Date: 14 November, 2022
Memo: The targeting of Jatupat Boonpattararaksa with Pegasus spyware
Prepared by: The Citizen Lab
Prepared for: Jatupat Boonpattararaksa

This memorandum is prepared for Jatupat Boonpattararaksa at his request and with his consent. It confirms that our forensic analysis of digital artifacts on Jatupat Boonpattararaksa's Apple device ("Jatupat Boonpattararaksa's device")[1] indicates that a device belonging to Jatupat Boonpattararaksa was compromised with Pegasus spyware. Pegasus spyware 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 Jatupat Boonpattararaksa with NSO Group's Pegasus spyware

Citizen Lab researchers analyzed forensic artifacts from Jatupat Boonpattararaksa's device and obtained a positive result, which indicates it was targeted and infected with NSO Group's Pegasus spyware. Our analysis indicates that a device belonging to Jatupat Boonpattararaksa was infected with Pegasus spyware in the following approximate time periods:

[1] The device with serial number G6TXQMXXXXXX.

1. On or around **2021-06-23**
2. On or around **2021-06-28**
3. On or around **2021-07-09**

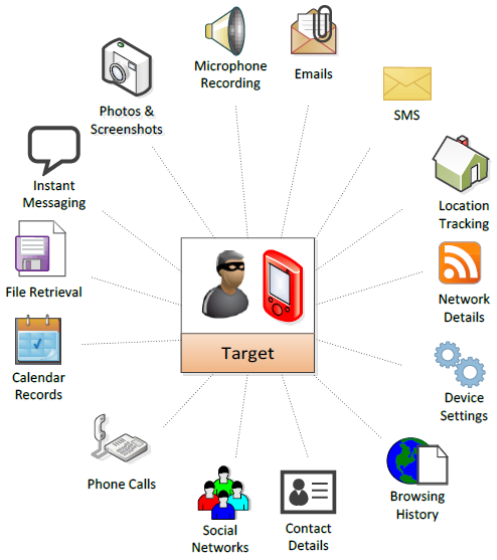
This does not preclude the possibility of other infections.

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.

Additionally, Pegasus spyware may be used to steal tokens allowing for persistent access to popular cloud accounts.

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).

วันที่: 14 พฤศจิกายน 2565
บันทึก: การโจมตี จตุภัทร์ บุญภัทรรักษา ด้วยสปายแวร์เพกาซัส
จัดเตรียมโดย: ซิติเซ็นแล็บ
จัดเตรียมเพื่อ: จตุภัทร์ บุญภัทรรักษา

บันทึกฉบับนี้จัดทำขึ้นเพื่อ จตุภัทร์ บุญภัทรรักษาตามความประสงค์และด้วยความยินยอมของเขา เป็นการยืนยันผลการวิเคราะห์เชิงนิติวิทยาศาสตร์ของพยานหลักฐานทางดิจิทัลในอุปกรณ์ยี่ห้อแอปเปิ้ลของ จตุภัทร์ บุญภัทรรักษา ("อุปกรณ์ของ จตุภัทร์ บุญภัทรรักษา")[1] ซึ่งพบว่าได้ถูกเจาะระบบโดยสปายแวร์เพกาซัส สปายแวร์เพกาซัสเป็นผลิตภัณฑ์ของเอ็นเอสโอกรุ๊ป

ข้อมูลพื้นฐาน

ซิติเซ็นแล็บเป็นห้องปฏิบัติการสหวิชาชีพตั้งอยู่ที่ Munk School of Global Affairs & Public Policy, มหาวิทยาลัยโตรอนโต เน้นการวิจัย การพัฒนา และการมีส่วนร่วมในนโยบายเชิงยุทธศาสตร์และกฎหมายระดับสูง ซึ่งเป็นจุดเชื่อมต่อระหว่างเทคโนโลยีสารสนเทศและการสื่อสาร สิทธิมนุษยชนและความมั่นคงระดับโลก

อำนาจหน้าที่ด้านงานวิจัยของซิติเซ็นแล็บ ครอบคลุมถึงการติดตามข้อมูลภัยคุกคามเชิงดิจิทัลที่มีต่อหน่วยงานภาคประชาสังคม รวมทั้งการติดตามข้อมูลการขยายตัวของอุตสาหกรรมสปายแวร์เชิงพาณิชย์ จากการดำเนินงานของซิติเซ็นแล็บเพื่อสอบสวนอุตสาหกรรมสปายแวร์เชิงพาณิชย์ ซิติเซ็นแล็บได้พัฒนาความสามารถในการจำแนกหลักฐานที่ยืนยันว่าอุปกรณ์ได้ถูกเจาะระบบด้วยสปายแวร์เพกาซัส

