.com/ ANONYMUS ANUNCIA QUE ATACARA PAGINA DE ARISTEGUI VER DETALLES: **http://unonoticias[.]net/9250302s/**
2015-08-20 19:20:46	SMS from +525525715066: IUSACELL/ Estimado cliente su factura esta lista, agradeceremos pago puntual por $17401.25 Detalles: **http://iusacell-movil[.]com[.]mx/8595070s/**
2015-08-20 19:34:05	SMS from +525525715066: USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA POR FAVOR ACUDE PRONTAMENTE A LA EMBAJADA. VER DETALLES: **http://bit[.]ly/1MAAWrO (http://smsmensaje[.]mx/9439115s/)**
2015-08-23 04:58:47	SMS from +525525715066: IUSACELL.com/ EL SIGUIENTE MENSAJE ESTA MARCADO COMO URGENTE REVISALO DESDE NUESTRO PORTAL VER **http://iusacell-movil[.]com[.]mx/7918310s/**
2015-08-24 03:03:48	SMS from +525585292665: UNOTV[.]com/ FAMILIA DE CHAPO SE REFUGIA EN GRANDES RESIDENCIAS EN DF ENTRE ELLAS SN JERONIMO VER DONDE: **http://unonoticias[.]net/6353793s/**
2015-08-24 15:31:38	SMS from +525525715066: ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR A NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA SAN JERONIMO. DETALLES: **http://bit[.]ly/1EQYOkG (http://mymensaje-sms[.]com/6649365s/)**
2015-08-24 15:31:59	SMS from +525585292665: ALERTA AMBER DF/ COOPERACION PARA LOCALIZAR A NINO DE 9 ANOS, DESAPARECIDO EN LA COLONIA SAN JERONIMO. DETALLES: **http://bit[.]ly/1EQYSB1 (http://mymensaje-sms[.]com/5186565s/)**
2015-09-02 18:43:23	SMS from +525585292665: Hola Carmen, solo para desearte una excelente tarde y compartirte la nota que publica proceso sobre el 3er informe: **http://bit[.]ly/1JNTfox (http://twiitter[.]com.mx/8527373s/)**
2015-09-05 15:39:41	SMS from +525585292665: IUSACELL[.]com / DESCUBRE LA NUEVA TELEFONIA Y CONOCE LAS APLICACIONES MAS SEGURAS PARA TU SMARTPHONE SEGUN EL PENTAGONO **http://bit[.]ly/1IQhzFw (http://iusacell-movil[.]com.mx/5726967s/)**
2015-09-25 18:47:50	SMS from +525585292665: Queridisima Carmen en la madrugada fallecio mi padre, estamos muy devastados. Mando datos del funeral ojala puedas ir: **http://bit[.]ly/1KDGbSR (http://smsmensaje[.]mx/4966295s/)**
2015-10-17 18:12:07	SMS from +525585292665: chatita como estas, espero que bien este mi numero nuevo checa esta noticia la subi a drive checala para borrarla urge **http://tinyurl[.]com/pfwmr88 (https://googleplay-store[.]com/7863372s/)**

