

Gazneli4_30PM_ver1

Designation List Report



Gazneli, Tamir

2024-09-04

P's Narrowed	01:31:32
D's Counters	00:09:36
TOTAL RUN TIME	01:41:08



Documents linked to video:

- P34
- P44
- P59
- P60
- P62
- P63
- P64
- P65
- P66



Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
7:01 - 7:03	Gazneli, Tamir 2024-09-04 7:01 MR. PEREZ-MARQUES: Mr. Gazneli, could 7:02 you state your name for the record? 7:03 A. My name is Tamir Gazneli.	00:00:06	Gazneli4_30PM_v er1.1
23:23 - 24:03	Gazneli, Tamir 2024-09-04 23:23 Q. So you joined NSO Group in May 2015, 23:24 is that correct? 23:25 A. Yes. 24:01 Q. How did you come to work for NSO 24:02 Group? 24:03 A. It is not May. It is November.	00:00:08	Gazneli4_30PM_v er1.2
25:09 - 25:11	Gazneli, Tamir 2024-09-04 25:09 Q. You started at NSO as a security 25:10 researcher, is that correct? 25:11 A. Yes.	00:00:05	Gazneli4_30PM_v er1.3
28:09 - 28:19	Gazneli, Tamir 2024-09-04 28:09 Q. In December 2017 you were promoted 28:10 to Security Research Team Leader. Is that 28:11 correct? 28:12 A. Yes. 28:13 Q. And what were your responsibilities 28:14 as Security Research Team Leader? 28:15 A. I was responsible for the team -- 28:16 one of the research teams in the research group. 28:17 Q. And what did that research team 28:18 focus on? 28:19 A. Android applications.	00:00:40	Gazneli4_30PM_v er1.4
28:20 - 28:21	Gazneli, Tamir 2024-09-04 28:20 Q. Which Android applications? 28:21 A. Not specific, just any.	00:00:05	Gazneli4_30PM_v er1.5
28:22 - 28:23	Gazneli, Tamir 2024-09-04 28:22 Q. Did that work relate at all to 28:23 WhatsApp, the work of that team?	00:00:04	Gazneli4_30PM_v er1.6
28:25 - 28:25	Gazneli, Tamir 2024-09-04 28:25 A. Part of the team.	00:00:02	Gazneli4_30PM_v er1.7
29:06 - 29:09	Gazneli, Tamir 2024-09-04 29:06 Q. How many people -- why don't we 29:07 start with how many about people were working on	00:00:08	Gazneli4_30PM_v er1.8

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	29:08 WhatsApp as part of the team that you led as 29:09 Security Research Team Leader?		
29:12 - 29:12	Gazneli, Tamir 2024-09-04 29:12 A. Four.	00:00:01	Gazneli4_30PM_v er1.9
29:21 - 30:10	Gazneli, Tamir 2024-09-04 29:21 And you supervised that team that was 29:22 working on WhatsApp during your time as Security 29:23 Team Research Leader. 29:24 A. Yes. 29:25 Q. And what were they doing with 30:01 respect to WhatsApp? 30:02 A. Research application. 30:03 Q. Again for the purpose of developing 30:04 installation vectors? 30:05 A. I will say it is developing the 30:06 software required for gaining access. 30:07 Q. As I understand it, installation 30:08 vectors are software required to gain access. Is 30:09 that consistent with your definition of what an 30:10 installation vector is?	00:01:06	Gazneli4_30PM_v er1.10
30:13 - 30:23	Gazneli, Tamir 2024-09-04 30:13 A. Can you define access? When you say 30:14 "access" what do you mean by access? 30:15 Q. You said access. "I will say it is 30:16 developing the software required for gaining 30:17 access." What did you mean by access? 30:18 A. Access to the data which resides on 30:19 the endpoint. 30:20 Q. That reside on the endpoint? 30:21 A. Yes. 30:22 Q. Meaning the target device? 30:23 A. Yes.	00:00:23	Gazneli4_30PM_v er1.11
31:04 - 31:08	Gazneli, Tamir 2024-09-04 31:04 Q. Okay. And so the team that was 31:05 working on WhatsApp that you supervised as 31:06 Security Research Team Leader was investigating 31:07 WhatsApp in order to develop software that could 31:08 be used to gain access to target devices?	00:00:17	Gazneli4_30PM_v er1.12
31:11 - 31:17	Gazneli, Tamir 2024-09-04	00:00:18	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	31:11 A. The team was researching Android 31:12 related applications and services in order to gain 31:13 access to the endpoint data. 31:14 Q. Okay. Now, you testified previously 31:15 that they were doing work -- you gave us the four 31:16 names who were doing work related to WhatsApp? 31:17 A. Yes.		er1.13
31:18 - 31:19	Gazneli, Tamir 2024-09-04 31:18 Q. And what work were they doing 31:19 related to WhatsApp?	00:00:02	Gazneli4_30PM_v er1.14
32:05 - 32:10	Gazneli, Tamir 2024-09-04 32:05 A. To understand how the application 32:06 works. 32:07 Q. For what purpose? 32:08 A. As I stated before, in order to 32:09 build the software that gets access to the 32:10 endpoint's data.	00:00:13	Gazneli4_30PM_v er1.15
37:24 - 38:01	Gazneli, Tamir 2024-09-04 37:24 Q. What is a 0 click exploit? 37:25 A. An exploit that does not require any 38:01 interaction from the target.	00:00:11	Gazneli4_30PM_v er1.16
39:01 - 39:07	Gazneli, Tamir 2024-09-04 39:01 Q. Let me ask it this way. You 39:02 understand that Heaven -- you are familiar with 39:03 the Heaven installation vector? 39:04 A. Yes. 39:05 Q. And that worked via WhatsApp, is 39:06 that right? That used WhatsApp messages as part 39:07 of the installation?	00:00:16	Gazneli4_30PM_v er1.17
39:10 - 39:14	Gazneli, Tamir 2024-09-04 39:10 A. Yes. 39:11 Q. And so when I say "via WhatsApp", 39:12 what I mean is the relationship between the 39:13 installation vector and WhatsApp, such as the one 39:14 that Heaven had. Is that clear to you?	00:00:14	Gazneli4_30PM_v er1.18
39:16 - 40:04	Gazneli, Tamir 2024-09-04 39:16 A. Yes. 39:17 Q. And so with that clarification, did 39:18 the team that you supervised as Security Research	00:01:04	Gazneli4_30PM_v er1.19

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	39:19 Team Leader develop 0 click exploits that worked 39:20 via WhatsApp? 39:21 A. It developed 0 click vectors 39:22 which -- one of the ways was via WhatsApp. 39:23 Q. Okay. Did those vectors that they 39:24 developed have names? 39:25 A. Heaven, Eden and ERISED. 40:01 Q. And so Heaven, Eden and ERISED were 40:02 developed by the researchers on the team that you 40:03 supervised as Security Research Team Leader? 40:04 A. Yes.		
41:05 - 41:09	Gazneli, Tamir 2024-09-04 41:05 Q. When we broke for the fire alarm, I 41:06 believe we had a question pending. I had asked 41:07 you whether you would agree that you are very 41:08 familiar personally with the Eden, Heaven and 41:09 ERISED exploits?	00:00:13	Gazneli4_30PM_v er1.20
41:11 - 41:19	Gazneli, Tamir 2024-09-04 41:11 A. I would say that I am familiar with 41:12 the exploits but not each and every line in the 41:13 code. 41:14 Q. But you led the team that developed 41:15 them, right? 41:16 A. Yes. 41:17 Q. You were promoted to Director of R&D 41:18 in January 2020. Is that correct? 41:19 A. Yes.	00:00:17	Gazneli4_30PM_v er1.21
44:19 - 44:24	Gazneli, Tamir 2024-09-04 44:19 Q. During your time as Director of R&D, 44:20 were any researchers that you supervised working 44:21 on installation vectors via WhatsApp? 44:22 A. Yes. 44:23 Q. Which vectors were those? 44:24 A. When I was of R&D it was ERISED.	00:00:34	Gazneli4_30PM_v er1.22
47:07 - 47:15	Gazneli, Tamir 2024-09-04 47:07 Q. In November 2022, you were promoted 47:08 to VP R&D, correct? 47:09 A. Yes. 47:10 Q. How did your responsibilities change	00:00:23	Gazneli4_30PM_v er1.23

