(21)

Defendant's witness testimony [Garuda] For Court's Use

Black Case No. P3370/2566

Red Case No.

Civil Court

6 September B.E. 2567 (2024)

Civil Procedure

	Mr. Jatupat Boonpattararaksa	Plaintiff
Between		
	N.S.O. GROUP TECHNOLOGIES LTD.	Defendant

I, Witness, have sworn in and testify that:

1. I, Professor Yuval Elovici
2. Date of birth: ________ Age: 58 years
3. Occupation: Professor at Ben Gurion University of the Negev, head of Cyber Security Research Center.
4. -
5. Involvement with litigants: none.

The witness continued to state:

As I am an Israeli national, I cannot testify in Thai and require an interpreter appointed by the defendant. I will testify in English with an interpreter to translate to Thai. Ms. Auruphan Suwanprasob is the appointed interpreter.

Responding to The Defendant's Lawyer's Examination:

I hold a bachelor's degree in mathematics and a master's degree in the field of electrical engineering. I also hold a Ph.D. in Information Systems as shown in documentary evidence Lor.11. I previously worked as a Major General. And at the same time, I studied for a doctoral degree in information systems. After that, I started working at Ben Gurion University of the Negev.

I collaborated with the German company named Doi Telecom, which later established the Cybersecurity Research Center at Ben Gurion University of the Negev. I teach information security and applied cryptography courses for master's degree students. I am an advisor to students in the master's program. Currently, there are 25 students who have graduated with Doctoral degrees, and 7 of whom are members and work across various universities.

My background of educational and work history is documented in documentary evidence Lor.12. The defense lawyer showed the witness a PowerPoint presentation on the screen, corresponding to documentary evidence Lor.14.

The witness testified that the introduction explains who I am. Page 3 covers the history and origin of cyberattacks. Identifying the origin of a cyberattack is difficult, and it is not 100% certain that there is an attacker. The primary reason is that attackers use sophisticated techniques to conceal their identity. At the very least, what I know is that attackers often employ the same technique, which is launching attacks to make it appear as if they were perpetrated from another country. This leads to misunderstandings about the origin of the attack. The attackers mimic the attack patterns to create confusion and mislead others into believing that the attack originated from a different country.

The important factor is the backdoor in the software called a "zero-click" exploit. The attacker might find this vulnerability and write code to exploit the backdoor to their advantage.

In slide 4, corresponding to documentary evidence Lor.14, the translation page No. 4, The plaintiff's allegation that their mobile device was attacked between June and July 2021 claims that the device was infiltrated by Pegasus software. Therefore, I would like to first explain the challenges and origins of the surveillance involved.

The method used by the attackers involves deliberately embedding their attack tools into the target's system or devices. This tactic is intended to mislead, making it appear as though the attack originated from another individual. To illustrate, it is akin to a thief breaking into a house and leaving behind a glass with someone else's fingerprints on it.

If attackers gain access to a system, they can alter all the data within it, such as timestamps and other evidentiary materials in the target's system, including LOG. The plaintiff generally described how their mobile phone was analyzed. From the plaintiff's claim, I am unable to find any details on the analysis conducted by Citizen Lab or any other organization, regarding their specific methodologies. What I do know is that MVT was used.

The only evidence I have seen is the MVT tool developed by Amnesty International. Amnesty International employed methodologies similar to those used by Citizen Lab or other organizations, but there was no examination of the plaintiff's mobile phone. I rely on the information provided by Amnesty International that the MVT tool was used. The MVT tool is the only tool I obtained through the internet. The tool I examined is the MVT tool, which is significant.

The MVT tool is designed to check if a phone has been compromised by malware. The MVT tool is available on the GitHub website, which is accessible to the public for download. Once downloaded, the MVT can be used to analyze whether the phone has been infected or not. The MVT file contains indicators, known as IOCs (Indicators of Compromise). Someone might claim to have specific forensic evidence that can be used to identify the attacker, such as the MVT tool, which is akin to a pregnancy test. This tool can confirm whether there is a pregnancy or not, but it cannot determine who the father is.