2015-10-25 23:39:29	SMS from +525525715066: Hola te envio invitacion electronica con detalles por motivo de mi fiesta de disfraces espero contar contigo alonso: **http://tinyurl[.]com/o2tq8rl (https://smsmensaje[.]mx/8623600s/)**
2016-02-09 17:46:42	SMS from +525552899427: Carmen hace 5 dias que no aparece mi hija te agradecere mucho que compartas su foto, estamos desesperados: **http://bit[.]ly/1KDekJ9 (https://smsmensaje[.]mx/5957475s/)**
2016-02-10 23:10:59	SMS from +525552899427: Querida Carmen fallecio mi hermano en un accidente, estoy devastada, envio datos del velorio, espero asistas: **http://bit[.]ly/1TTjm6D (https://smsmensaje[.]mx/6056487s)**
2016-02-11 22:30:48	SMS from +525568850176: Hace 7 dias desaparecio mi hija de 8 a?os en ecatepec, por favor ayudame a compartir su foto, estamos desesperados: **https://smsmensaje[.]mx/7430255t/**
2016-02-11 22:32:15	SMS from +525568850176: Hace 7 dias desaparecio mi hija de 8 a?os en ecatepec, por favor ayudame a compartir su foto, estamos desesperados: **https://smsmensaje[.]mx/7430255t/**
2016-02-11 23:58:10	SMS from +525568850176: Perdon en el sms anterior no se veia la foto, la reenvio, por favor compartela queremos a nuestra ni?a de vuelta: **https://smsmensaje[.]mx/7430255t/**
2016-02-15 04:02:23	SMS from +525547311580: Vinieron unas personas a extorsionarnos si no les dabamos 100mil pesos saben quienes somos tome fotos mira **https://fb-accounts[.]com/1324052s/**
2016-02-24 15:45:04	SMS from +525552899427: UNOTV[.]com/ LANZA TELEVISA DESPLEGADOS EN TODOS SUS MEDIOS;CRITICA POSTURA DE ORGANIZACION ARTICULO 19. VER: **http://bit[.]ly/1SU5N7q (https://unonoticias[.]net/6809853s/)**
2016-02-25 15:27:59	SMS from +525552899427: has realizado un Retiro/Compra Tarjeta**** M.N monto $3,500.00 verifica detalles de operacion: **http://bit[.]ly/21jxVFW (https://unonoticias[.]net/2250072s/)**
2016-03-10 16:09:38	SMS from +529993190183: ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MAS IMPORTANTES: **http://bit[.]ly/225VXRR (https://smsmensaje[.]mx/8807734s/)**
2016-03-11 16:19:14	SMS from +529993190183: ARISTEGUI NOTICIAS ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA RESUMEN DE LAS NOTICIAS MAS IMPORTANTES: **https://smsmensaje[.]mx/4701759s/**
2016-04-05 14:42:23	SMS from +528120754135: ARISTEGUINOTICIASONLINE[.]mx ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: **http://bit[.]ly/1q3n16a (https://smsmensaje[.]mx/7974159s/)**
2016-04-07 20:54:12	SMS from +528120953203: ARISTEGUINOTICIASONLINE[.]mx ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: **https://smsmensaje[.]mx/1119786s/**

2016-04-12 21:42:40	SMS from +528120943682: ARISTEGUINOTICIASONLINE[.]mx ESTRENA SERVICIO DE SMS. SUSCRIBASE Y RECIBIRA LAS NOTICIAS MAS IMPORTANTES: **https://smsmensaje[.]mx/2365691s/**
2016-05-11 18:30:07	SMS from +525585401284: UNOTV[.]com/ CONFIRMA PGR QUE HIJO MAYOR DE AMLO LLEVA 48 HRS DESAPARECIDO. DETALLES: **http://bit[.]ly/1QYVKaM (https://unonoticias[.]net/5911276s/)**
2016-05-13 15:19:47	SMS from +528120531318: Perdon x molestarte pero hace 3 dias que no aparece mi hija te agradecere que me ayudes a compartir su foto: **http://bit[.]ly/1Oo7cSS (https://smsmensaje[.]mx/8984621s/)**
2016-06-03 18:03:24	SMS from +525585401299: Carmen la pagina esta intermitente, esta apareciendo este error al intentar ingresar: **http://bit[.]ly/1WzrZ8T (https://smsmensaje[.]mx/9371877s/)**
2016-06-09 19:19:10	SMS from +528120990524: Eres mierda porque yo me ando cojiendo a tu pareja mientras tu pendejeas y de prueba te mando esta foto: **http://bit[.]ly/1rfaNHR (https://smsmensaje[.]mx/9449190s/)**
2016-06-13 17:38:35	SMS from +525585401299: Hace 3 dias que no aparece mi hija, estamos desesperados, te agradecere que me ayudes a compartir su foto: **http://bit[.]ly/235giae (https://smsmensaje[.]mx/1239663s/)**
2016-06-15 21:21:29	SMS from +528122090316: Buenas tardes Carmen, unicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: **http://bit[.]ly/1twXSDl (https://smsmensaje[.]mx/1911343s/)**
2016-06-22 21:35:59	SMS from +529993190053: UNOTV[.]com/ REVELAN VIDEO DONDE CRISTIANO RONALDO SE ENFADA Y AVIENTA MICROFONO DE REPORTERO. VIDEO EN: **https://unonoticias[.]net/2068822s/**
2016-06-28 21:32:09	SMS from +528120696998: UNOTV[.]com/ ATENTADO TERRORISTA EN ESTAMBUL DEJA 30 MUERTOS/SECUESTRAN REPORTERO DE TELEVISA/FALLECE CHACHITA **http://bit[.]ly/295RNq7 (https://smsmensaje[.]mx/1656017s/)**
2016-07-01 16:45:44	SMS from +528122090348: UNOTV[.]com/ CARMEN ARISTEGUI YA FIRMO CONTRATO PARA REGRESAR A LA RADIO. DETALLES: **https://unonoticias[.]net/3423165s/**
2016-07-04 20:32:34	SMS from +528121050415: UNOTV[.]com/ AMARILLISMO DE ARISTEGUI VS REALIDAD/ VAN 30 DETENIDOS EN ATENTADO DE ESTAMBUL/ CHILE CAMPEON **http://bit[.]ly/29eWzzv (https://unonoticias[.]net/9436744s/)**
2016-07-05 18:42:59	SMS from +525536438524: **https://fb-accounts[.]com/2102272t/**
2016-07-06 21:56:08	SMS from +528122090257: Hace 5 dias q no aparece mi hija te agradecere mucho q compartan su foto, estamos destrozados es un infierno: **http://bit[.]ly/29rnk6c (https://smsmensaje[.]mx/7960742s/)**

