Exhibit CC

UNREDACTED VERSION OF DOCUMENT

PROPOSED TO BE FILED UNDER SEAL

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC. and
META PLATFORMS, INC.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES
LIMITED and Q CYBER
TECHNOLOGIES LIMITED,

Defendants.

Case No. 19-cv-07123-PJH

EXPERT REPORT OF ANTHONY VANCE

August 30, 2024

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY

Project Zero.[12] When reports were received from outside security researchers, a standard process was followed to remediate them.[13] This secure software practice resulted in remediating an exploit in December 2018 that is discussed in more detail in Sections VI and VII.

Fourth, Meta (formerly known as Facebook) provided security personnel to support WhatsApp and its development team, including:

- A security team, with at least one security team member devoted to WhatsApp full time.[14]
- A malware security team that assisted with security incident investigations.[15] In my experience, very few organizations have a dedicated team to detect, investigate, and remediate malware incidents.
- An incident response team.[16]
- A "red team" that simulated attackers and helped to identify potential exploitation vectors in WhatsApp.[17]

The above points demonstrate that security was a high priority for WhatsApp and Meta generally, that Plaintiffs took reasonable measures to secure the WhatsApp platform, and that it proactively carried out projects to improve the security of the same.

VI. WhatsApp made at least two changes to the WhatsApp servers in December 2018 that prevented, restricted, or interrupted the operation of NSO Malware

On September 3, 2018, a WhatsApp security engineer created a project task entitled, "T33535414 - Malformed Whatsapp voip_settings can be used to (at least) DoS a victim with no user interaction," to remediate an issue identified in a report submitted by an external security researcher.[18] The security impact of this was described as:

> A malicious person can make an arbitrary victim user's WhatsApp crash and then insta-crash repeatedly whenever it's being opened. Further exploitation might be possible in case there are e.g. buffer overflow vulnerabilities in the voip_settings parsing code.[19]

This issue was remediated in a software update on WhatsApp's servers that was deployed between December 3–5. On December 5 at 1:27pm. WhatsApp received confirmation from the external security researcher that the issue was remediated.[20]

Unbeknownst to WhatsApp at the time, this software update had the result of disrupting NSO malware. On December 5, around 11:11am Israel Standard Time, [redacted] Head of Sales

[12] See, e.g., https://googleprojectzero.blogspot.com/2018/12/adventures-in-video-conferencing-part-3.html and https://googleprojectzero.blogspot.com/2018/12/adventures-in-video-conferencing-part-4.html, accessed 8/27/2024.
[13] Gheorghe Dep., Aug. 16, 2024, at 52:21–25. Ibid. at 53:1–25; 54:1–21; 55:7 – 20.
[14] Ibid., at 36:17–25; 37:1–9; 68:6–13.
[15] Ibid., at 190–191:24–25, 1–3.
[16] Ibid., at 74:5–14.
[17] Ibid., at 57:1–23.
[18] See WA-NSO-00166464, p. 1.
[19] Ibid.
[20] Ibid.

for NSO until 2020,[21] sent a WhatsApp message to a group of 30 recipients:

> Hib team,
>
> No heaven installations till [sic] further notice please. In continue [sic] to [redacted] mail.[22]

"Heaven" is the code name for a covert or "zero-click" installation vector related to Pegasus that worked by exploiting WhatsApp.[23] This has been acknowledged by an NSO witness in deposition testimony, and is also evident from code residing on an Amazon Web Services (AWS) server involved in the May 2019 attack (the "AWS Server"). NSO previously stated that, "At certain times prior to January 2021, the AWS Server was being used by NSO's research and development department, to house computer code that **comprised part of the Pegasus system**" (emphasis added).[24] Files produced by NSO from this server include the Python program "__init__.py," which contains the documentation string:

> API implementation for the heaven attack vector[25]

The program also contains a statement that imports the "exploit" function from the "exploits" and "heaven" submodules within the "attackVectors" module:

> from attackVectors.heaven.exploits import exploit[26]

Approximately nine minutes after [redacted] WhatsApp message, [redacted] a key member of the technology support team at NSO,[27] sent a WhatsApp message to 54 recipients :

> Hi all,
>
> WhatsApp had [sic] made changes in their servers that currently fail all installations and can cause crashes that risk the Hummingbird vector.
>
> We need to immediately pause all Hummingbird installations cross [sic] all systems (Customer sites (P2 &P3, Tactical covert), Sales) until [NSO's] Android research team will be able to provide a solution.
>
> Official message to clients was synced with CEs (BoaT).

[21] See Plaintiffs' Notice of Motion and Motion for Issuance of a Letter Rogatory Pursuant to the Hague Convention; Memorandum of Points and Authorities and Support, (Dkt. 335-2) at p. 7.
[22] SHANER_WHATSAPP_00001100.
[23] Eshkar Dep. 122:24 – 123:2; 124:6 – 8; In cybersecurity, an attack vector is a method or means of attacking a victim computer. See *DRAFT NIST Special Publication 800-154: Guide to Data-Centric System Threat Modeling*, p. 5, https://csrc.nist.gov/pubs/sp/800/154/ipd, accessed 8/30/2024.
[24] See Decl. of Chaim Gelfand in Support , filed 7/15/2024.
[25] WA-NSO-00016952, line 2. The files of the AWS Server produced were acquired November 9, 2020. *See* Decl. of Chaim Gelfand Supp. Defs. Opp. To Pls. Mot. to Compel Discovery Regarding AWS Server (Dkt. 339-1), at 3:16.
[26] WA-NSO-00016952, line 10.
[27] See *Plaintiffs' Notice of Motion and Motion for Issuance of a Letter Rogatory Pursuant to the Hague Convention; Memorandum of Points and Authorities and Support*, (Dkt. 335-2) at p. 7.