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	47:11 at that point?		
	47:12 A. Now I am leading the entire R&D of		
	47:13 the company.		
	47:14 Q. Who do you report to as VP R&D?		
	47:15 A. To the CEO.		
50:04 - 50:15	Gazneli, Tamir 2024-09-04	00:00:33	Gazneli4_30PM_v er1.24
	50:04 Q. And so you do speak to prospective		
	50:05 customers about the capabilities of the technology		
	50:06 in your role as VP R&D?		
	50:07 A. Whenever it is required, yes.		
	50:08 Q. As Director of R&D, did you interact		
	50:09 with customers?		
	50:10 A. Yes.		
	50:11 Q. For the same purposes?		
	50:12 A. Say for limited responsibilities,		
	50:13 but like more smaller responsibilities, due to the		
	50:14 fact that I was Director for only Android, but		
	50:15 yes.		
67:06 - 67:09	Gazneli, Tamir 2024-09-04	00:00:13	Gazneli4_30PM_v er1.25
	67:06 Q. Let me just take a step back for a		
	67:07 moment to see if I can make our terminology clear.		
	67:08 Eden, Heaven and ERISED are all installation		
	67:09 vectors that worked via WhatsApp, correct?		
67:12 - 68:06	Gazneli, Tamir 2024-09-04	00:01:05	Gazneli4_30PM_v er1.26
	67:12 A. Heaven, Eden and ERISED were		
	67:13 installation vectors that were activated via		
	67:14 WhatsApp.		
	67:15 Q. During the period April 29, 2018 to		
	67:16 May 10, 2020, were any installation vectors in use		
	67:17 besides Heaven, Eden and ERISED that were		
	67:18 activated via WhatsApp?		
	67:19 A. No.		
	67:20 Q. So those are the three, yes?		
	67:21 A. Yes.		
	67:22 Q. And am I right that NSO sometimes		
	67:23 refers to them collectively as Hummingbird?		
	67:24 A. Yes.		
	67:25 Q. And does the term Hummingbird		
	68:01 include any vectors other than those three?		
	68:02 A. No.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	68:03 Q. So if I refer to the Hummingbird		
	68:04 vectors, you will understand that I am referring		
	68:05 to those three?		
	68:06 A. In respect to the timeframe, yes.		
69:22 - 70:04	Gazneli, Tamir 2024-09-04	00:00:26	Gazneli4_30PM_v er1.27
	69:22 Q. So the WhatsApp client, the server		
	69:23 functionality. Is anything else part of the		
	69:24 ecosystem you described that enables one WhatsApp		
	69:25 clients to communicate with another?		
	70:01 A. No.		
	70:02 Q. And so as part of the development of		
	70:03 the Hummingbird installation vectors, NSO		
	70:04 investigated that ecosystem. Is that right?		
70:07 - 70:15	Gazneli, Tamir 2024-09-04	00:00:38	Gazneli4_30PM_v er1.28
	70:07 A. We developed an internal environment		
	70:08 that enabled us to work on our devices.		
	70:09 Q. What does that mean?		
	70:10 A. That means that we used WhatsApp		
	70:11 clients that were installed on company owned		
	70:12 devices and used the functionality that was		
	70:13 developed internally which enabled communication		
	70:14 between the clients that were used in this		
	70:15 internal environment.		
74:06 - 74:25	Gazneli, Tamir 2024-09-04	00:01:15	Gazneli4_30PM_v er1.29
	74:06 Q. And so as part of that you developed		
	74:07 servers that, to the best extent you can, aim to		
	74:08 replicate the functionality of the WhatsApp		
	74:09 servers?		
	74:10 A. Yes.		
	74:11 Q. And the purpose is to investigate or		
	74:12 research how messages would be treated by WhatsApp		
	74:13 servers. Right?		
	74:14 A. No.		
	74:15 Q. What is the purpose?		
	74:16 A. The purpose was to research the		
	74:17 WhatsApp client on the target's device, and in		
	74:18 order to build the software to eventually gain		
	74:19 access to the data that resides on it.		
	74:20 Q. And why was it necessary to create		
	74:21 that internal version of the WhatsApp servers as		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	74:22 part of the R&D process?		
	74:23 A. This is a practice done by any cyber		
	74:24 company, whether defensive or offensive, in order		
	74:25 to work in the internal environments.		
76:06 - 76:15	Gazneli, Tamir 2024-09-04	00:00:35	Gazneli4_30PM_v er1.30
	76:06 Q. Right. And then at some point does		
	76:07 the testing progress to actually testing it		
	76:08 through WhatsApp's actual ecosystem?		
	76:09 A. After reaching the capability in the		
	76:10 internal server, then there is a phase of testing		
	76:11 in the real environment, yes.		
	76:12 Q. And with respect to the Hummingbird		
	76:13 vectors, when did NSO reach the point of testing		
	76:14 the installation vectors in WhatsApp's actual		
	76:15 ecosystem?		
76:18 - 76:22	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.31
	76:18 A. I don't recall the exact month this		
	76:19 was done.		
	76:20 Q. Approximately?		
	76:21 A. Approximately, it was near		
	76:22 April 2018.		
80:02 - 80:05	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.32
	80:02 Were any live WhatsApp accounts created		
	80:03 during any phase of the testing of the Hummingbird		
	80:04 vectors by NSO?		
	80:05 A. Yes.		
81:03 - 81:07	Gazneli, Tamir 2024-09-04	00:00:21	Gazneli4_30PM_v er1.33
	81:03 Q. And so could you say approximately		
	81:04 how many WhatsApp accounts were created as part of		
	81:05 the testing of the Hummingbird vectors?		
	81:06 A. I don't have the exact number, but I		
	81:07 can estimate it is about 50 numbers.		
81:16 - 81:19	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.34
	81:16 Q. Do you have any understanding of		
	81:17 approximately how many times -- let me put it this		
	81:18 way -- on how many target devices the Hummingbird		
	81:19 vectors have been successfully used by NSO?		
81:21 - 82:03	Gazneli, Tamir 2024-09-04	00:00:20	Gazneli4_30PM_v er1.35
	81:21 A. When you say Hummingbird was used,		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	81:22 what do you mean by that?		
	81:23 Q. Used as -- successfully used as an		
	81:24 installation vector to cause the installation of		
	81:25 the agent?		
	82:01 A. In which timeframe?		
	82:02 Q. What I will call the relevant		
	82:03 timeframe, so April 2018 to May 2020?		
82:06 - 82:06	Gazneli, Tamir 2024-09-04	00:00:02	Gazneli4_30PM_v er1.36
	82:06 A. I don't have an exact number.		
82:20 - 82:23	Gazneli, Tamir 2024-09-04	00:00:08	Gazneli4_30PM_v er1.37
	82:20 Q. I understand you don't have the		
	82:21 exact number. I am asking for an approximate		
	82:22 number. Tens, hundreds, thousands, tens of		
	82:23 thousands?		
82:25 - 83:03	Gazneli, Tamir 2024-09-04	00:00:10	Gazneli4_30PM_v er1.38
	82:25 A. It is not tens of thousands but it		
	83:01 is not hundreds.		
	83:02 Q. So thousands?		
	83:03 A. In between, yes.		
83:09 - 83:11	Gazneli, Tamir 2024-09-04	00:00:05	Gazneli4_30PM_v er1.39
	83:09 Q. In between what?		
	83:10 A. In between hundreds and tens of		
	83:11 thousands.		
83:22 - 84:02	Gazneli, Tamir 2024-09-04	00:00:16	Gazneli4_30PM_v er1.40
	83:22 Q. The term "Pegasus", does that to you		
	83:23 mean the agent or is it broader than the agent?		
	83:24 A. This is the name of the product.		
	83:25 Q. And does that include the		
	84:01 installation vectors or would Pegasus be the agent		
	84:02 itself?		
84:04 - 84:23	Gazneli, Tamir 2024-09-04	00:00:49	Gazneli4_30PM_v er1.41
	84:04 MR. PEREZ-MARQUES: I just want to		
	84:05 clarify our terminology so I can make the		
	84:06 questions clearer.		
	84:07 A. The product that is called Pegasus		
	84:08 eventually delivers the data to the customers		
	84:09 which are sent to the customers by the agent, and		
	84:10 and the agent installed using installation		
	84:11 investigators.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	84:12 Q. And so the agent is part of Pegasus?		
	84:13 A. Yes.		
	84:14 Q. And the installation vectors are		
	84:15 part of Pegasus?		
	84:16 A. Yes.		
	84:17 Q. And the agent is the piece of		
	84:18 Pegasus that actually delivers information to		
	84:19 customers?		
	84:20 A. Yes.		
	84:21 Q. And that information is obtained		
	84:22 from the target devices?		
	84:23 A. Yes.		
87:19 - 88:02	Gazneli, Tamir 2024-09-04	00:00:35	Gazneli4_30PM_v er1.42
 P59.2	87:19 Q. I would like to show you what we		
	87:20 have marked as Exhibit 2032.		
	87:21 (Exhibit 2032 marked for identification)		
	87:22 This is a multipage document with the		
	87:23 Bates stamp NSO_WHATSAPP_00045678. Do you		
	87:24 recognize this document?		
	87:25 A. Do you want me to go over it?		
	88:01 Q. Feel free to flip through it. The		
	88:02 first question is just whether you recognize it.		
88:03 - 88:15	Gazneli, Tamir 2024-09-04	00:00:28	Gazneli4_30PM_v er1.43
	88:03 Do you recognize this document?		
	88:04 A. Yes.		
	88:05 Q. What is it?		
	88:06 A. Some kind of training material,		
	88:07 training -- customer facing material.		
	88:08 Q. Customer facing material or training		
	88:09 material?		
	88:10 A. Training.		
	88:11 Q. Training. Is it a product		
	88:12 description for Pegasus?		
	88:13 A. Yes.		
	88:14 Q. So the endpoint solution that is		
	88:15 referred to here is Pegasus?		
88:18 - 88:18	Gazneli, Tamir 2024-09-04	00:00:01	Gazneli4_30PM_v er1.44
	88:18 A. Yes.		
89:02 - 89:20	Gazneli, Tamir 2024-09-04	00:00:58	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
P59.6.1	89:02	Q. The third paragraph there revs to	er1.45
	89:03	Pegasus as a "breakthrough solution, developed by	
	89:04	veterans of elite intelligence agencies". Do you	
	89:05	see that? It is the third paragraph under	
	89:06	"Overview"?	
	89:07	A. Yes.	
	89:08	Q. And do you agree with the	
	89:09	characterization of Pegasus as a breakthrough	
	89:10	solution?	
	89:11	A. As for the date, I think it was	
	89:12	breakthrough, yes.	
	89:13	Q. It is a highly innovative product?	
	89:14	A. Yes.	
	89:15	Q. Highly sophisticated?	
	89:16	A. I think it depends on the definition	
	89:17	of sophisticated. By what means?	
	89:18	Q. Would you consider it a very	
	89:19	sophisticated product?	
	89:20	A. Yes.	
	90:23 - 91:02	Gazneli, Tamir 2024-09-04	
90:23	Q. So I am asking you, as the person		
90:24	who is presenting NSO's knowledge with respect to		
90:25	the R&D that led to Pegasus, is it accurate that		
91:01	it was developed by veterans of elite intelligence		
91:02	agencies?		
91:05 - 91:07	Gazneli, Tamir 2024-09-04	00:00:09	Gazneli4_30PM_v er1.47
91:05	A. Part of the company that developed		
91:06	the solution were veterans of elite		
91:07	intelligence --		
91:08 - 91:10	Gazneli, Tamir 2024-09-04	00:00:06	Gazneli4_30PM_v er1.48
91:08	Q. Would you agree that Pegasus was		
91:09	developed by personnel with highly specialized		
91:10	expertise?		
91:13 - 91:17	Gazneli, Tamir 2024-09-04	00:00:23	Gazneli4_30PM_v er1.49
91:13	A. I would say the development of		
91:14	Pegasus requires, in terms of research, specific		
91:15	capabilities that according to my resume you can		
91:16	see that may be acquired. So what is the		
91:17	question?		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
91:18 - 91:23	<p>Gazneli, Tamir 2024-09-04</p> <p>91:18 Q. The question was whether you agree 91:19 that Pegasus was developed by personnel with 91:20 highly specialized expertise? 91:21 A. I would say that the research field 91:22 which is part of Pegasus requires specialized 91:23 expertise.</p>	00:00:19	Gazneli4_30PM_v er1.50
91:24 - 92:09	<p>Gazneli, Tamir 2024-09-04</p> <p>91:24 Q. What about the development field 91:25 with respect to the agent itself? 92:01 A. This is development per se, as any 92:02 development. 92:03 Q. And it also requires specialized 92:04 expertise? 92:05 A. It requires understanding of 92:06 internals of the framework. I don't see it as 92:07 specialized expertise, as any other specialized 92:08 expertise required for developing any other 92:09 application.</p>	00:00:25	Gazneli4_30PM_v er1.51
92:10 - 92:16	<p>Gazneli, Tamir 2024-09-04</p> <p>92:10 Q. The next section here, 1.1, refers 92:11 to smartphone data interception challenges. Do 92:12 you see that? "Overcoming smartphone data 92:13 interception challenges"? 92:14 A. Yes. 92:15 Q. And those are challenges that 92:16 Pegasus is able to overcome?</p>	00:00:18	Gazneli4_30PM_v er1.52
97:14 - 98:15	<p>Gazneli, Tamir 2024-09-04</p> <p> P59.8.1 97:14 Q. On page 3, under "Cyber Intelligence 97:15 for the Mobile World". Do you see that section? 97:16 A. Yes.</p> <p> P59.8.2 97:17 Q. The second paragraph states "EPS". 97:18 EPS means endpoint solution, right? 97:19 A. Yes. 97:20 Q. And that means Pegasus, in the 97:21 context of this document? 97:22 A. Yes. 97:23 Q. "EPS silently deploys an invisible 97:24 software (SW) component (agent) on a target's 97:25 device which extracts and securely transmits data</p>	00:01:22	Gazneli4_30PM_v er1.53


Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	98:01 for intelligence analysis."		
	98:02 Do you see that?		
	98:03 A. Yes.		
	98:04 Q. And what does it mean that the agent		
	98:05 is deployed silently?		
	98:06 A. This defines how the agent is		
	98:07 installed, not the installation vector itself.		
	98:08 Q. And what does it mean that the agent		
	98:09 is deployed silently?		
	98:10 A. It means that the target is not		
	98:11 aware that the agent is being installed.		
	98:12 Q. Right. And the other services that		
	98:13 are part of the broader ecosystem are also		
	98:14 unaware. Isn't that part of it as well, as we		
	98:15 discussed earlier?		
98:17 - 98:20	Gazneli, Tamir 2024-09-04	00:00:13	Gazneli4_30PM_v er1.54
	98:17 A. This activity should be concealed,		
	98:18 yes.		
	98:19 Q. And NSO designed Pegasus with the		
	98:20 objective that it be concealed, isn't that right?		
98:22 - 99:09	Gazneli, Tamir 2024-09-04	00:00:47	Gazneli4_30PM_v er1.55
	98:22 A. It is part of being software that is		
	98:23 being used by the type of customers that are using		
	98:24 these cyber intelligence tools, the product should		
	98:25 be as concealed as possible.		
	99:01 Q. It also says that -- it refers to		
 P59.11.5	99:02 the software component as "invisible". Do you see		
	99:03 that in that same sentence?		
	99:04 A. Yes.		
	99:05 Q. And that means that the software		
	99:06 component is invisible to the target, right?		
	99:07 A. Yes.		
	99:08 Q. And also invisible to other services		
	99:09 involved in the ecosystem, right?		
99:12 - 99:20	Gazneli, Tamir 2024-09-04	00:00:42	Gazneli4_30PM_v er1.56
	99:12 A. It is invisible to the target, as by		
	99:13 nature of the product, and the agent is invisible.		
	99:14 Yes, the answer is yes.		
	99:15 Q. And that is by design, is that		
	99:16 right? NSO designed the product so that it would		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	99:17 be invisible not only to the target but to others 99:18 as well? 99:19 A. This is a requirement of such 99:20 software capabilities.		
103:06 - 103:14  Clear	Gazneli, Tamir 2024-09-04 103:06 At the time in 2018 and 2019 that NSO 103:07 had 0 click installation vectors for Android via 103:08 WhatsApp -- let me start with this. 103:09 Did NSO have 0 click installation 103:10 vectors during that time period for Android, other 103:11 than the Hummingbird vectors? 103:12 A. During that time period? 103:13 Q. Yes. 103:14 A. No.	00:00:25	Gazneli4_30PM_v er1.57
105:22 - 106:02	Gazneli, Tamir 2024-09-04 105:22 MR. PEREZ-MARQUES: Mr. Gazneli, what 105:23 are the advantages of 0 click installation vectors 105:24 over 1 click installation vectors? 105:25 A. 0 click installation vectors do not 106:01 require any interaction by the target. 106:02 Q. And why is that preferable?	00:00:22	Gazneli4_30PM_v er1.58
106:05 - 106:08	Gazneli, Tamir 2024-09-04 106:05 A. From the customer's point of view, 0 106:06 click installation vectors are more concealed and 106:07 they enable them to execute their operations in 106:08 more concealed ways.	00:00:19	Gazneli4_30PM_v er1.59
107:05 - 107:18  P59.8.3	Gazneli, Tamir 2024-09-04 107:05 Q. So I would like to go back to 107:06 Exhibit 2032, which you still have in front of 107:07 you. The next section on page 3 has a section 107:08 titled "Benefits of our endpoint solution". Do 107:09 you see that? 107:10 A. Yes. 107:11 Q. And the first benefit identified is 107:12 global coverage. Is that right? 107:13 A. Yes. 107:14 Q. It states: 107:15 "Monitor targets' devices while they 107:16 connect to the internet from any location."	00:00:36	Gazneli4_30PM_v er1.60

