Date: 17 December, 2021
Memo: The targeting of Roman Giertych with Pegasus spyware
Prepared by: The Citizen Lab
Prepared for: Roman Giertych

This memorandum is prepared for Roman Giertych at his request and with his consent. It confirms that our forensic analysis of digital artifacts from Roman Giertych's Apple device ("Roman Giertych's device")[1] indicates that a phone in his possession was infected with Pegasus spyware, which is made by NSO Group.

Background

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

The Citizen Lab's research mandate includes tracking digital threats against civil society actors, as well as tracking the proliferation of the mercenary spyware industry. As part of the Citizen Lab's investigations into the mercenary spyware industry, the Citizen Lab has developed the ability to identify evidence of device compromise with Pegasus spyware.

Confirming the infection of Roman Giertych with NSO Group's Pegasus spyware

Citizen Lab researchers analyzed forensic artifacts from Roman Giertych's device and obtained a positive result for Pegasus spyware. Close inspection indicated that Roman Giertych's device had been restored from a previous iPhone. The restore process carried over high confidence indicators that the previous iPhone was repeatedly infected with NSO Group's

[1] The device has serial number FK1ZPM08N70X.

Pegasus spyware. Mr Giertych advises us that the reason for the change of phones was that the prior device ceased functioning normally, and is currently non-functional.

Evidence showed that the old phone he had was infected with Pegasus spyware during the following approximate time periods:

1. On or around **2019-09-05**
2. On or around **2019-09-11**
3. On or around **2019-09-12**
4. On or around **2019-09-13**
5. On or around **2019-09-16**
6. On or around **2019-09-22**
7. On or around **2019-09-23**
8. On or around **2019-09-24**
9. On or around **2019-09-25**
10. On or around **2019-09-29**
11. On or around **2019-09-30**
12. On or around **2019-10-01**
13. On or around **2019-10-04**
14. On or around **2019-10-21**
15. On or around **2019-10-22**
16. On or around **2019-11-18**
17. On or around **2019-11-22**
18. On or around **2019-12-04**

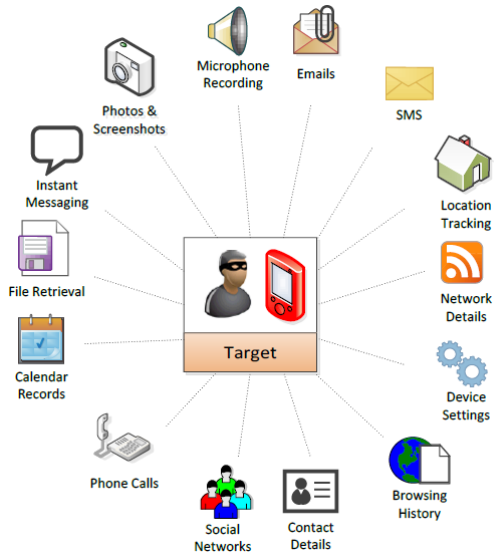
This does not preclude the possibility of other infections.

What a successful infection with Pegasus spyware can do

Pegasus is a surveillance tool that provides its operator complete access to a target's mobile device. Pegasus allows the operator to extract passwords, files, photos, web history, contacts, as well as identity data (such as information about the mobile device).

Pegasus can take screen captures, and monitor user inputs, as well as activating a telephone's microphone and camera. This enables attackers to monitor all activity on the device and in the vicinity of the device, such as conversations conducted in a room.

Pegasus also allows the operator to record chat messages as they are sent and received (including messages sent through "encrypted" / disappearing-message-enabled texting apps like WhatsApp or Telegram), as well as phone and VoIP calls (including calls through "encrypted" calling apps).



NSO marketing material showing some of what Pegasus can monitor on a target's device.
Source: NSO Marketing Materials

For some chat programs, Pegasus also supports the extraction of past message logs. Pegasus also allows the operator to track the target's location. As with any infection, spyware may also allow for the modification or manipulation of data on a device.

More information about NSO Group and its Pegasus spyware

Pegasus spyware is sold and marketed by NSO Group (which goes by the name Q Cyber Technologies, as well as other names). NSO Group is an Israeli-based company which develops and sells spyware technology, including Pegasus.[2] NSO Group is majority-owned by Novalpina Capital, a European private equity firm based in London.[3]

NSO Group claims it sells its spyware strictly to government clients only and that all of its exports are undertaken in accordance with Israeli government export laws and oversight mechanisms. NSO Group also claims to abide by a human rights policy. However, the number of documented cases in which their technology is used abusively to target civil society continues to grow.

You can review Citizen Lab research into NSO Group at this website: https://citizenlab.ca/tag/nso-group/

[2] Note that in specific transactions for this technology, the Pegasus spyware may be given other codenames.
[3] For more information on NSO Group, you can find a summary of key public reporting here. Further, exhibits filed in the ongoing litigation between WhatsApp/Facebook and NSO Group in the United States provide insight into Pegasus' functions and NSO Group's operations (see, in particular, Exhibit 10 of the complaint).