2016-07-12 21:20:25	SMS from +528120697015: UNOTV[.]com/ FILMAN A REPORTERO Y PERIODISTA CUANDO SON LEVANTADOS POR COMANDO ARMADO EN TAMAULIPAS. VIDEO: **https://unonoticias[.]net/1887451s/**
2016-07-14 20:29:40	SMS from +528122090358: ESTIMADO USUARIO ha realizado un Retiro/Compra Tarjeta M.N de ****** el 14/07/16 10:52:00 AM. Ver DETALLES: **https://banca-movil[.]com/4982255s/**
2016-07-15 23:56:16	SMS from **+528122090286**: Mi rey te mando mis fotos encueradita y abiertita asi como te gusta, las ves y las borras eh: **http://bit[.]ly/29lQvyh (https://smsmensaje[.]mx/3376811s/)**
2016-07-18 17:50:57	SMS from +523319983437: Hola oye abriste nuevo facebook? Me llego una solicitud de un face con tus fotos pero con otro nombre mira: **https://fb-accounts[.]com/1607422s/**
2016-07-19 17:55:54	SMS from +528113788852: Hola buen martes. Oye que pedo con el puto Lopez Doriga? Mira lo que escribio sobre ti hoy, urge desmentirlo: **http://bit[.]ly/29LfZfD (https://smsmensaje[.]mx/9093723s/)**
2016-07-22 21:33:26	SMS from **+525576169290**: Estimado cliente Unefon te informa su saldo vencido al de la llnea 5539290869, es por $4,278. DETALLES: **https://ideas-telcel[.]com[.]mx/4729605s/**
2016-07-23 17:51:28	SMS from **+525576169290**: Amigo,hay una pseudo cuenta de fb y twitter identica a la tuya checala para que la denuncies mira checala: **https://fb-accounts[.]com/9543697s/**
2016-07-25 21:01:24	SMS from **+528122090359**: Bienvenido Club CHICAS CALIENTES, se ha aplicado un cargo de $875.85 a su linea, si desea cancelar ingrese a: **http://bit[.]ly/2a0hZ2l (https://smsmensaje[.]mx/6881768s/)**
2016-07-28 22:47:46	SMS from **+528120990542**: UNOTV[.]com/ VIRAL EL VIDEO DE FUERTE GOLPE QUE RECIBE EN LA CARA OSORIO CHONG PROPINADO POR MAESTRO. VIDEO: **https://unonoticias[.]net/6328951s/**

Forensic traces for MXJRN3

No timestamps are available as these SMS messages where found in previous screenshots.

Date (UTC)	Event
	SMS from **+523332078807**: Buenas noches Sandra, unicamente paso a saludarte y enviarte esta nota de Proceso que es importante retomar: **http://bit[.]ly/25JHLDm (https://smsmensaje[.]mx/5727775s/)**
	SMS from **+525546613611**: Sandra amiga acaba de morir mi esposo, estamos devastadas, te envio los datos del velatorio espero asistas: **http://bit[.]ly/28hMScw (https://smsmensaje[.]mx/6050864s/)**
	SMS from **+524446613611**: Hace 3 dias quo no aparence mi hija, estamos desesperados, te agradecere que me ayudes a compartit su foto: **http://bit[.]ly/235hzhv (https://smsmensaje[.]mx/4159043s/)**

SMS from **+518122090332**: Sandra, mi mama esta muy grave, tal vez no pase la noche te envio datos de donde esta internada ojala vengas: **http://bit[.]ly/1PQsLvX (https://smsmensaje[.]mx/6395084s/)**

Forensic traces for MXJRN4

This Pegasus attack message was original discovered and published as part of collaborative investigation between Citizen Lab, R3D, SocialTic and Article 19.

