RSF REPORTERS WITHOUT BORDERS GERMANY

Investigation Report

16th of January, 2024

Viktor Schlüter, Janik Besendorf

Contents

1 Preface

The Digital Security lab was provided data from Loïc Lawson's iPhone. An analysis was performed on the 18th of December 2023, consisting of automated and manual analysis steps.

2 Analysis of Loïc Lawson's iPhone

2.1 Analysis Results

Our analysis identified the execution of several processes that can be tied to the Pegasus spyware by NSO Group. The phone was initially infected on the 1st of Februar in 2021. After that 23 signs of reinfection could be identified. The initial infection indicator was observed in past cases of the RSF Digital Security Lab and has been confirmed by its technical partners to be connected to Pegasus Infections, including Amnesty Tech's Security Lab. The indicators for reinfections are publicly known indicators of Pegasus infections.

2.2 Proof of Execution of Pegasus Processes

23 malicious processes were executed in a suspicious folder on Loïc Lawson's device over the span of five months. No legitimate processes under that name exist in either current or past versions of iOS. The com.apple.xpc.roleaccountd.staging folder being used by Pegasus is consistent with previous analysis by Citizenlab and Amnesty Tech.

All of the process names below, with the exception of "stagegrad" are in the list of Pegasus Indicators published by Amnesty Tech. This is an additional indicator that the phone was compromised by Pegasus.

The execution of the processes show the times when the attacker renewed the infection. They range from February 2021 to July 2021, establishing a time frame during which the phone was infected periodically by Pegasus spyware.

Time	Process Path
2021-07-10 12:19:00.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/bundpwrd
2021-06-27 22:34:14.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/faskeepd

Time	Process Path
2021-06-23 11:19:48.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/launchafd
2021-06-20 20:23:40.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/eventstorpd
2021-06-04 15:10:20.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/corecomnetd
2021-05-27 11:15:08.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/actmanaged
2021-05-18 14:33:07.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/corecomnetd
2021-05-07 12:38:08.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/brfstagingd
2021-04-24 20:02:01.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/brstaged
2021-04-17 18:14:12.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/keybrd
2021-04-14 08:10:54.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/faskeepd
2021-04-10 13:39:59.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/launchafd
2021-04-07 15:34:13.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/accountpfd
2021-03-26 12:44:03.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/launchrexd
2021-03-19 17:31:55.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/llmdwatchd
2021-03-11 10:28:34.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/eventfssd
2021-03-06 13:40:54.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/boardframed

Time	Process Path
2021-03-03 13:50:39.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/eventstorpd
2021-02-26 15:01:02.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/aggregatenotd
2021-02-19 03:30:29.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/xpccfd
2021-02-15 18:40:13.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/lobbrogd
2021-02-13 18:18:29.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/natgd
2021-02-08 02:25:37.000000	/private/var/db/com.apple.xpc.roleaccountd.staging/stagegrad

3 Analysis of Anani Sossou's iPhone

3.1 Analysis Results

Our analysis identified the execution of several processes that can be tied to the Pegasus spyware by NSO Group. The phone was initially infected on the 10th of October in 2021. After that two signs of reinfection could be identified. The initial infection indicator was observed in past cases of the RSF Digital Security Lab and has been confirmed by its technical partners to be connected to Pegasus Infections, including Amnesty Tech's Security Lab.

The processes in this case were also located under `/private/var/db/com.apple.xpc.roleaccountd.staging/`, which is the same folder where the processes from Loïc Lawson's phone were located. They were executed on 2021-10-27 05:27:47 and 2021-11-04 00:15:41.