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	107:17 Right?		
	107:18 A. Yes.		
108:20 - 111:08	Gazneli, Tamir 2024-09-04	00:03:18	Gazneli4_30PM_v er1.61
	108:20 Q. It is the agent that monitors target		
	108:21 devices, right, not the vector?		
	108:22 A. The agent is the one that monitors		
	108:23 target devices, yes.		
	108:24 Q. And is it correct that Pegasus can		
	108:25 monitor a target's devices from any location?		
	109:01 A. As for the potential of the agent,		
	109:02 yes.		
 P59.8.4	109:03 Q. The next bullet states:		
	109:04 "Unlimited access to targets' mobile		
	109:05 devices. Remotely and covertly collect		
	109:06 information about a target's relationships,		
	109:07 locations, phone calls, plans and activities."		
	109:08 Do you see that?		
	109:09 A. Yes.		
	109:10 Q. And is that an accurate statement of		
	109:11 Pegasus' capabilities?		
	109:12 A. Yes, it is like.		
 P59.8.5	109:13 Q. A few bullets down there is a bullet		
	109:14 that begins "Operate target devices". Do you see		
	109:15 that?		
	109:16 A. Yes.		
	109:17 Q. It says:		
	109:18 "Activate the microphone to listen in on		
	109:19 a target's environment. Turn on the camera to		
	109:20 take snapshots and take screenshots to collect		
	109:21 non-communications data of high intel value."		
	109:22 Is that an accurate statement of		
	109:23 Pegasus' capabilities?		
	109:24 A. Yes.		
	109:25 Q. Is it fair to say that the purpose		
	110:01 of Pegasus is to obtain information from a		
	110:02 target's devices?		
	110:03 A. Yes.		
	110:04 Q. And among other capabilities Pegasus		
	110:05 has the ability to turn on a device microphone?		
	110:06 A. In some types of agents, yes.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	110:07 Q. And to take photos with a device		
	110:08 camera, that is also a capability of Pegasus?		
	110:09 A. Yes.		
	110:10 Q. And it had those capabilities in		
	110:11 2019?		
	110:12 A. Yes.		
	110:13 Q. And it continues to have those		
	110:14 capabilities today?		
	110:15 A. As I said before, it depends on		
	110:16 agents, the specifics of the agent.		
	110:17 Q. How so?		
	110:18 A. Eventually the vector defines what		
	110:19 are the capabilities that the agent can ask.		
	110:20 Q. So certain vectors can only make		
	110:21 available certain functionality of the agent?		
	110:22 A. Yes.		
	110:23 Q. And with respect to Pegasus as		
	110:24 installed by the Hummingbird vectors, did Pegasus		
	110:25 in 2019 have the capability to turn on device		
	111:01 microphones and take snapshots?		
	111:02 A. Yes.		
	111:03 Q. The section I read also describes		
	111:04 the information obtained as having high intel		
	111:05 value. Do you see that?		
	111:06 A. Yes.		
	111:07 Q. And do you agree that the		
	111:08 information obtained by Pegasus is valuable?		
111:11 - 111:14	Gazneli, Tamir 2024-09-04	00:00:08	Gazneli4_30PM_v er1.62
	111:11 A. The value of the intel is in the		
	111:12 eyes of the customer.		
	111:13 Q. And the information is valuable to		
	111:14 NSO's customers, yes?		
111:17 - 111:24	Gazneli, Tamir 2024-09-04	00:00:27	Gazneli4_30PM_v er1.63
	111:17 A. Eventually the customers seek to get		
	111:18 access to the data that is on the device, and part		
	111:19 of it is using microphone and camera, snapshots,		
	111:20 as it states here.		
	111:21 Q. And not limited to microphone and		
	111:22 snapshots, but the information obtained through		
	111:23 Pegasus is valuable to NSO's customers. Isn't		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	111:24 that right?		
112:03 - 112:09	Gazneli, Tamir 2024-09-04	00:00:17	Gazneli4_30PM_v er1.64
	112:03 A. We believe that this is information		
	112:04 that customers would like to get access to. That		
	112:05 is why we developed the capabilities.		
	112:06 Q. Right, and because they consider it		
	112:07 valuable, they are willing to pay NSO typically		
	112:08 millions of dollars to license the Pegasus		
	112:09 technology. Right?		
112:12 - 112:14	Gazneli, Tamir 2024-09-04	00:00:08	Gazneli4_30PM_v er1.65
	112:12 A. Because they value the information		
	112:13 they are willing to buy the software in order to		
	112:14 use it.		
112:23 - 113:13	Gazneli, Tamir 2024-09-04	00:00:40	Gazneli4_30PM_v er1.66
	112:23 Q. It says:		
	112:24 "The EPS solution uses cutting edge		
	112:25 technology."		
	113:01 Do you agree with that characterization?		
	113:02 A. Yes.		
 P59.11.1	113:03 Q. If we go to page 6, there is a		
	113:04 section 3.2 titled "Agent Installation Vectors".		
	113:05 Do you see that?		
	113:06 A. Yes.		
	113:07 Q. It states that:		
	113:08 "Installing an agent on a target's		
	113:09 device is the heart of any intelligence operation		
	113:10 using EPS."		
	113:11 Do you see the language I just read?		
	113:12 A. Yes.		
	113:13 Q. Do you agree with that?		
113:16 - 113:17	Gazneli, Tamir 2024-09-04	00:00:05	Gazneli4_30PM_v er1.67
	113:16 A. This is what it says.		
	113:17 Q. Do you agree with it?		
113:20 - 113:25	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.68
	113:20 A. I would read the entire sentence,		
	113:21 which states "Installing the agent on target's		
	113:22 device is the heart of any intelligence operation		
	113:23 using EPS, and each installation is carefully		
	113:24 planned to ensure success."		


Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
114:02 - 114:09	<p>113:25 Q. Do you agree with that?</p> <p>Gazneli, Tamir 2024-09-04</p> <p>114:02 A. Again, it states the operations from</p> <p>114:03 the customer's eyes and the value of the</p> <p>114:04 intelligence from the customer's eyes.</p> <p>114:05 Q. But from your perspective, as the</p> <p>114:06 head of R&D at NSO, do you agree that installing</p> <p>114:07 an agent on the target's device is the heart of</p> <p>114:08 any intelligence operation using EPS or using</p> <p>114:09 Pegasus?</p>	00:00:21	Gazneli4_30PM_v er1.69
114:13 - 114:20	<p>Gazneli, Tamir 2024-09-04</p> <p>114:13 A. Being the agent of the software</p> <p>114:14 enables the access to the data which customers</p> <p>114:15 value and need to get for their operations. This</p> <p>114:16 is the beginning of the operation.</p> <p>114:17 Q. The installation is the beginning?</p> <p>114:18 A. Installing the agent.</p> <p>114:19 Q. Why is installation so important to</p> <p>114:20 an intelligence operation using Pegasus?</p>	00:00:27	Gazneli4_30PM_v er1.70
114:23 - 115:03	<p>Gazneli, Tamir 2024-09-04</p> <p>114:23 A. Customers seek to get access to data</p> <p>114:24 and these type of solutions are one of the ways</p> <p>114:25 for them to get access.</p> <p>115:01 Q. The installation is what makes the</p> <p>115:02 information extraction possible, right?</p> <p>115:03 A. Yes.</p>	00:00:22	Gazneli4_30PM_v er1.71
116:03 - 116:06	<p> P59.11.2</p> <p>116:03 Q. Specifically, when it says "a covert</p> <p>116:04 message is sent to a mobile device", in 2018 and</p> <p>116:05 2019, NSO was sending such covert messages via</p> <p>116:06 WhatsApp. Isn't that right?</p>	00:00:13	Gazneli4_30PM_v er1.72
116:09 - 117:15	<p>Gazneli, Tamir 2024-09-04</p> <p>116:09 A. In 2018 and 2019 the solutions</p> <p>116:10 used -- the solution was communicating with</p> <p>116:11 target's device in order to activate the</p> <p>116:12 vulnerability.</p> <p>116:13 Q. But this language here says "a</p> <p>116:14 covert message is sent to a mobile device". Do</p> <p>116:15 you see that language?</p>	00:01:40	Gazneli4_30PM_v er1.73

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	116:16 A. Yes.		
	116:17 Q. And in the Hummingbird vectors that		
	116:18 message was being sent via WhatsApp. Isn't that		
	116:19 right?		
	116:20 A. This was the only way to communicate		
	116:21 between peer to peer.		
	116:22 Q. And so it was being sent via		
	116:23 WhatsApp in the Hummingbird vector via WhatsApp?		
	116:24 A. Messages were sent to target's		
	116:25 device.		
	117:01 Q. Via WhatsApp, right?		
	117:02 A. Yes, via WhatsApp.		
	117:03 Q. That is how the Hummingbird vectors		
	117:04 worked?		
	117:05 A. In this timeframe, yes.		
 P59.11.3	117:06 Q. The next sentence states that:		
	117:07 "The message triggers the smartphone to		
	117:08 download and install the agent."		
	117:09 Correct? Do you see that language?		
	117:10 A. Yes.		
	117:11 Q. As to the Hummingbird vectors, is		
	117:12 that correct, that the message transmitted via		
	117:13 WhatsApp would trigger a target device to download		
	117:14 the Pegasus agent?		
	117:15 A. Yes.		
118:02 - 118:14	Gazneli, Tamir 2024-09-04	00:00:36	Gazneli4_30PM_v er1.74
 P59.11.4	118:02 Q. What does "the installation is		
	118:03 completely invisible" mean?		
	118:04 A. The second point talks about		
	118:05 download and installing the agent. The third		
	118:06 topic talks about this installation phase and		
	118:07 states that the installation of agent, which is		
	118:08 already on the device, it is not exposed to		
	118:09 anything else, is completely invisible, and cannot		
	118:10 be stopped. Therefore it is visible and cannot be		
	118:11 stopped on the device.		
	118:12 Q. Got it. So that refers to the		
	118:13 installation at the agent?		
	118:14 A. Yes.		
120:18 - 120:22	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
 Clear	120:18 Q. And as to Eden, Heaven and ERISED, 120:19 the message that would trigger the download of the 120:20 agent were transmitted via WhatsApp. Is that 120:21 right? 120:22 A. Yes.		er1.75
125:11 - 125:19	Gazneli, Tamir 2024-09-04 125:11 Q. And during that time when you were 125:12 meeting with customers did you ever hear from 125:13 customers that the capabilities NSO was offering 125:14 were different or superior to what others -- what 125:15 they had seen elsewhere in the market? 125:16 A. Some of them. Again, it depends 125:17 which competitor met before. 125:18 Q. Some of them made that point? 125:19 A. Yes.	00:00:28	Gazneli4_30PM_v er1.76
126:13 - 127:21	Gazneli, Tamir 2024-09-04 126:13 Q. And Pegasus obtains text 126:14 information, correct? 126:15 A. Yes. 126:16 Q. And audio information? 126:17 A. Yes. 126:18 Q. Including intercepted calls? 126:19 A. These are intercepted on the device. 126:20 Q. Right. But that is part of the 126:21 information that Pegasus obtains from target 126:22 devices? 126:23 A. Of course. 126:24 Q. I didn't get your answer. 126:25 A. Yes. 127:01 Q. It also can gather what is referred 127:02 to here as environmental taps, meaning microphone 127:03 recordings. Yes? 127:04 A. Yes. 127:05 Q. And it can obtain photos and videos 127:06 from the device, right? 127:07 A. Yes. 127:08 Q. And take new photos, correct? 127:09 A. Yes. 127:10 Q. And it obtains location information, 127:11 is that right?	00:01:27	Gazneli4_30PM_v er1.77