ยืนยันการติดสปายแวร์เพกาซัสของเอ็นเอสโอกรุ๊ปในอุปกรณ์ของ จตุภัทร์ บุญภัทรรักษา

นักวิจัยของซิติเซ็นแล็บได้วิเคราะห์พยานหลักฐานทางดิจิทัลจากอุปกรณ์ของ จตุภัทร์ บุญภัทรรักษาและพบว่ามีผลในเชิงบวก ซึ่งหมายถึงว่าอุปกรณ์นี้ได้ถูกโจมตีและติดสปายแวร์เพกาซัสของเอ็นเอสโอกรุ๊ป การวิเคราะห์ของเราชี้ว่า โทรศัพท์เครื่องนี้ได้ติดสปายแวร์เพกาซัสในช่วงเวลาต่อไปนี้โดยประมาณ

1. ในวันที่หรือช่วงวันที่ **2564-06-23**
2. ในวันที่หรือช่วงวันที่ **2564-06-28**
3. ในวันที่หรือช่วงวันที่ **2564-07-09**

[1] อุปกรณ์ชิ้นนี้มีเลขซีเรียลนัมเบอร์คือ G6TXQMXXXXXX.

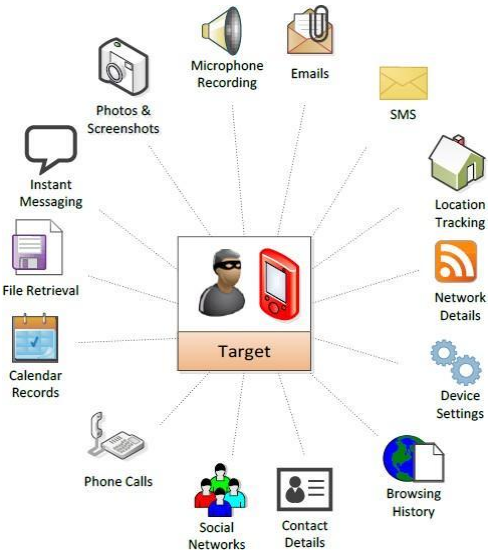
ทั้งนี้อาจมีความเสี่ยงที่จะมีการติดสปายแวร์ในช่วงเวลาอื่น

การติดสปายแวร์เพกาซัสส่งผลกระทบอย่างไรบ้าง

เพกาซัสเป็นเครื่องมือสอดแนมข้อมูล ทำให้ผู้ควบคุมสามารถเข้าถึงอุปกรณ์มือถือที่เป็นเป้าหมายได้อย่างเบ็ดเสร็จ เพกาซัสอนุญาตให้ผู้ควบคุมสามารถเข้าถึงพาสเวิร์ด, ไฟล์, รูปภาพ, ประวัติการชมเว็บไซต์, รายชื่อผู้ติดต่อ, รวมทั้งข้อมูลเชิงอัตลักษณ์อย่างอื่น (เช่น ข้อมูลเกี่ยวกับอุปกรณ์มือถือดังกล่าว)

เพกาซัสสามารถสั่งการให้แคปหน้าจอ และติดตามการคีย์ข้อมูลของผู้ใช้งาน รวมทั้งสามารถเปิดใช้งานไมโครโฟนและกล้องถ่ายรูปในโทรศัพท์ได้ เป็นเหตุให้ผู้โจมตีสามารถติดตามการเคลื่อนไหวทั้งปวงในอุปกรณ์ดังกล่าว และในบริเวณใกล้เคียงกับอุปกรณ์ เช่น การสนทนาที่เกิดขึ้นในห้อง

เพกาซัสยังเปิดโอกาสให้ผู้ควบคุมสามารถบันทึกข้อความการสื่อสารที่มีการส่งออกและรับเข้ามา (รวมทั้งข้อความที่ส่งผ่าน “การเข้ารหัส” / แอปส่งข้อความที่กำหนดให้ข้อความนั้นหายไปหลังการส่ง เช่น WhatsApp หรือ Telegram) รวมทั้งข้อมูลการโทรศัพท์หรือการพูดคุยผ่านระบบ VoIP (รวมทั้งการโทรศัพท์ผ่านแอป “ที่มีการเข้ารหัส”)