Date (UTC)	Event
2016-05-12 19:06:04	SMS from + 528112889362: Tengo pruebas clave y fidedignas en contra de servidores publicos, ayudame tiene que ver con este asunto **http://bit[.]ly/1s2eguc (https://secure-access10[.]mx/2618844s/)**

Forensic traces for RWHRD1 – Carine Kanimba

Date (UTC)	Event
2020-11-24 13:26:03	Process record deleted from ZPROCESS (IN: 12.86 MB, OUT: 168.99 MB)
2021-01-28 22:42:56	Process: **Diagnosticd**
2021-01-31 18:28:39	Process: **dhcp4d**
2021-01-31 23:59:02	Process: **libtouchregd**
2021-02-02 13:54:23	Process: **MobileSMSd**
2021-02-13 19:44:12	Process: **vm_stats**
2021-02-21 23:10:09	Process: **launchrexd**
2021-02-21 23:10:09	Process: **mptbd**
2021-02-22 15:39:00	Process: **PDPDialogs**
2021-03-16 13:33:22	Process: **neagentd**
2021-03-17 15:27:06	Process: **CommsCenterRootHelper**
2021-03-21 06:06:45	Process: **roleaboutd**
2021-03-23 17:37:31	Process: **contextstoremgrd**
2021-03-28 00:36:43	Process: **otpgrefd**

2021-03-31 13:57:01	Process: **vm_stats**
2021-04-06 21:29:56	Process: **locserviced**
2021-04-09 19:09:18	Process: **bluetoothfs**
2021-04-23 01:48:56	Process: **eventfssd**
2021-04-23 20:43:14	Process: **com.apple.Mappit.SnapshotService**
2021-04-23 23:01:44	Process: **aggregatenotd**
2021-04-24 22:01:47	Process: **ReminderIntentsUIExtension**
2021-04-24 22:01:54	Process: **ReminderIntentsUIExtension**
2021-04-28 13:34:53	Process: **com.apple.rapports.events**
2021-04-28 13:34:57	Process: **com.apple.rapports.events** (IN: 0.01 MB, OUT: 0.00 MB)
2021-04-28 13:34:57	Process: **com.apple.rapports.events**
2021-04-28 13:35:40	Process: **com.apple.rapports.events**
2021-04-28 16:08:40	Process: **xpccfd**
2021-05-03 08:07:38	Traces from zero-click attack attempt over iMessage
2021-05-08 07:28:40	Traces from zero-click attack attempt over iMessage
2021-05-16 12:30:10	Traces from zero-click attack attempt over iMessage
2021-05-17 13:39:16	iMessage lookup for account **benjiburns8[@]gmail.com**
2021-05-17 13:40:12	Traces from zero-click attack attempt over iMessage
2021-06-14 00:06:00	Attack related push notifications over iMessage
2021-06-14 00:09:33	Process crash detected
2021-06-14 00:12:57	Process: **com.apple.rapports.events**
2021-06-14 00:17:12	Process: **faskeepd**
2021-06-14 00:17:12	Process: **lobbrogd**

2021-06-14 00:17:12	Process: **neagentd**
2021-06-14 00:17:12	Process: **com.apple.rapports.events**
2021-06-14 17:38:44	Process: **faskeepd**
2021-06-14 17:38:44	Process: **lobbrogd**
2021-06-14 17:38:44	Process: **neagentd**
2021-06-14 17:39:59	Process: **faskeepd**
2021-06-14 17:39:59	Process: **lobbrogd**
2021-06-14 17:39:59	Process: **neagentd**
2021-06-15 18:26:22	Process: **faskeepd**
2021-06-15 18:26:22	Process: **lobbrogd**
2021-06-15 18:26:22	Process: **neagentd**
2021-06-15 18:28:16	Process: **faskeepd**
2021-06-15 18:28:16	Process: **lobbrogd**
2021-06-15 18:28:16	Process: **neagentd**
2021-06-15 18:30:12	Process: **faskeepd**
2021-06-15 18:30:12	Process: **lobbrogd**
2021-06-15 18:30:12	Process: **neagentd**
2021-06-16 00:04:37	Process: **faskeepd**
2021-06-16 00:04:37	Process: **lobbrogd**
2021-06-16 00:04:37	Process: **neagentd**
2021-06-16 18:49:50	Process: **faskeepd**
2021-06-16 18:49:50	Process: **lobbrogd**
2021-06-16 18:49:50	Process: **neagentd**