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	127:12 A. Yes.		
	127:13 Q. And it had all those capabilities in		
	127:14 2018 and 2019?		
	127:15 A. Yes.		
	127:16 Q. Including as installed by the		
	127:17 Hummingbird vector, it would have all those		
	127:18 capabilities?		
	127:19 A. The only part which I am not sure		
	127:20 about it, about its support is intercepting calls.		
	127:21 Maybe it was able part of the time.		
128:17 - 129:03	Gazneli, Tamir 2024-09-04	00:01:06	Gazneli4_30PM_v er1.78
	128:17 Q. What is the anonymizing transmission		
	128:18 network that is used or that was used in		
	128:19 connection with Pegasus during the relevant		
	128:20 period?		
	128:21 A. In what level do you ask the		
	128:22 question? The technical parts or --		
	128:23 Q. How would you explain what it is?		
	128:24 A. It is -- I have explained this to		
	128:25 you. It is an infrastructure which is deployed at		
	129:01 every client site to ensure that it is possible to		
	129:02 trace back to an operating organization, thus		
	129:03 ensuring full deniability from that site.		
130:11 - 130:13	Gazneli, Tamir 2024-09-04	00:00:11	Gazneli4_30PM_v er1.79
	130:11 Q. What was NSO's role in establishing		
	130:12 an anonymizing transmission network for a		
	130:13 particular customer back in 2018/19?		
130:17 - 130:24	Gazneli, Tamir 2024-09-04	00:00:35	Gazneli4_30PM_v er1.80
	130:17 A. So as for the infrastructure which		
	130:18 is deployed on the customer side, it involves		
	130:19 purchases of infrastructure which are done by the		
	130:20 White Services teams and eventually deployed on		
	130:21 the target customers' ecosystem in order to enable		
	130:22 them to use the software.		
	130:23 Q. Would it also involve leasing		
	130:24 third-party servers?		
131:03 - 131:07	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.81
	131:03 A. It involves working with third-party		
	131:04 providers in order to get the infrastructure		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	131:05 required.		
	131:06 Q. And doing so in a way that could not		
	131:07 be traced back to NSO or the customer?		
131:11 - 131:17	Gazneli, Tamir 2024-09-04	00:00:22	Gazneli4_30PM_v er1.82
	131:11 A. As it says here, the goal is		
	131:12 deniability of the customer and includes the		
	131:13 deniability of the company.		
	131:14 Q. And the White Services team that you		
	131:15 mentioned, what is their role?		
	131:16 A. To make those purchases for		
	131:17 infrastructure in an anonymized way.		
131:21 - 131:23	Gazneli, Tamir 2024-09-04	00:00:05	Gazneli4_30PM_v er1.83
	131:21 (Exhibit 2017 marked for identification)		
 P44.2	131:22 I am showing you what has been marked as		
	131:23 Exhibit 2017. This is a Confluence document, is		
131:23 - 132:16	Gazneli, Tamir 2024-09-04	00:00:47	Gazneli4_30PM_v er1.84
	131:23 Exhibit 2017. This is a Confluence document, is		
	131:24 that right?		
	131:25 A. Yes.		
	132:01 Q. What is Confluence?		
	132:02 A. It is a software for documenting.		
 P44.2.3	132:03 Q. The document is dated January 25,		
	132:04 2018. Do you see that?		
	132:05 A. Yes.		
	132:06 Q. And it has a heading that is		
	132:07 partially redacted, "2.50", then a redaction and		
	132:08 then "Android". Do you see that?		
	132:09 A. Yes.		
	132:10 Q. Do you recognize this document?		
	132:11 A. Yes.		
	132:12 Q. What is it?		
	132:13 A. It is a release page that states		
	132:14 that a version is being released.		
	132:15 Q. A new version of Pegasus, correct?		
	132:16 A. Yes.		
137:24 - 139:09	Gazneli, Tamir 2024-09-04	00:01:48	Gazneli4_30PM_v er1.85
 Clear	137:24 Q. And so if at this point Pegasus 2.50		
	137:25 including Heaven was not yet clear to go to		
	138:01 customers, when was Heaven clear to go to		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	138:02 customers?		
	138:03 A. As I recall, I think around		
	138:04 April/May this was ready enough to be deployed.		
	138:05 Q. Around April or May 2018?		
	138:06 A. Yes. Just a second. No. It was		
	138:07 around October.		
	138:08 Q. October 2018?		
	138:09 A. Yes, ready for broad deployment.		
	138:10 Q. What do you mean by "broad		
	138:11 deployment"?		
	138:12 A. All customers could get the		
	138:13 solution.		
	138:14 Q. When was the first time, to your		
	138:15 knowledge, that any NSO customer was able to use a		
	138:16 version of Pegasus that included Hummingbird?		
	138:17 A. I don't recall the exact month for		
	138:18 that.		
	138:19 Q. But it would have been between		
	138:20 January and October?		
	138:21 A. Yes.		
	138:22 Q. When it says "The first 0 click's		
	138:23 installation vector for broad Android devices", is		
	138:24 it right that beyond this before this point others		
	138:25 had installation vectors for Android but they were		
	139:01 not broad?		
	139:02 A. No, we didn't have any solution at		
	139:03 all for Android.		
	139:04 Q. It includes "thanks for putting so		
	139:05 much effort to imagine, create and release this		
	139:06 complex version". Do you see that?		
	139:07 A. Yes.		
	139:08 Q. What were the efforts that went into		
	139:09 producing Heaven?		
139:13 - 139:21	Gazneli, Tamir 2024-09-04	00:00:21	Gazneli4_30PM_v er1.86
	139:13 A. I can answer from the R&D side.		
	139:14 Q. Mm hmm.		
	139:15 A. It is finding vulnerabilities,		
	139:16 building the installation chain and chaining		
	139:17 altogether to an installation vector of the agent.		
	139:18 Q. It notes that this is a significant		

Gazneli4_30PM_ver1



DESIGNATION	SOURCE	DURATION	ID
	139:19 milestone for Pegasus. Do you see that?		
	139:20 A. Yes.		
	139:21 Q. Do you agree with that?		
139:25 - 140:01	Gazneli, Tamir 2024-09-04	00:00:07	Gazneli4_30PM_v er1.87
	139:25 A. Any 0 click solution whatsoever is a		
	140:01 significant milestone for Pegasus.		
140:02 - 140:06	Gazneli, Tamir 2024-09-04	00:00:10	Gazneli4_30PM_v er1.88
	140:02 Q. When you refer to -- when I asked		
	140:03 you about the efforts that went into producing		
	140:04 Heaven you said you could answer on the R&D side,		
	140:05 the first thing you mentioned was finding		
	140:06 vulnerabilities. What did you mean by that?		
140:09 - 140:16	Gazneli, Tamir 2024-09-04	00:00:40	Gazneli4_30PM_v er1.89
	140:09 A. I would say that this domain		
	140:10 requires finding the flaws in the ecosystem and in		
	140:11 the services in order to be able to build the		
	140:12 installation floor, the installation vector, and		
	140:13 eventually deploy the agent.		
	140:14 Q. And with respect to Heaven, the		
	140:15 vulnerabilities that the team was working to find		
	140:16 were vulnerabilities in WhatsApp's ecosystem?		
140:19 - 140:20	Gazneli, Tamir 2024-09-04	00:00:04	Gazneli4_30PM_v er1.90
	140:19 A. The vulnerabilities in Heaven were		
	140:20 in WhatsApp client.		
142:18 - 145:13	Gazneli, Tamir 2024-09-04	00:04:55	Gazneli4_30PM_v er1.91
	142:18 Q. My fundamental question is how did		
	142:19 the R&D team at NSO go about finding		
	142:20 vulnerabilities in the WhatsApp client?		
	142:21 A. They researched the activity of the		
	142:22 WhatsApp client in order to find flaws and to		
	142:23 build the installation vectors which, as I said,		
	142:24 is built to eventually deliver the agent payload.		
	142:25 Q. How did the team research the		
	143:01 activity of the WhatsApp client?		
	143:02 A. What does the question refer to in		
	143:03 how?		
	143:04 Q. That is my question. How did they		
	143:05 do that? You said they researched the activity of		
	143:06 the WhatsApp client. How did they do that?		

DESIGNATION	SOURCE	DURATION	ID
143:07	A. So I will get back to the		
143:08	explanation about the ecosystem we built		
143:09	internally. We built internal ecosystem of		
143:10	WhatsApp server that enabled us internally to send		
143:11	messages between two peers between customer owned		
143:12	devices, and having this ability enables us to		
143:13	research the activity of the WhatsApp client.		
143:14	Q. How did you know how to build that		
143:15	internal ecosystem?		
143:16	A. What do you mean by how?		
143:17	Q. How did you determine what the		
143:18	characteristics of that internal ecosystem should		
143:19	be in order to operate like a WhatsApp client?		
143:20	A. We have the client and we have the		
143:21	server between them.		
143:22	Q. And so how do you go from having the		
143:23	client to building an ecosystem that replicates		
143:24	it?		
143:25	A. So as a researcher, especially in		
144:01	Android, you have the ability to gain the		
144:02	routabilities on any Android devices. These		
144:03	abilities are stated for anyone using the web.		
144:04	Whenever you have route access on a device, you		
144:05	have the ability to monitor the traffic that is in		
144:06	and out the monitored device, and then you have		
144:07	access to the traffic from peer to peer. Using		
144:08	this knowledge you can use it to build the		
144:09	ecosystem which is required for this activity.		
144:10	Q. Is there anything else that the NSO		
144:11	R&D team did to find vulnerabilities in the		
144:12	WhatsApp client?		
144:13	A. We, the R&D research group, used all		
144:14	the tools it should use in order to be able to		
144:15	find the vulnerabilities.		
144:16	Q. What are those tools?		
144:17	A. Basically, there are two types of		
144:18	tools, called IDA and JEB.		
144:19	Q. Can you spell those?		
144:20	A. I-D-A.		
144:21	Q. And what was the other?		
144:22	A. J-E-B.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	144:23 Q. And what is IDA?		
	144:24 A. These are tools available for		
	144:25 procurement -- anyone can buy it -- which enable		
	145:01 you to analyze code.		
	145:02 Q. What is the difference between IDA		
	145:03 and JEB?		
	145:04 A. IDA enables you to analyse native		
	145:05 code and JEB analyzes Java code.		
	145:06 Q. Other than using those two tools,		
	145:07 what else did the R&D team do to find		
	145:08 vulnerabilities in the WhatsApp client?		
	145:09 A. As I said before, it monitored the		
	145:10 transmission between peer to peer as for the		
	145:11 communication, in order to understand the		
	145:12 responses and the message content that should be		
	145:13 sent from side to side.		
146:13 - 146:14	Gazneli, Tamir 2024-09-04	00:00:06	Gazneli4_30PM_v er1.92
	146:13 Q. As part of this work did NSO		
	146:14 researchers reverse engineer any WhatsApp code?		
146:16 - 146:25	Gazneli, Tamir 2024-09-04	00:00:31	Gazneli4_30PM_v er1.93
	146:16 A. Do you want to define what reverse		
	146:17 engineering is?		
	146:18 Q. What do you understand reverse		
	146:19 engineering to mean?		
	146:20 A. I would say that using these tools I		
	146:21 talked about, IDA and JEB, the research group had		
	146:22 the ability to understand how the code functions,		
	146:23 some of the parts.		
	146:24 Q. Mm hmm. What do you understand		
	146:25 reverse engineering to mean?		
147:03 - 147:09	Gazneli, Tamir 2024-09-04	00:00:25	Gazneli4_30PM_v er1.94
	147:03 A. I would talk about the aim of this		
	147:04 activity, and the aim is to learn the mechanisms		
	147:05 and the way client functions.		
	147:06 Q. And that is something NSO's research		
	147:07 group did with respect to WhatsApp client, as part		
	147:08 of the development of the Hummingbird vectors?		
	147:09 A. Yes.		
152:24 - 153:02	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
 P60.2	152:24 Q. Let me show you what we will mark -- 152:25 I think we are up to 2033. 153:01 (Exhibit 2033 marked for identification) 153:02 This is Exhibit 2033. This is		er1.95
153:02 - 153:17	Gazneli, Tamir 2024-09-04	00:00:53	Gazneli4_30PM_v er1.96
 P60.2.1	153:02 This is Exhibit 2033. This is 153:03 a multipage document beginning on 153:04 NSO_WHATSAPP_00008957 through 8962. It has the 153:05 title at the top "Heaven OpSec." Do you recognize 153:06 Exhibit 2033? 153:07 A. Yes. 153:08 Q. What is it? 153:09 A. It is an OpSec document for Heaven 153:10 vector. 153:11 Q. What does that mean, an OpSec 153:12 document? 153:13 A. It is OpSec team's analysis results 153:14 and suggestions how will be the best in terms of 153:15 this vector to be developed and used. 153:16 Q. And concealed, right? 153:17 A. Yes.		
153:20 - 154:08	Gazneli, Tamir 2024-09-04	00:00:45	Gazneli4_30PM_v er1.97
	153:20 Q. Again I don't think the reporter got 153:21 your answer. You said "yes", right? 153:22 A. Yes. 153:23 Q. And so was this a document that was 153:24 prepared by the operational security team within 153:25 R&D? 154:01 A. Yes. 154:02 Q. Did you have any role in preparing 154:03 this document? 154:04 A. No. 154:05 Q. Do you know approximately when it 154:06 was prepared? 154:07 A. Not the exact date but if I remember 154:08 right it was around the beginning of 2018.		
154:17 - 155:03	Gazneli, Tamir 2024-09-04	00:00:23	Gazneli4_30PM_v er1.98
 P60.2.2	154:17 Q. The first one listed there says: 154:18 "Resources of value we want to protect." 154:19 The first one is:		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	154:20 "Exploits and techniques that are being 154:21 used as part of the installation vector. The most 154:22 important asset we want to protect, the WhatsApp 154:23 exploit." 154:24 Do you see that? 154:25 A. Yes. 155:01 Q. And that refers to the 0 click 155:02 WhatsApp exploit that was known at this time as 155:03 Heaven?		
155:06 - 155:09	Gazneli, Tamir 2024-09-04 155:06 A. At that particular time that was the 155:07 exploit. 155:08 Q. Why was the Heaven exploit the most 155:09 important asset that this team wanted to protect?	00:00:10	Gazneli4_30PM_v er1.99
155:12 - 156:02	Gazneli, Tamir 2024-09-04 155:12 A. Again, this is the OpSec team's 155:13 assessment of the specific capability, and he was 155:14 directed to assess the Heaven capability, and as 155:15 part of all the resources which are listed here, 155:16 and we can go over each and every one of them, 155:17 protecting the exploit is the most important in 155:18 this list. 155:19 Q. More important even than the 155:20 clients' identities? 155:21 A. Yes -- 155:22 Q. More important than target 155:23 awareness? 155:24 A. In order to be able to handle the 155:25 risks in terms of client's identity, so target 156:01 awareness, you wanted to start having the ability, 156:02 the vulnerability, so yes.	00:00:52	Gazneli4_30PM_v er1.100
157:07 - 157:13	Gazneli, Tamir 2024-09-04 157:07 Q. What is WIS? 157:08 A. This is the acronym of WhatsApp 157:09 installation server, but it means an Android 157:10 server which is responsible for installing the end 157:11 solution. 157:12 Q. And installing it by transmitting a 157:13 message through WhatsApp?	00:00:20	Gazneli4_30PM_v er1.101



Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
157:16 - 158:01	Gazneli, Tamir 2024-09-04 157:16 A. Installing it by sending the 157:17 required messages to the target's WhatsApp client. 157:18 Q. And you understand that those 157:19 WhatsApp messages travel through WhatsApp's 157:20 ecosystem? 157:21 A. Any message in the WhatsApp 157:22 ecosystem travels through WhatsApp's ecosystem. 157:23 Q. Including the ones that were being 157:24 sent as part of the Hummingbird installation 157:25 vectors, right? 158:01 A. Yes.	00:00:22	Gazneli4_30PM_v er1.102
158:14 - 158:18  P60.2.3	Gazneli, Tamir 2024-09-04 158:14 Q. It says: 158:15 "Fingerprint is done by sending a forged 158:16 request from a client that mimics a server 158:17 response to the target WA client." 158:18 What does that mean?	00:00:11	Gazneli4_30PM_v er1.103
158:21 - 158:22	Gazneli, Tamir 2024-09-04 158:21 A. As I read it, it means send specific 158:22 message from one client to the target client.	00:00:11	Gazneli4_30PM_v er1.104
159:12 - 159:13	Gazneli, Tamir 2024-09-04 159:12 Q. Okay. So what does "forged request" 159:13 mean?	00:00:02	Gazneli4_30PM_v er1.105
159:19 - 159:20	Gazneli, Tamir 2024-09-04 159:19 A. It says that it mimics servers 159:20 response to the client's target.	00:00:07	Gazneli4_30PM_v er1.106
159:24 - 160:06	Gazneli, Tamir 2024-09-04 159:24 Q. What does it mean that it mimics the 159:25 server response? 160:01 A. This is a response that the server 160:02 generates, and it mimics that message towards the 160:03 client, the target's client. 160:04 Q. So it sends a message that appears 160:05 to be a server response? 160:06 A. Yes.	00:00:25	Gazneli4_30PM_v er1.107
162:04 - 162:11	Gazneli, Tamir 2024-09-04 162:04 Q. And the forged request that is	00:00:26	Gazneli4_30PM_v er1.108

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	162:05 referred to there, that is the same thing as the		
	162:06 mimicked server response, or are those two		
	162:07 different things?		
	162:08 A. This is the same one.		
	162:09 Q. So it is a message sent by WIS that		
	162:10 appears to be legitimate WhatsApp traffic but is		
	162:11 not, right?		
162:14 - 162:21	Gazneli, Tamir 2024-09-04	00:00:19	Gazneli4_30PM_v er1.109
	162:14 A. This is legitimate by the target		
	162:15 that received it and by the ecosystem that		
	162:16 transferred the message from peer to peer.		
	162:17 Q. But it is not an actual response		
	162:18 from the WhatsApp server, right?		
	162:19 A. It could be.		
	162:20 Q. Right. It appears to be, right?		
	162:21 A. No, it could be.		
162:23 - 163:19	Gazneli, Tamir 2024-09-04	00:00:59	Gazneli4_30PM_v er1.110
	162:23 Q. So then I am going to have to go		
	162:24 back because you lost me. When it says it is a		
	162:25 forged request that mimics a server response, you		
	163:01 are saying that could be a legitimate WhatsApp		
	163:02 server response, so it is not forged or mimicked.		
	163:03 It actually could just be a WhatsApp server		
	163:04 response?		
	163:05 A. It is mimicked and forged in terms		
	163:06 of maybe sequence, maybe timing, maybe content,		
	163:07 but it for sure can be a valid response from the		
	163:08 server.		
	163:09 Q. Right, except that it doesn't		
	163:10 originate from the WhatsApp server. It originates		
	163:11 from WIS?		
	163:12 A. You stated before that everything is		
	163:13 transferred -- transformed throughout the WhatsApp		
	163:14 servers, so it practically originated from -- got		
	163:15 sent through and landed on the WhatsApp client, on		
	163:16 the target's device.		
	163:17 Q. Right, originating from WIS?		
	163:18 A. Yes, and transferring to WhatsApp		
	163:19 ecosystem.		
163:20 - 163:22	Gazneli, Tamir 2024-09-04	00:00:07	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	163:20 Q. But it is not a request that the 163:21 WhatsApp client, the standard WhatsApp client 163:22 would have the ability to send?		er1.111
163:25 - 164:09	Gazneli, Tamir 2024-09-04 163:25 A. We will have to discuss what is -- 164:01 who is using and what are the capabilities of 164:02 WhatsApp client. 164:03 Q. But I couldn't open up my WhatsApp 164:04 and send this forged request right now, could I? 164:05 A. No. 164:06 Q. So it is something that NSO, through 164:07 its R&D function, developed the capability to 164:08 transmit. 164:09 A. Yes.	00:00:31	Gazneli4_30PM_v er1.112
183:04 - 183:13	 P60.2.4 183:04 Q. And so it says: 183:05 "In order to attack we initiate a 183:06 WhatsApp voice call with target." 183:07 Do you see that? 183:08 A. Yes. 183:09 Q. And that is the first step of what 183:10 you call phase one? 183:11 A. Yes. 183:12 Q. And that WhatsApp voice call is 183:13 initiated from NSO's WIS. Is that right?	00:00:25	Gazneli4_30PM_v er1.113
183:16 - 184:13	 P60.2.5 183:16 A. NSO's WIS code is able to send 183:17 messages that initiates the WhatsApp voice call, 183:18 on the endpoint WhatsApp target, WhatsApp client. 183:19 Q. It continues: 183:20 "As part of the call, initiation 183:21 handshake between our WIS client and target's 183:22 WhatsApp client." 183:23 Let me pause there. What does that 183:24 refer to, "Initiation handshake between our WIS 183:25 client and target's WhatsApp client"? 184:01 A. As I said, this is part of protocol 184:02 messages which are required to initiate the 184:03 WhatsApp call. It is not a single message. It is 184:04 back and forth messages which are handshaked	00:01:14	Gazneli4_30PM_v er1.114

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	184:05 between the source and the target.		
	184:06 Q. And that occurs through the WhatsApp		
	184:07 servers?		
	184:08 A. As we said before, every		
	184:09 transmission between two peers have to be		
	184:10 transmitted through WhatsApp servers.		
	184:11 Q. Including this transmission that we		
	184:12 are talking about here?		
	184:13 A. Including this, yes.		
186:10 - 186:22	Gazneli, Tamir 2024-09-04	00:00:42	Gazneli4_30PM_v er1.115
	186:10 Q. You were going to answer. On the		
	186:11 source side, it is not a WhatsApp client, it is		
	186:12 the WIS which NSO created. Isn't that correct?		
	186:13 A. The messages are built and sent from		
	186:14 the WIS client. These messages have to be sent		
	186:15 from an application. Client is notified, which he		
	186:16 uses to connect to the application and sends the		
	186:17 messages through a real and active client.		
	186:18 Q. Through an active WhatsApp account?		
	186:19 A. Yes.		
	186:20 Q. And whose account would that be?		
	186:21 A. Accounts were established for the		
	186:22 customer.		
187:24 - 188:01	Gazneli, Tamir 2024-09-04	00:00:10	Gazneli4_30PM_v er1.116
	187:24 Q. And so the message is created by the		
	187:25 WIS but transmitted through that WhatsApp client?		
	188:01 A. Yes.		
188:02 - 188:11	Gazneli, Tamir 2024-09-04	00:00:27	Gazneli4_30PM_v er1.117
	188:02 Q. And when you said it has		
	188:03 connectivity, the WIS has connectivity to a		
	188:04 genuine WhatsApp client, what did you mean by		
	188:05 that?		
	188:06 A. I mean that it has to be -- it has		
	188:07 to have a way to connect the target and send the		
	188:08 message to the target.		
	188:09 Q. So the WIS is able to send the		
	188:10 message it created through that WhatsApp client?		
	188:11 A. Yes.		
188:12 - 188:25	Gazneli, Tamir 2024-09-04	00:00:38	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	188:12 Q. Got it. And that WhatsApp client on 188:13 the initiating side would be one that -- an 188:14 account that NSO created? 188:15 A. As part of deployment, each customer 188:16 has his own set of WhatsApp clients that were used 188:17 for this operation. 188:18 Q. Created by NSO, right? 188:19 A. Yes. 188:20 Q. Through the White Services team? 188:21 A. Yes. 188:22 Q. And those would be anonymized as 188:23 well? 188:24 A. Yes, as part of the operation 188:25 requirements for the customer to be anonymized.		er1.118
189:25 - 190:15  P60.2.6	Gazneli, Tamir 2024-09-04 189:25 Q. It says: 190:01 "As part of the call we add to a 190:02 specific field (property) of the messages request 190:03 payload that is named relay servers and usually 190:04 contains five constant IP addresses of relay 190:05 servers." 190:06 What does that mean? 190:07 A. As part of the initiation of the 190:08 WhatsApp voice call, the data that is transmitted 190:09 during the voice call is transmitted to relay 190:10 servers which are designed to transmit data from 190:11 peer to peer. What it states, that we had the 190:12 ability to add specific field to the property and 190:13 to the payload request sent, which is named relay 190:14 servers, which usually contains five constant IPs 190:15 and an additional one.	00:01:10	Gazneli4_30PM_v er1.119
191:07 - 192:15  P60.2.7	Gazneli, Tamir 2024-09-04 191:07 Q. In a normal WhatsApp communication, 191:08 there would only be the five relay servers. 191:09 Right? 191:10 A. Yes. 191:11 Q. That is what it means by "usually 191:12 has five relay servers", right? 191:13 A. Yes. 191:14 Q. And it continues:	00:01:32	Gazneli4_30PM_v er1.120

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	191:15 "When a standard WhatsApp client 191:16 initiates a voice call, it goes out with 5 IP 191:17 addresses." 191:18 And that is what you were referring to, 191:19 right? 191:20 A. Yes. 191:21 Q. So the message as sent from WIS was 191:22 different than what is called here as a 191:23 standard -- what would come from a standard 191:24 WhatsApp client, right? 191:25 A. A standard WhatsApp client would -- 192:01 as it states here, five IP addresses. 192:02 Q. And the message sent from WIS would 192:03 have six? 192:04 A. The message sent from WIS enforces 192:05 to add additional one. 192:06 Q. Sorry, enforces? 192:07 A. Yes, enforces to add to that list 192:08 additional one relay server -- 192:09 Q. Right, so the message sent by WIS is 192:10 different. It has six relay servers instead of 192:11 five, right? 192:12 A. Yes. 192:13 Q. What do you mean when you say it 192:14 enforces to add to this list one additional relay 192:15 server?		
192:18 - 193:01	Gazneli, Tamir 2024-09-04 192:18 Q. Is that what you said? I was not 192:19 sure I heard you correctly. Is the word 192:20 "enforces"? 192:21 A. I used the word enforces. What I 192:22 was talking about is -- it is read from the 192:23 written text, the usual at least contains five, 192:24 and then it says we had the ability to add one 192:25 additional relay servers list, which is forcing or 193:01 adding an additional one.	00:00:29	Gazneli4_30PM_v er1.121
195:19 - 196:01	Gazneli, Tamir 2024-09-04 195:19 Q. Let me ask it this way. What is 195:20 transmitted via that sixth relay server? 195:21 A. Additional messages.	00:00:32	Gazneli4_30PM_v er1.122