Documentary Evidence Lor.14, translation page no.4, The witness explained that the procedure for using the MVT involves extracting data from the mobile phone. Afterward, MVT tests the data in the phone against files called Stix Format, which contain indicators of vulnerabilities to determine whether the mobile phone has been compromised. The MVT tool will clearly synthesize which IOCs (Indicators of Compromise) or vulnerabilities are found in the mobile phone data, which is forensic evidence.

Firstly, the documents attached to the complaint, according to the Citizen Lab report, indicate that Citizen Lab used its methodology to analyze the Pegasus software, as referenced in documentary evidence Jor.41. After reading it, it's quite astonishing (sarcastically) that, if it were me, I wouldn't have written it that way.

According to documentary evidence Jor.41, on page 28, which is highlighted with a yellow marker. The witness read the mentioned text and testified that, after reading it, they questioned, "How could such a conclusion be reached?" I would like to provide an example: If someone were to use Pegasus software to send a link to a criminal or a pedophile, and those individuals did not open the link but forwarded it to someone else, resulting in that person who opened the link becoming infected with spyware. It is very easy to falsify or make it appear as though it is Pegasus software.

Secondly, the translation on page 9 of documentary evidence Lor.14. The method used to determine the origin of an attack and identify the attacker can never be 100% certain. For example, in the same way as with pregnancy, a test can confirm whether someone is pregnant, and you can use a DNA test to prove who the father is. DNA testing is a method with a very high degree of certainty in establishing paternity.

I demonstrate that the method being used is not comparable to what I have described. It is not equivalent to DNA testing.

On page 9, an experiment was conducted using the MVT tool on a file containing IOCs to check whether the mobile phone had Pegasus software. A mobile phone was used, and IOCs were added into the phone without infecting it with Pegasus spyware. The phone was then analyzed using MVT, and the MVT indicated that the phone had been attacked by Pegasus software, even though no Pegasus software was actually used. When compared to a pregnancy test, if there is no result indicating pregnancy, it cannot tell who the father is.

The issue that arises is that the method used to test the attack on the plaintiff's mobile phone makes it quite easy to falsify the origin. This leads to errors, where one looks at the IOC file, observes what has been added, and wrongly attributes the attack to another individual.

The final point concerns the lack of evidence. Even though there are numerous reports and documents attached to the complaint, none of these documents or pieces of evidence provide a detailed analysis of what was found on the plaintiff's mobile phone. I have conducted tests using MVT, as detailed in Appendix A of my document, which is the logs.

I conducted tests using MVT, which should have generated logs, but they do not appear as shown in the plaintiff's documents. If we consider that there are no logs, even as an expert, I am unable to prove or determine what was done to the plaintiff's mobile phone.

The conclusion on page 11 highlights that it is easy to accuse or blame others for being responsible. The testing method is unreliable and cannot verify accuracy because there are no logs or records. Therefore, it is impossible to confirm or prove the correctness or incorrectness of the results.

The defense lawyer presented the witness with documentary evidence Lor.10, and the witness testified that the report stated that the same method was used in the system attack.

Zero-day exploitation is the use of Zero-day. It is not necessarily the case that only one organization would be aware of this; multiple organizations or agencies could also know about it and take advantage of it. Additionally, other attackers might use the same method.

Zero-day exploits are vulnerabilities in a system that are not known to the general public. For example, it's like a small window on the roof of a house that only a few people may know about, while others might be unaware of its existence and that it can be used to gain entry into the house.

Zero-day exploits and N-day or One-day are different. One-day refers to when knowledge of a vulnerability has been publicly disclosed, meaning everyone is aware of it. On the first day of discovery, it is known as a "One-day" exploit, and by the next day, it becomes "Two-day," continuing to "N-day" until the vulnerability is finally patched or closed.

From One-day to during N-day, there is a vulnerability that attackers can exploit. Some attackers, smarter than others, might know about it before it is known as N-day. If the N-day is not reached, or if the software company has not yet patched the vulnerability, during this time, attackers can exploit the software or take advantage of the vulnerability.

Responding to the Plaintiff's Lawyer's Cross-Examination

The plaintiff's lawyer asked whether the witness had ever worked for a company that developed spyware. The witness responded that they had never done so. The plaintiff's lawyer asked whether the witness had known the defendant prior to being contacted to testify in this case. The witness responded that they had only heard of the defendant through the news.