เอกสารการโฆษณาของเอ็นเอสโอชี้ให้เห็นถึงข้อมูลที่เพกาซัสสามารถสอดแนมได้ในอุปกรณ์ที่เป็นเป้าหมาย
แหล่งข้อมูล: เอกสารการโฆษณาของเอ็นเอสโอ

สำหรับโปรแกรมแชตบางอย่าง เพกาซัสช่วยให้สามารถคัดแยกล็อกไฟล์บันทึกข้อมูลการส่งข้อความในอดีต เพกาซัสยังเปิดโอกาสให้ผู้ควบคุมสามารถติดตามที่อยู่ของเป้าหมาย เช่นเดียวกับการติดสปายแวร์อย่างอื่น สปายแวร์นี้ยังอาจช่วยให้สามารถแก้ไขหรือดัดแปลงข้อมูลในอุปกรณ์นั้นได้

นอกจากนั้น สปายแวร์เพกาซัสยังอาจถูกใช้เพื่อขโมย tokens หรือลายเซ็นดิจิทัล ทำให้ผู้ควบคุมสามารถเข้าถึงบัญชีคลาวด์ที่มีการใช้อย่างแพร่หลายอย่างต่อเนื่อง

ข้อมูลเพิ่มเติมเกี่ยวกับเอ็นเอสโอกรุ๊ปและสปายแวร์เพกาซัสของบริษัท

สปายแวร์เพกาซัสจัดจำหน่ายและวางตลาดโดยเอ็นเอสโอกรุ๊ป (ซึ่งบางครั้งใช้ชื่อบริษัทว่า Q Cyber Technologies รวมทั้งชื่ออื่น ๆ) เอ็นเอสโอกรุ๊ปเป็นบริษัทซึ่งตั้งอยู่ในอิสราเอล และพัฒนาและจำหน่ายเทคโนโลยีสปายแวร์ รวมทั้งเพกาซัส[2] เอ็นเอสโอกรุ๊ปมีผู้ถือหุ้นใหญ่คือ Novalpina Capital บริษัทหุ้นนอกตลาดหลักทรัพย์จากยุโรป ซึ่งมีสำนักงานอยู่ที่ลอนดอน[3]

เอ็นเอสโอกรุ๊ปอ้างว่ามีนโยบายขายสปายแวร์เฉพาะกับลูกค้าที่เป็นรัฐบาลเท่านั้น และการส่งออกผลิตภัณฑ์ทั้งหมดดำเนินการอย่างสอดคล้องตามกฎหมายส่งออกและกลไกควบคุมของรัฐบาลอิสราเอล เอ็นเอสโอกรุ๊ปยังอ้างว่าได้ปฏิบัติตามนโยบายด้านสิทธิมนุษยชน อย่างไรก็ดี จากการเก็บข้อมูลในหลายกรณีพบว่ามีการใช้เทคโนโลยีของบริษัทในทางมิชอบเพื่อโจมตีภาคประชาสังคมเพิ่มมากขึ้นเรื่อย ๆ

ท่านสามารถศึกษางานวิจัยของซิติเซ็นแล็บเกี่ยวกับเอ็นเอสโอกรุ๊ปได้ที่เว็บไซต์: https://citizenlab.ca/tag/nso-group/

[2] โปรดสังเกตว่าในธุรกรรมบางอย่างของเทคโนโลยีนี้ อาจมีการใช้ชื่อรหัสที่แตกต่างไปสำหรับสปายแวร์เพกาซัส
[3] สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเอ็นเอสโอกรุ๊ป ท่านสามารถอ่านบทสรุปรายงานสาธารณะที่สำคัญได้ ที่นี่ นอกจากนั้น ยังมีการยื่นหลักฐานในการฟ้องคดีที่เกิดขึ้นระหว่าง WhatsApp/Facebook กับเอ็นเอสโอกรุ๊ปในศาลสหรัฐอเมริกา ซึ่งจะช่วยให้ทราบข้อมูลในระดับลึกเกี่ยวกับการทำงานของเพกาซัส และการดำเนินงานของเอ็นเอสโอกรุ๊ป (โปรดดู โดยเฉพาะ Exhibit 10 ของคำฟ้องในคดีดังกล่าว)