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	195:22 Q. From where?		
	195:23 A. Generated, as we said, from the WIS		
	195:24 server through the source WhatsApp client it is		
	195:25 connected to to transmit the messages to the		
	196:01 target WhatsApp client.		
199:03 - 199:10	Gazneli, Tamir 2024-09-04	00:00:24	Gazneli4_30PM_v er1.123
	199:03 Q. You don't know. Okay. This whole		
	199:04 installation flow, it requires the target to have		
	199:05 a WhatsApp client, is that right?		
	199:06 A. Yes.		
	199:07 Q. So it operates by sending a message		
	199:08 to the target's WhatsApp client, meaning their		
	199:09 WhatsApp application on their mobile device?		
	199:10 A. Yes.		
201:18 - 201:25	Gazneli, Tamir 2024-09-04	00:00:26	Gazneli4_30PM_v er1.124
 P60.3.1	201:18 Q. So what does that mean when it says		
	201:19 "We send an encrypted message to the target. The		
	201:20 message is encrypted in a non-standard way that is		
	201:21 unknown to the target's WhatsApp client"?		
	201:22 A. As I understand it, we use		
	201:23 encryption method that the target cannot detect as		
	201:24 a valid one or possible one and therefore discards		
	201:25 the message.		
205:04 - 205:07	Gazneli, Tamir 2024-09-04	00:00:11	Gazneli4_30PM_v er1.125
	205:04 to your answer but let me ask it. That feature		
	205:05 here, that it only sends specific messages, that		
	205:06 is not the only way the WIS is different from a		
	205:07 legitimate subscriber of WhatsApp, is it?		
205:09 - 205:18	Gazneli, Tamir 2024-09-04	00:00:40	Gazneli4_30PM_v er1.126
	205:09 A. So my answer was WIS server		
	205:10 implements and enables to craft end messages and		
	205:11 content that is required for the installation		
	205:12 phase or gaining remote code execution on the		
	205:13 target's WhatsApp client.		
	205:14 Q. And those messages are different		
	205:15 than the messages that would be sent by a regular		
	205:16 WhatsApp subscriber, right?		
	205:17 A. If by "regular" you mean one that		
	205:18 holds device in hand, the answer is yes.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
206:12 - 208:05	Gazneli, Tamir 2024-09-04	00:02:38	Gazneli4_30PM_v er1.127
 P60.3.2	<p>206:12 Q. The next section down there is sort</p> <p>206:13 of a header there that says "Threat Actors</p> <p>206:14 Involved". Do you see that?</p> <p>206:15 A. Yes.</p> <p>206:16 Q. And that refers to parties that</p> <p>206:17 might compromise the secrecy of the WhatsApp</p> <p>206:18 installation vector?</p> <p>206:19 A. I would have to read it.</p> <p>206:20 Q. Go for it. Go ahead.</p> <p>206:21 A. Okay.</p> <p>206:22 Q. So "threat actors" there refers to</p> <p>206:23 parties that might compromise the operational</p> <p>206:24 security of the installation vector. Is that</p> <p>206:25 right?</p> <p>207:01 A. As titled maybe, but I don't think</p> <p>207:02 the content is relevant for this headline.</p> <p>207:03 Q. So maybe it refers to -- what do you</p> <p>207:04 understand "threat actors" to mean, as NSO and Q's</p> <p>207:05 corporate representative?</p> <p>207:06 A. Threat actors is as you said, but I</p> <p>207:07 said that the content of the paragraph doesn't</p> <p>207:08 necessarily address the "threat actors" as the</p> <p>207:09 headline states.</p> <p>207:10 Q. But we agree that threat actors</p> <p>207:11 means parties that might compromise operational</p> <p>207:12 security?</p> <p>207:13 A. Yes.</p> <p>207:14 Q. Meaning parties that might detect</p> <p>207:15 and seek to prevent the exploit?</p> <p>207:16 A. Yes.</p> <p>207:17 Q. And one of those is WhatsApp itself,</p> <p>207:18 right?</p> <p>207:19 A. Yes.</p> <p>207:20 Q. In fact, there are three identified;</p> <p>207:21 first WhatsApp, then WhatsApp anti-spamming model</p> <p>207:22 and measures and then target. Right?</p> <p>207:23 A. Yes.</p> <p>207:24 Q. That is what is identified as threat</p> <p>207:25 actors to operational security in this document?</p> <p>208:01 A. Yes.</p>		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	208:02 Q. And you understood during your time		
	208:03 working on the Hummingbird vectors that WhatsApp		
	208:04 would try to shut down the installation vectors if		
	208:05 they were detected. Right?		
208:08 - 208:12	Gazneli, Tamir 2024-09-04	00:00:11	Gazneli4_30PM_v er1.128
	208:08 A. WhatsApp would shut down or close		
	208:09 any vulnerability it knew about or exists.		
	208:10 Q. Including the vulnerabilities that		
	208:11 were being exploited for the Hummingbird vectors,		
	208:12 right?		
208:15 - 209:05	Gazneli, Tamir 2024-09-04	00:01:01	Gazneli4_30PM_v er1.129
	208:15 A. If it discovered it, yes.		
	208:16 Q. And so that discovery by WhatsApp is		
	208:17 something that the OpSec team worked to avoid. Is		
	208:18 that right?		
	208:19 A. OpSec team, as I said at the		
	208:20 beginning document, are placing new suggestions		
	208:21 that from their point of view would like to be		
	208:22 implemented. Whether any suggestion here is		
	208:23 implemented or not, it really depends on the		
	208:24 capability and whether it can be applied or not.		
	208:25 Q. But my question was more general,		
	209:01 not about specific suggestions, that discovery of		
	209:02 the exploits by WhatsApp is something that the		
	209:03 OpSec team worked to avoid. Isn't that right?		
	209:04 A. They suggested ways so that the		
	209:05 capability would prolong much longer time.		
209:22 - 210:02	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.130
 P60.3.3	209:22 Q. Sure. So under the WhatsApp section		
	209:23 of actors it says "We know WhatsApp has spam		
	209:24 solving measures". Do you see that?		
	209:25 A. Yes.		
	210:01 Q. And what does that refer to, spam		
	210:02 solving measures?		
210:05 - 210:12	Gazneli, Tamir 2024-09-04	00:00:21	Gazneli4_30PM_v er1.131
 P60.3.4	210:05 A. As it states afterward: "Users can		
	210:06 block people from messaging when something fishy		
	210:07 is noticed about them."		
	210:08 Q. And that is your understanding of		



Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	210:09 spam solving measures?		
	210:10 A. As far as I understand it, it talks		
	210:11 about the ability WhatsApp added to client to		
	210:12 block specific users.		
212:06 - 212:17	Gazneli, Tamir 2024-09-04	00:00:29	Gazneli4_30PM_v er1.132
	212:06 Q. Okay. But what we have in this		
	212:07 section here, these are not suggestions from the		
	212:08 OpSec team. These are observations about		
	212:09 WhatsApp's anti-spamming measures, correct?		
	212:10 A. Observations, and his understanding		
	212:11 of the features.		
	212:12 Q. Understanding of WhatsApp's		
	212:13 anti-spamming features, right?		
	212:14 A. Yes.		
	212:15 Q. And the purpose of reciting them		
	212:16 here was to formulate a strategy for how those		
	212:17 features could be avoided. Isn't that right?		
212:20 - 213:03	Gazneli, Tamir 2024-09-04	00:00:36	Gazneli4_30PM_v er1.133
	212:20 A. I would say these are his		
	212:21 understandings how these mechanisms work in order		
	212:22 to be taken under consideration during the		
	212:23 installation flow implementation.		
	212:24 Q. In order to avoid detection, right?		
	212:25 A. This could be understandings that		
	213:01 may even relate to not avoid measures but to even		
	213:02 be able to finish and complete the installation		
	213:03 flow successfully.		
213:11 - 213:12	Gazneli, Tamir 2024-09-04	00:00:04	Gazneli4_30PM_v er1.134
	213:11 The whole purpose -- this is an		
	213:12 Operation Security document, right?		
213:15 - 214:01	Gazneli, Tamir 2024-09-04	00:00:25	Gazneli4_30PM_v er1.135
	213:15 A. This is a draft.		
	213:16 Q. Prepared by -- you identified the		
	213:17 individual. A member of the Operation Security		
	213:18 team, right?		
	213:19 A. Yes.		
	213:20 Q. And you said the purpose of this is		
	213:21 suggestions for operational security, right. That		
	213:22 was your testimony, right?		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	213:23 A. Yes.		
	213:24 Q. Right. And suggestions for		
	213:25 operational security means ways to maintain the		
	214:01 secrecy of this exploit, right?		
214:04 - 214:04	Gazneli, Tamir 2024-09-04	00:00:01	Gazneli4_30PM_v er1.136
	214:04 A. No.		
214:05 - 214:15	Gazneli, Tamir 2024-09-04	00:00:20	Gazneli4_30PM_v er1.137
	214:05 Q. What does operational security mean?		
	214:06 A. To maintain its operation.		
	214:07 Q. Maintain its operation?		
	214:08 A. Mm hmm.		
	214:09 Q. And maintaining its operation		
	214:10 requires maintaining its secrecy?		
	214:11 A. Also.		
	214:12 Q. As part of maintaining its		
	214:13 operation, because I think you testified you		
	214:14 understood if WhatsApp detected the exploit it		
	214:15 would seek to close the vulnerability. Correct?		
214:18 - 214:18	Gazneli, Tamir 2024-09-04	00:00:01	Gazneli4_30PM_v er1.138
	214:18 A. Yes.		
214:19 - 214:22	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.139
	214:19 Q. And the purpose in that context of		
	214:20 identifying and reciting WhatsApp's anti-spamming		
	214:21 measures is to avoid those measures interfering		
	214:22 with the operation. Isn't that right?		
214:25 - 215:11	Gazneli, Tamir 2024-09-04	00:00:45	Gazneli4_30PM_v er1.140
	214:25 A. As I said before, this is that		
	215:01 team's or employee's understanding of the measures		
	215:02 and his wishes on how he sees the operational		
	215:03 security should be taken under consideration in		
	215:04 the vector, whether it can be or cannot be taken		
	215:05 under consideration in this specific vector.		
	215:06 (Inaudible) is a matter of question.		
	215:07 Q. But you agree that the reason that		
	215:08 observations about WhatsApp's anti-spamming		
	215:09 measures are included in this operation security		
	215:10 document is so that to avoid those measures		
	215:11 compromising the secrecy of the operation?		
215:14 - 215:14	Gazneli, Tamir 2024-09-04	00:00:02	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	215:14 Q. Isn't that why this is in here?		er1.141
215:17 - 215:24	Gazneli, Tamir 2024-09-04	00:00:24	Gazneli4_30PM_v
	215:17 A. This is here in order to whoever		er1.142
	215:18 builds the operational -- the installation		
	215:19 vectors, the research team would take under		
	215:20 consideration all the relevant measures that can		
	215:21 be met during the implementation of the exploit or		
	215:22 the vector.		
	215:23 Q. To avoid detection and compromise		
	215:24 the operation, right?		
216:02 - 216:05	Gazneli, Tamir 2024-09-04	00:00:16	Gazneli4_30PM_v
	216:02 A. I wouldn't say to avoid. There are		er1.143
	216:03 sections here which are relevant not for		
	216:04 avoidance, as I said, even enabling the completion		
	216:05 of the installation flow.		
228:22 - 228:24	Gazneli, Tamir 2024-09-04	00:00:07	Gazneli4_30PM_v
 P60.4.1	228:22 which is that this section, "Threat Landscape",		er1.144
	228:23 identifies aspects of the exploit that could lead		
	228:24 to detection risk. Is that right?		
229:02 - 229:23	Gazneli, Tamir 2024-09-04	00:01:08	Gazneli4_30PM_v
	229:02 A. As far as I understand it, it states		er1.145
	229:03 or lists the parts in the flow which are most		
	229:04 exposed.		
	229:05 Q. To the risk of compromising		
	229:06 operational security, right?		
	229:07 A. Yes.		
 P60.4.2	229:08 Q. And the first one mentioned there is		
	229:09 "non-standard requests sent by the WIS server and		
	229:10 and routed through WA servers", and it continues:		
	229:11 "Assuming the requests that are sent by		
	229:12 the WIS, their flow traffic rate and sources may		
	229:13 be inspected by WhatsApp, content may not be		
	229:14 inspected due to end to end encryption."		
	229:15 Do you see that?		
	229:16 A. Yes.		
	229:17 Q. And so again you would agree that		
	229:18 non-standard requests are sent in connection		
	229:19 with -- let me start over.		
	229:20 You agree that in connection with the		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	229:21 Hummingbird vectors, non-standard requests were 229:22 sent by the WIS server and routed through WhatsApp 229:23 servers?		
230:01 - 230:18	Gazneli, Tamir 2024-09-04 230:01 A. I would say that WIS server creates 230:02 messages, that some of them may be non-standard 230:03 and routed through (inaudible) servers, and those 230:04 servers had all the right and ability to decide 230:05 whether to route them or not. 230:06 Q. And when you say all the right, are 230:07 you talking in legal terms? 230:08 A. No. 230:09 Q. And it is identifying the risk that 230:10 the requests might be inspected by WhatsApp, 230:11 right, as a threat to operational security? 230:12 A. It is a fact. 230:13 Q. The second risk identified as the 230:14 non-standard activity of the WIS client doesn't 230:15 send standard data to WhatsApp, sends only very 230:16 specific requests, and that was another aspect of 230:17 the exploit that risked compromising operational 230:18 security?	00:00:59	Gazneli4_30PM_v er1.146
230:21 - 231:10	Gazneli, Tamir 2024-09-04 230:21 A. This is one of the aspects of the 230:22 WIS client. As we said, it only implements 230:23 specific requests and messages relevant for the 230:24 installation flow. 230:25 Q. And the third risk identified is 231:01 that "target's device WhatsApp crash logs sent to 231:02 WhatsApp servers for analysis". Do you see that? 231:03 A. Yes. 231:04 Q. And what do you understand that to 231:05 mean? 231:06 A. If the standard procedure 231:07 application crashes, it sends the crash logs 231:08 content files to the application specific servers. 231:09 Q. And that also created a risk of 231:10 WhatsApp detecting the exploit?	00:00:52	Gazneli4_30PM_v er1.147
 P60.4.3			
231:13 - 231:25	Gazneli, Tamir 2024-09-04 231:13 A. If somehow the installation flow may	00:00:39	Gazneli4_30PM_v er1.148