The plaintiff's lawyer asked whether the witness was already aware that the defendant's company produces spyware, and specifically spyware used for surveillance purposes. The witness testified that the purpose of the defendant's product is to assist in law enforcement efforts against terrorists or pedophiles, cases that cannot be addressed effectively through other means.

The plaintiff's lawyer asked whether the company must implement measures to prevent the use of its product on individuals who are not terrorists or involved in serious crimes, such as pedophiles. The witness testified that, to their knowledge, the defendant does not control how the product is used.

The plaintiff's lawyer asked whether the witness was aware that the defendant had been accused of human rights violations globally through the use of Pegasus software, including by the European Council. The witness testified that they had read about it but did not know the details of the complaints.

The plaintiff's lawyer asked whether the development of Pegasus spyware requires a system to prevent the detection of attack traces or fingerprints of the spyware. The witness testified that they disagreed with the term "spyware," stating that it is a tool used for lawful data collection by government agencies but acknowledged that it cannot prevent attacks. For example, if I were a company that manufactures and sells guns, I wouldn't be able to prevent someone from using the gun to shoot someone.

The plaintiff's lawyer asked whether Pegasus is designed to be difficult to detect. The witness testified that spyware is a tool for lawful data collection (lawful interception) and is designed to evade detection when being monitored by law enforcement agencies.

The plaintiff's lawyer asked whether the sale of Pegasus requires approval from the Israeli Ministry of Defense. The witness testified that, to their knowledge, this is correct but added that I am a technical expert and requested not to be asked questions unrelated to technical matters.

The plaintiff's lawyer asked whether the witness had tested the MVT tool from Amnesty International, as referenced in documentary evidence Lor.13. The witness testified that Amnesty International developed the MVT tool and made it available for anyone to download and use.

The plaintiff's lawyer asked whether the version of the MVT tool was the 2021 version. The witness confirmed this was correct, as stated in documentary evidence Lor.13, point 3, which clearly indicated that the 2021 version was used. The witness also emphasized that the version was not the issue.

The plaintiff's lawyer asked whether documentary evidence Lor.13, points 9 and 9.2, pertain to the testing of the Pegasus version that involves clicking a link. The witness testified that this is correct. Citizen Lab claims that a link was copied and resulted in infection, and point 9.2 states that the infection was successful, causing the tested phone (in the United States) to become infected. The Pegasus link was sent to UAE activist Davis Mansour. [TRANSLATOR NOTE: VERBATIM]

The plaintiff's lawyer asked whether the report in documentary evidence L.13 aligns with the document in documentary evidence Jor.41, page 28, and inquired if it pertains to an attack in 2016. The witness testified that this is correct.

The plaintiff's lawyer asked whether Pegasus spyware was developed to be a zero-click exploit in 2019. The witness testified that this is possible, but they do not know for certain. They also mentioned that both link-based and link-free methods could potentially be used simultaneously.

The plaintiff's lawyer asked whether the examination of the plaintiff's mobile phone would involve a link or not. The witness testified that they do not know, as they have never received the plaintiff's mobile phone for inspection.

The plaintiff's lawyer presented the witness with documentary evidence Lor.13, Appendix A, page 4, and asked whether the phone the witness examined was an iPhone 14 running iOS 16.6. The witness testified that this is correct.

The plaintiff's lawyer then asked whether the plaintiff in this case would be using the same iOS phone. The witness responded that this is not the issue because what needs to be proven is the methodology. I stated that I cannot examine the plaintiff's phone, so I cannot verify the actual phone of the plaintiff.

The plaintiff's lawyer asked the witness to refer to documentary evidence Lor.13, page 7, point 11.6, and inquired whether IOCs or Indicators of Compromise, if disclosed by a company that has investigated the attack by Pegasus spyware—such as Citizen Lab or Amnesty International—could be used by the producers to develop weaknesses in their own Pegasus spyware. The witness testified that it is possible that this could be correct, but there must be evidence proving the methods used by those organizations. Simply stating that there has been an attack is insufficient; there must be supporting evidence. The witness acknowledged that Amnesty International has disclosed IOCs but noted that there are no reports. However, they are confident that everyone uses the IOCs and that this information can be downloaded by anyone, with ongoing updates.