2021-06-16 21:54:15	Process: **faskeepd**
2021-06-16 21:54:15	Process: **lobbrogd**
2021-06-16 21:54:15	Process: **neagentd**
2021-06-18 08:13:35	Process: **faskeepd**
2021-06-18 15:21:00	Attack related push notifications over iMessage
2021-06-18 15:26:04	Process crash detected
2021-06-18 15:26:08	Process: **com.apple.Mappit.SnapshotService**
2021-06-18 15:26:16	Process: **com.apple.Mappit.SnapshotService**
2021-06-18 15:31:12	Process: **launchrexd**
2021-06-18 15:31:12	Process: **frtipd**
2021-06-18 15:31:12	Process: **ReminderIntentsUIExtension**
2021-06-19 16:00:16	Process: **launchrexd**
2021-06-19 16:00:16	Process: **frtipd**
2021-06-19 16:00:16	Process: **ReminderIntentsUIExtension**
2021-06-20 00:06:25	Process: **launchrexd**
2021-06-20 00:06:25	Process: **frtipd**
2021-06-20 00:06:25	Process: **ReminderIntentsUIExtension**
2021-06-20 19:52:25	Process: **launchrexd**
2021-06-20 19:52:25	Process: **frtipd**
2021-06-20 19:52:26	Process: **ReminderIntentsUIExtension**
2021-06-20 19:53:58	Process: **launchrexd**
2021-06-20 19:53:58	Process: **frtipd**
2021-06-20 19:53:58	Process: **ReminderIntentsUIExtension**

2021-06-22 03:57:10	Process: **launchrexd**
2021-06-22 03:57:10	Process: **frtipd**
2021-06-22 03:57:10	Process: **ReminderIntentsUIExtension**
2021-06-22 04:06:51	Process: **launchrexd**
2021-06-22 04:06:51	Process: **frtipd**
2021-06-22 04:06:51	Process: **ReminderIntentsUIExtension**
2021-06-23 00:01:02	Process: **launchrexd**
2021-06-23 00:01:02	Process: **frtipd**
2021-06-23 00:01:02	Process: **ReminderIntentsUIExtension**
2021-06-23 14:31:39	Process: **launchrexd**
2021-06-23 20:46:00	Attack related push notifications over iMessage
2021-06-23 20:48:56	Process crash detected
2021-06-23 20:54:16	Process crash detected
2021-06-23 20:55:10	Process: **otpgrefd**
2021-06-23 20:59:35	Process: **otpgrefd**
2021-06-23 20:59:35	Process: **launchafd**
2021-06-23 20:59:35	Process: **vm_stats**
2021-06-23 22:21:13	Attack artifact on disk: /private/var/tmp/vditcfwheovjf/cc/**otpgrefd**/
2021-06-24 12:16:22	Process: **otpgrefd**
2021-06-24 12:16:22	Process: **launchafd**
2021-06-24 12:16:22	Process: **vm_stats**
2021-06-24 12:24:29	Process: **otpgrefd**
2021-06-26 21:56:00	Attack related push notifications over iMessage

2021-06-26 23:25:32	Process: **smmsgingd**
2021-06-29 22:26:00	Attack related push notifications over iMessage
2021-06-29 22:30:46	Process crash detected
2021-06-29 22:36:01	Process: **launchafd**
2021-06-29 22:36:01	Process: **otpgrefd**
2021-06-29 22:36:01	Process: **dhcp4d**
2021-06-29 22:36:01	Process: **ctrlfs**
2021-06-30 00:09:19	Process: **launchafd**
2021-06-30 00:09:19	Process: **otpgrefd**
2021-06-30 00:09:19	Process: **dhcp4d**
2021-07-01 00:09:32	Process: **launchafd**
2021-07-01 00:09:32	Process: **otpgrefd**
2021-07-01 00:09:32	Process: **dhcp4d**
2021-07-01 12:16:43	Process: **launchafd**
2021-07-01 12:16:43	Process: **otpgrefd**
2021-07-01 12:16:43	Process: **dhcp4d**
2021-07-01 21:42:19	Process: **launchafd**
2021-07-03 06:06:37	iMessage lookup for account **benjiburns8[@]gmail.com**
2021-07-03 06:07:00	Attack related push notifications over iMessage
2021-07-03 06:22:16	Process crash detected
2021-07-03 06:32:56	Process: **actmanaged**
2021-07-03 06:32:56	Process: **misbrigd**
2021-07-03 06:32:56	Process: **Diagnostics-2543**

2021-07-03 06:32:56	Process: **gssdp**
2021-07-03 15:23:18	Process: **actmanaged**

Topics

- Research
- Blog