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	231:14 lead to a WhatsApp client crash on the target		
	231:15 device, then according to the statement and the		
	231:16 standing of how things in this domain work the		
	231:17 WhatsApp crash would be uploaded to the servers.		
	231:18 Q. Creating a risk of detection, right?		
	231:19 A. That depends on the content of the		
	231:20 message -- of the crash and the ability of the		
	231:21 other side to understand what is in the crash.		
	231:22 Q. But potentially creating a risk of		
	231:23 detection, creating a risk of potential detection,		
	231:24 right?		
	231:25 A. Yes.		
235:19 - 235:22	Gazneli, Tamir 2024-09-04	00:00:10	Gazneli4_30PM_v er1.149
	235:19 Q. But you agree that some of these are		
	235:20 suggestions for how to avoid WhatsApp's security		
	235:21 mechanisms as the author understood those security		
	235:22 mechanisms?		
235:25 - 237:06	Gazneli, Tamir 2024-09-04	00:02:36	Gazneli4_30PM_v er1.150
	235:25 A. Some of them, if those specific		
	236:01 mechanisms were implemented on the server side,		
	236:02 may potentially detect unusual activity on the		
	236:03 servers.		
	236:04 Q. And these are suggestions for how to		
	236:05 avoid such detection, right?		
	236:06 A. I wouldn't say avoid but minimize		
	236:07 the risk.		
	236:08 Q. And were certain of these		
	236:09 countermeasures implemented?		
	236:10 A. I would have to read through.		
	236:11 Q. Take a moment. I know it is two		
	236:12 pages of countermeasures here, but go ahead.		
	236:13 A. Are you asking about the whole		
	236:14 section?		
	236:15 Q. Yes, the countermeasures and		
	236:16 mitigations starts on page 8960 and continues on		
	236:17 to 961.		
	236:18 A. For now I can address the		
	236:19 fingerprint stage if you want and then I can		
	236:20 continue.		
	236:21 Q. You can answer just yes or no, were		


Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	236:22 any of the suggested counter measures in the 236:23 fingerprint section implemented by NSO? 236:24 A. For any the answer is yes, but in 236:25 order to answer exactly which and how many, I 237:01 would have to read it all. 237:02 Q. Fair enough. So let's drop that. 237:03 Would you agree, as a general matter, that NSO 237:04 took steps to minimize the risk of detection by 237:05 WhatsApp of the Hummingbird vectors? 237:06 A. Yes.		
243:10 - 244:21	Gazneli, Tamir 2024-09-04	00:01:48	Gazneli4_30PM_v er1.151
 P62.2.1	243:10 Q. Let me show you what has been marked 243:11 as Exhibit 2035, another Confluence document with 243:12 the header 2.52 Android. Do you see that on the 243:13 Bates NSO_WHATSAPP ending 288? 243:14 A. Yes. 243:15 (Exhibit 2035 marked for identification) 243:16 Q. We looked in another exhibit at a 243:17 document that concerned the release of Pegasus 243:18 2.50. Do you recall that? 243:19 A. Yes. 243:20 Q. And that Pegasus 2.50 included 243:21 Heaven for the first time. Do you recall that? 243:22 A. Yes. 243:23 Q. Do you recognize this document, 243:24 Exhibit 2035? 243:25 A. Yes. 244:01 Q. And 2.52 refers to a version of 244:02 Pegasus, is that right? 244:03 A. Yes. 244:04 Q. And it notes that 2.52, Pegasus 2.52 244:05 is officially approved for production, right? 244:06 A. Yes.		
 P62.2.2	244:07 Q. And it notes that among the 244:08 enhancements included for Heaven specifically is 244:09 "support for the most updated WhatsApp Version 244:10 2.18.46 that was released by WhatsApp less than a 244:11 week ago". Do you see that? 244:12 A. Yes. 244:13 Q. And so this reflects NSO working to		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	<p>244:14 quickly update the Heaven vector to respond to a</p> <p>244:15 software update by WhatsApp?</p> <p>244:16 A. WhatsApp versions are released --</p> <p>244:17 were released every two weeks, so according to</p> <p>244:18 what it states -- it doesn't state it has to be</p> <p>244:19 updated. Maybe no change was required. Support</p> <p>244:20 doesn't mean that any change is required</p> <p>244:21 because --</p>		
245:18 - 247:01	<p>Gazneli, Tamir 2024-09-04</p> <p>245:18 Q. What is the process to update</p> <p>245:19 Pegasus to reflect WhatsApp updates?</p> <p>245:20 A. It depends on the version.</p> <p>245:21 Q. Which team of individuals are</p> <p>245:22 responsible or were responsible in the relevant</p> <p>245:23 time period for updating the Hummingbird exploits</p> <p>245:24 to respond to WhatsApp updates?</p> <p>245:25 A. For all that was required or related</p> <p>246:01 to the vulnerabilities part, it is the research</p> <p>246:02 team.</p> <p>246:03 Q. For which part?</p> <p>246:04 A. Vulnerabilities part.</p> <p>246:05 Q. Is the research team?</p> <p>246:06 A. Yes.</p> <p>246:07 Q. And what process would they</p> <p>246:08 undertake to update the Hummingbird vectors in</p> <p>246:09 response to WhatsApp updates?</p> <p>246:10 A. Download the new version to the</p> <p>246:11 internal ecosystem, execute the installation flow</p> <p>246:12 and, if it works right, just update the version</p> <p>246:13 numbers supported and if not then to be adjusted</p> <p>246:14 accordingly to the changes that were done in the</p> <p>246:15 application.</p> <p>246:16 Q. And so even if no change was</p> <p>246:17 required you would update the version number of</p> <p>246:18 Pegasus?</p> <p>246:19 A. Yes.</p> <p>246:20 Q. And would IDA and JEB be used as</p> <p>246:21 part of that updating process?</p> <p>246:22 A. It depends what was updated and what</p> <p>246:23 has to be done in order to adjust to it.</p>	00:01:39	Gazneli4_30PM_v er1.152

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	246:24 Q. So with respect to some updates, 246:25 yes? 247:01 A. Some updates.		
247:04 - 247:17  Clear	Gazneli, Tamir 2024-09-04 247:04 Q. Let's do tab 32, please. By the 247:05 way, Mr. Gazneli, we talked earlier about the 247:06 information that Pegasus allows a customer to 247:07 access from a target device. Do you recall that 247:08 generally? 247:09 A. Yes. 247:10 Q. Is that generally the same 247:11 information that you could access if you had a 247:12 password to the device? 247:13 A. Password in terms of -- 247:14 Q. Mm hmm. 247:15 A. -- physical access to the device? 247:16 Q. Yes? 247:17 A. Yes.	00:00:54	Gazneli4_30PM_v er1.153
248:25 - 249:03	Gazneli, Tamir 2024-09-04 248:25 Q. You understand you have been 249:01 designated, subject to your counsel's objections, 249:02 as to the impact of the April 2018 WhatsApp update 249:03 on the relevant spyware?	00:00:10	Gazneli4_30PM_v er1.156
249:09 - 249:13	Gazneli, Tamir 2024-09-04 249:09 MR. AKROTIRIANAKIS: The designation is 249:10 "Efforts to develop new covert lawful intercept 249:11 technologies during the time period at issue in 249:12 this case that could be used with respect to 249:13 Android devices."	00:00:18	Gazneli4_30PM_v er1.157
249:20 - 249:23	Gazneli, Tamir 2024-09-04 249:20 MR. PEREZ-MARQUES: So you are 249:21 designated, subject to your counsel's objections, 249:22 on topic 28, right? 249:23 A. Yes.	00:00:05	Gazneli4_30PM_v er1.158
250:01 - 250:03	Gazneli, Tamir 2024-09-04 250:01 MR. PEREZ-MARQUES: You are also 250:02 designated on topic 29, defendant's efforts to 250:03 circumvent the April 2018 WhatsApp update?	00:00:07	Gazneli4_30PM_v er1.159
250:04 - 250:12	Gazneli, Tamir 2024-09-04	00:00:25	Gazneli4_30PM_v

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	250:04 MR. AKROTIRIANAKIS: The designation in 250:05 respect of Exhibit 29 is defendant's efforts to 250:06 develop new covert lawful intercept technologies 250:07 during the time period at issue in this case that 250:08 could be used with respect to Android devices. It 250:09 is the same designation. 250:10 MR. PEREZ-MARQUES: Okay, and so that is 250:11 a yes, you are designated on that topic? 250:12 A. Yes.		er1.160
250:13 - 251:01	Gazneli, Tamir 2024-09-04 250:13 Q. And so do you recall in May 2018 the 250:14 vectors losing their functionality, the 250:15 Hummingbird vectors? 250:16 A. As I said, if you wanted to 250:17 introduce me the exact change that was done then I 250:18 can address the question, but as I said, version 250:19 was released every two weeks, so whether it is 250:20 relevant to the exploitation or not, things may be 250:21 changed and need to be addressed, so I cannot 250:22 recall the exact specific changes that happened on 250:23 that version. 250:24 Q. Is it right to assume that most 250:25 WhatsApp updates did not compromise the 251:01 functionality of the vectors?	00:00:41	Gazneli4_30PM_v er1.161
251:04 - 251:06	Gazneli, Tamir 2024-09-04 251:04 A. No. 251:05 Q. No? Many of them did? 251:06 A. Yes.	00:00:04	Gazneli4_30PM_v er1.162
251:18 - 251:24	Gazneli, Tamir 2024-09-04 251:18 Q. In those instances up to the time 251:19 period at least of May 2019, when a WhatsApp 251:20 software update compromised the functionality of 251:21 the Hummingbird vectors, NSO was able to find a 251:22 way to restore their functionality. Isn't that 251:23 right? 251:24 A. Yes.	00:00:21	Gazneli4_30PM_v er1.163
252:11 - 253:18	Gazneli, Tamir 2024-09-04 252:11 (Exhibit 2037 marked for identification.) 252:12 This will be 2037, which is a WhatsApp	00:01:23	Gazneli4_30PM_v er1.164

 Clear

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
🔗 P65.2	252:13	chat between various participants on July 9, 2018.	
	252:14	Do you see that?	
🔗 P65.3.1	252:15	A. Okay, yes.	
	252:16	Q. The second page includes a message,	
	252:17	the third one down, from Yossi Monsingo. Do you	
	252:18	see that?	
	252:19	A. Yes.	
	252:20	Q. Do you know who that is?	
	252:21	A. Yes.	
	252:22	Q. Who is that?	
	252:23	A. I don't recall his exact position at	
	252:24	that same time but he worked in customer facing or	
	252:25	NOC.	
	253:01	Q. Like customer support of some kind?	
	253:02	A. Yes.	
	253:03	Q. Not a member of the R&D team?	
	253:04	A. No.	
	253:05	Q. And he writes -- his message	
	253:06	includes an update that WhatsApp released a new	
	253:07	version two days ago that is not yet supported but	
253:08	probably tomorrow R&D will release a new package.		
253:09	Do you see that?		
253:10	A. Yes.		
253:11	Q. And that again reflects NSO updating		
253:12	its installation vectors in response to software		
253:13	updates from WhatsApp?		
253:14	A. Yes.		
253:15	Q. And the two or three day timeframe,		
253:16	is that typical of how long it would take the R&D		
253:17	department to update the vectors in response to a		
🗑️ Clear	253:18	WhatsApp update.	
253:21 - 255:04	Gazneli, Tamir 2024-09-04	00:01:47	Gazneli4_30PM_v er1.165
🔗 P34.2.1	253:21	A. No.	
	253:22	Q. How long would be typical?	
	253:23	A. It depends on the changes.	
	253:24	Q. What would the range be?	
	253:25	A. It may be from one day to half a	
	254:01	year.	
	254:02	Q. This was previously marked as	
254:03	Exhibit 2007, which is a WhatsApp message between		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
P34.2.2	254:04	various participants on December 5, 2018.	
	254:05	A. Yes.	
	254:06	Q. It states in the second message	
	254:07	down:	
	254:08	"WhatsApp has made changes in their	
	254:09	servers that currently fail all installations and	
	254:10	can cause crashes that risk the Hummingbird	
	254:11	vector."	
	254:12	Do you see that?	
	254:13	A. Yes.	
	254:14	Q. And do you recall in December 2018 a	
	254:15	WhatsApp update that caused all Hummingbird	
	254:16	installations to crash?	
	254:17	A. Yes.	
	254:18	Q. What do you recall about that?	
	254:19	A. I recall that that specific change	
	254:20	was around our ability to end that specific relay	
	254:21	server that we talked about previously, and	
	254:22	controlling the target's WhatsApp client to choose	
	254:23	that specific relay server for communication.	
254:24	Q. And the reference here, when it says		
254:25	"can cause crashes that risk the Hummingbird		
255:01	vector", that relates back to what we saw in the		
255:02	OpSec document about crashes potentially		
255:03	generating logs that would be reviewed by		
255:04	WhatsApp?		
255:07 - 255:12	Gazneli, Tamir 2024-09-04	00:00:19	Gazneli4_30PM_v er1.166
	255:07 A. This relates to crashes that after		
	255:08 the change may occur on the target's devices.		
	255:09 Q. And the reason they would risk the		
	255:10 Hummingbird vector is potentially, among other		
	255:11 reasons, because they could be reviewed by		
	255:12 WhatsApp, the crash logs?		
255:15 - 255:17	Gazneli, Tamir 2024-09-04	00:00:09	Gazneli4_30PM_v er1.167
	255:15 A. They are uploaded to the server of		
	255:16 the vendor and whether they review them or not is		
	255:17 their decision to make.		
256:16 - 258:12	Gazneli, Tamir 2024-09-04	00:02:22	Gazneli4_30PM_v er1.168
	256:16 Q. Did the NSO R&D team in fact work on		
	256:17 a solution to restore the Hummingbird vectors		

DESIGNATION	SOURCE	DURATION	ID
	256:18	after this December 2018 update?	
	256:19	A. Yes.	
	256:20	Q. And was that successful, that	
	256:21	effort?	
	256:22	A. That was Eden.	
	256:23	Q. So Heaven was made not operational	
	256:24	by the December 2018 update. Is that right?	
	256:25	A. Yes.	
	257:01	Q. And subsequently NSO released Eden?	
	257:02	A. Yes.	
 P64.2.1	257:03	Q. If we look at -- I am going to show	
	257:04	you another document. This is 2038.	
	257:05	(Exhibit 2038 marked for identification)	
	257:06	This is a WhatsApp chat on January 15,	
	257:07	2019 among various participants. In the first	
 P64.2.2	257:08	message someone named Gilad says in the last line:	
	257:09	"Bottom line, Eden works fine on S3 and	
	257:10	can be demonstrated" with a sort of smiley	
	257:11	emoticon. Do you see that?	
	257:12	A. Yes.	
	257:13	Q. What is S3.	
	257:14	A. Sales 3.	
	257:15	Q. What is sales 3?	
	257:16	A. It is an infrastructure for making	
	257:17	demonstrations for our services.	
	257:18	Q. And is this the approximate timing	
	257:19	of when Eden became ready for use at least for	
	257:20	demonstration purposes.	
	257:21	A. For demonstration, yes.	
	257:22	Q. And then when did Eden go live for	
	257:23	use by customers?	
	257:24	A. If I remember right, about a month	
	257:25	after.	
	258:01	Q. So this reflects NSO's fix or	
	258:02	response to the problem that was created by the	
	258:03	December 2018 update?	
	258:04	A. This is we doing our job to	
	258:05	delivering the customers the software they needed.	
	258:06	Q. Right. So after the December 2018	
	258:07	update, NSO customers couldn't use the 0 click	
	258:08	Android installation vectors, right?	

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	258:09 A. Right.		
	258:10 Q. And Eden, once it was released,		
	258:11 allowed them to do so again, right?		
	258:12 A. Right.		
258:13 - 258:16	Gazneli, Tamir 2024-09-04	00:00:08	Gazneli4_30PM_v er1.169
	258:13 Q. And between Heaven and Eden was		
	258:14 there any other -- was there any 0 click Android		
	258:15 installation vector in operation?		
	258:16 A. No.		
262:02 - 262:24	Gazneli, Tamir 2024-09-04	00:01:15	Gazneli4_30PM_v er1.170
	262:02 (Exhibit 2039 marked for identification.)		
 P66.2	262:03 Q. This is Exhibit 2039, which is a		
	262:04 WhatsApp chat from May 12, 2019. Again various		
 P66.3.1	262:05 participants. In the second page Tomer Timor has		
	262:06 a message. Who is Mr. Timor?		
	262:07 A. He was, if I am right, at that stage		
	262:08 presales employee.		
	262:09 Q. Presales?		
	262:10 A. Yes.		
	262:11 Q. He says in the sort of third		
	262:12 paragraph down:		
	262:13 "So bottom line, Eden has finished its		
	262:14 duty with us as a patch was done on the server		
	262:15 side with the application it works with."		
	262:16 Do you recall this event?		
	262:17 A. Yes.		
	262:18 Q. And what does that refer to? What		
	262:19 is the event that is being described here?		
	262:20 A. Closure of ability to trigger the		
	262:21 vulnerability on the target's WhatsApp client.		
	262:22 Q. So this reflect WhatsApp's		
	262:23 remediation of the exploit that is described in		
	262:24 the complaint?		
263:02 - 263:19	Gazneli, Tamir 2024-09-04	00:00:48	Gazneli4_30PM_v er1.171
	263:02 A. It refers to changes that were done,		
	263:03 whether on the server side and the client side, in		
	263:04 order to prevent us from triggering the		
	263:05 vulnerabilities.		
	263:06 Q. And so after this point, after that		
	263:07 update in May 12 or around May 12, 2019, was NSO		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
P66.3.2	263:08	able to use Eden after that point?	
	263:09	A. No.	
	263:10	Q. In the next paragraph down he said:	
	263:11	"I heard some sales managers talking in	
	263:12	a dramatic way. Your job is to make sure they	
	263:13	remember that along the years NSO has proven time	
	263:14	after time that one of its biggest value is the	
	263:15	ability to 'survive' this harsh environment of the	
	263:16	cat and mouse game."	
	263:17	Do you see that.	
263:18	A. Yes.		
263:19	Q. What does that refer to?		
263:22 - 264:05	Gazneli, Tamir 2024-09-04	00:00:41	Gazneli4_30PM_ver1.172
263:22	A. This is a domain that you are not in		
263:23	control how long your capability will prolong at		
263:24	least for total control, and that is why he quotes		
263:25	cat and mouse game. The ecosystem that you were		
264:01	working or acting makes changes eventually, forces		
264:02	you to adjust it.		
264:03	Q. So NSO designs an exploit, the		
264:04	exploit gets shut down. NSO designs another,		
264:05	right?		
264:08 - 264:09	Gazneli, Tamir 2024-09-04	00:00:02	Gazneli4_30PM_ver1.173
264:08	Q. Is that generally the cat and mouse		
264:09	game?		
264:12 - 264:19	Gazneli, Tamir 2024-09-04	00:00:26	Gazneli4_30PM_ver1.174
264:12	A. This is the domain that you have to		
264:13	stay -- to keep and find new vulnerabilities after		
264:14	the systems get changed.		
264:15	Q. That is just inherent to the domain		
264:16	in which NSO operates, right?		
264:17	A. Yes.		
264:18	Q. When something gets shut down, you		
264:19	have to work to develop another?		
264:22 - 266:07	Gazneli, Tamir 2024-09-04	00:02:02	Gazneli4_30PM_ver1.175
264:22	A. Eventually you have to provide --		
264:23	you want to provide the 1 click and 0 click		
264:24	solutions to customers, and it doesn't relate to a		
264:25	specific service or application.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	265:01 Q. And at this point in May 2019 when		
	265:02 the WhatsApp update prevented Eden from working		
	265:03 did NSO have any 0 click Android solutions?		
	265:04 A. No.		
	265:05 Q. Did the R&D group subsequently find		
	265:06 another 0 click installation vector for Android		
	265:07 devices?		
	265:08 A. Yes.		
	265:09 Q. What was that?		
	265:10 A. ERISED.		
	265:11 Q. When was ERISED approved for		
	265:12 production?		
	265:13 A. I don't recall the exact date.		
	265:14 Q. If we back to the exhibit we were		
	265:15 looking at, in that same message from Mr. Timor he		
	265:16 says:		
 P66.3.3	265:17 "R&D are working hard on different		
	265:18 directions. Hopefully we will have good news		
	265:19 soon, but please remember that our technological		
	265:20 status is still great as we as a company have the		
	265:21 resources to find something new in a relatively		
	265:22 short time."		
	265:23 Do you agree with his statement, sir?		
	265:24 A. He was optimistic.		
	265:25 Q. Is it accurate that at this point,		
	266:01 in May 2019, NSO's R&D group was working hard on		
	266:02 potential solutions to restore 0 click capability?		
	266:03 A. As a research group and development		
	266:04 team, you constantly work on research in order to		
	266:05 find possible ways, rapid solutions. As I		
	266:06 explained before, eventually we are producing a		
	266:07 product for customers.		
266:14 - 266:22	Gazneli, Tamir 2024-09-04	00:00:57	Gazneli4_30PM_v
 Clear	266:14 Q. Do you remember when ERISED began to		er1.176
	266:15 be used by customers, approximately?		
	266:16 A. It is really not an exact time. I		
	266:17 couldn't tell.		
	266:18 Q. What is your best estimate?		
	266:19 A. If I recall right, it was close to		
	266:20 the end of the year.		

Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	266:21 Q. So late 2019?		
	266:22 A. If I recall right.		
267:02 - 267:04	Gazneli, Tamir 2024-09-04	00:00:07	Gazneli4_30PM_v er1.177
	267:02 Q. And up to that date in May 2020, did		
	267:03 ERISED remain in use?		
	267:04 A. Yes.		
267:05 - 267:10	Gazneli, Tamir 2024-09-04	00:00:34	Gazneli4_30PM_v er1.178
	267:05 Q. So as to whether NSO has ever		
	267:06 stopped using ERISED, I assume that is a question		
	267:07 you are not willing to answer?		
	267:08 A. Regarding ERISED, the		
	267:09 vulnerabilities in ERISED was not in WhatsApp at		
	267:10 all and that part was eventually closed.		
267:22 - 268:06	Gazneli, Tamir 2024-09-04	00:00:21	Gazneli4_30PM_v er1.179
	267:22 Q. But did it also work by transmitting		
	267:23 WhatsApp messages?		
	267:24 A. It was our decision whether to		
	267:25 trigger it using WhatsApp messages or not.		
	268:01 Q. So it could be triggered using		
	268:02 WhatsApp messages?		
	268:03 A. Yes.		
	268:04 Q. And were those WhatsApp messages		
	268:05 sent via WhatsApp servers?		
	268:06 A. Yes.		
269:19 - 269:23	Gazneli, Tamir 2024-09-04	00:00:22	Gazneli4_30PM_v er1.180
	269:19 Q. Just to be clear, after WhatsApp		
	269:20 closed the vulnerability that was being exploited		
	269:21 by Eden in May 2019, NSO worked on developing a		
	269:22 new 0 click exploit that also worked, at least in		
	269:23 part, by transmitting WhatsApp messages. Yes?		
270:01 - 270:05	Gazneli, Tamir 2024-09-04	00:00:18	Gazneli4_30PM_v er1.181
	270:01 A. We researched for a new solution.		
	270:02 We found vulnerability in the system which was		
	270:03 specific for Samsung and we decided to implement		
	270:04 it and build installation flow based on WhatsApp		
	270:05 application.		
270:06 - 270:10	Gazneli, Tamir 2024-09-04	00:00:14	Gazneli4_30PM_v er1.182
	270:06 Q. And after WhatsApp closed the		
	270:07 vulnerability that was being exploited by Eden,		


Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
	270:08 NSO succeeded in developing a new 0 click 270:09 installation vector that operated in part through 270:10 delivering WhatsApp messages, yes?		
270:13 - 270:24	Gazneli, Tamir 2024-09-04 270:13 A. We found additional vulnerability 270:14 which we were able to build installation for using 270:15 that. 270:16 Q. And that installation vector, 270:17 ERISED, which used WhatsApp servers and WhatsApp 270:18 messages remained in use by NSO customers as of at 270:19 least May 2020. Is that right? 270:20 A. Yes. 270:21 Q. So, with this lawsuit pending, NSO 270:22 was actively making available to its customers a 0 270:23 click exploit that involved the transmission of 270:24 messages over WhatsApp servers?	00:00:40	Gazneli4_30PM_v er1.183
271:01 - 271:08	Gazneli, Tamir 2024-09-04 271:01 A. I don't recall the exact time that 271:02 the lawsuit was filed. 271:03 Q. It was filed in October 2019. So 271:04 with that context, with this lawsuit pending NSO 271:05 was actively making available to its customers a 0 271:06 click exploit that involved the transmission of 271:07 messages over WhatsApp servers. Correct? 271:08 A. Yes.	00:00:23	Gazneli4_30PM_v er1.184
278:16 - 278:23	Gazneli, Tamir 2024-09-04 278:16 Q. And defendants needed WhatsApp 278:17 credentials to gain access to the WhatsApp 278:18 servers. Isn't that right? 278:19 A. We need WhatsApp credentials in 278:20 order to connect to the real WhatsApp environment 278:21 as a legitimate client. 278:22 Q. As if you were a legitimate client? 278:23 A. Yes.	00:00:22	Gazneli4_30PM_v er1.185
299:21 - 300:23	Gazneli, Tamir 2024-09-04 299:21 Q. The call offer, at least for some of 299:22 the Hummingbird vectors, manipulated the 299:23 connecting tone DESC field. Is that right? 299:24 A. Yes.	00:01:23	Gazneli4_30PM_v er1.186


Gazneli4_30PM_ver1

DESIGNATION	SOURCE	DURATION	ID
299:25	Q. And is that true of all three of the		
300:01	Hummingbird vectors?		
300:02	A. No.		
300:03	Q. Which ones is it true of?		
300:04	A. For Heaven and Eden.		
300:05	Q. And who at defendants came up with		
300:06	the idea to manipulate that particular field?		
300:07	A. The research team.		
300:08	Q. When did defendants come up with		
300:09	that idea?		
300:10	A. During the research efforts that		
300:11	were done as part of the vulnerability research		
300:12	and the exploitation research.		
300:13	Q. And roughly what was the time period		
300:14	when that work was being done?		
300:15	A. Beginning of 2018 or end of 2017.		
300:16	Q. And defendants, as part of at least		
300:17	the Eden and Heaven vectors, would insert a bash		
300:18	script in the connecting tone desc field?		
300:19	A. Yes.		
300:20	Q. And WhatsApp users using the		
300:21	official WhatsApp client app could not use the		
300:22	connecting tone desc field. Is that right?		
300:23	A. Right.		

P's Narrowed	01:31:32
D's Counters	00:09:36
TOTAL RUN TIME	01:41:08

 Documents linked to video:

- P34
- P44
- P59
- P60
- P62
- P63
- P64

 P65
P66