The plaintiff's lawyer asked whether the witness, in being confident that others use the same information, has ever personally contacted Citizen Lab, Amnesty International, or any other organizations. The witness testified that he has never contacted these organizations. These organizations conceal or keep hidden the methods used in their testing processes.

The plaintiff's lawyer asked whether, if these organizations disclosed their testing methods or revealed all IOCs, the defendant could use that information to develop spyware to make it harder to detect. The witness testified that if the phone data were extracted and tested against the IOCs, even if the IOCs were not disclosed, if there had been an attack using Pegasus, the defendant would likely be aware that others know the detection methods. Therefore, the company would probably seek ways to modify its own software.

Amnesty International will update the list of IOCs and has published articles. Even if the IOCs are disclosed and the company is aware that its software is being detected, it would still need to develop or update its own software accordingly.

The plaintiff's lawyer asked the witness whether they were aware that the process of testing to determine if something has been falsified as Pegasus is a method that cannot be disclosed and is not accessible to the general public. The witness testified that without knowledge of computers, it cannot be done. However, if someone is in the industry, such as a software developer, they would be able to do so.

The plaintiff's lawyer asked whether, in documentary evidence Lor.13, paragraph 1, the witness did not conduct the experiment themselves. The witness testified that this is correct and that an engineer performed the experiment for them.

The plaintiff's lawyer asked whether the testing in Appendix A of documentary evidence Lor.13 was conducted on a phone that had not been attacked by Pegasus spyware. The witness testified that this is correct.

The plaintiff's lawyer asked whether, typically, a device that has been compromised by Pegasus spyware would show signs of tampering. The witness testified that they do not know because they did not conduct the examination.

The plaintiff's lawyer asked how the examination of the plaintiff's device is conducted according to documentary evidence Jor.42, including the methods, steps, and details involved. The witness testified that they did not know. They added that simply answering yes or no would be insufficient. From the plaintiff's documents, it is understood that Amnesty International uses the same methods, and it is presumed that similar methods must have been applied to the plaintiff's mobile phone as well.

The plaintiff's lawyer asked whether the witness had previously testified in other courts in Hungary and Poland that the defendant used Pegasus spyware on victims utilizing the MVT method, and whether the witness had ever given testimony in those cases. The witness testified that they had never done so.

The plaintiff's lawyer asked whether the witness had ever written an article or academic work arguing against the MVT. The witness testified that they had never done so but mentioned that they have conducted research on mobile phone examinations.

The plaintiff's lawyer asked whether the witness had ever examined a mobile phone that had been attacked by Pegasus spyware. The witness testified that they had never done so.

The plaintiff's lawyer asked whether the witness had ever detected a device that had been compromised by Pegasus spyware, similar to what was reported in documentary evidence L.13. The witness testified that they had not. They explained that the experiment detailed in documentary evidence L.23 involved testing the framework of the organization to evaluate the reliability of the MVT test results.

The plaintiff's lawyer asked whether documentary evidence L.13 includes a comparison between the actual Pegasus spyware and the results of the examination of false Pegasus spyware. The witness testified that they could not confirm whether such a comparison was made. They explained that the testing conducted as per documentary evidence L.13 was to determine whether the MVT tool could easily deceive the system.

The plaintiff's lawyer asked whether documentary evidence Lor.13 had undergone any checks or peer review by other computer scientists. The witness testified that it had not.

The plaintiff's lawyer asked the witness whether, according to documentary evidence Lor.10, page 2, the examination of the attack was conducted from November 2023 to July 2024. The witness testified that those dates are as stated. The lawyer then asked whether the report was generated in August 2024, to which the witness replied that it was correct. The lawyer further inquired if this report was produced after the plaintiff was attacked in 2020. The witness confirmed that this was true, stating that it serves to prove the principle.

The plaintiff's lawyer asked whether documentary evidence Lor.10, pages 2 and 3, paragraph one, describes a watering hole attack. The witness testified that this is possible. The lawyer then asked whether a watering hole attack targets a website, which is different from attacking the plaintiff's phone. The witness responded that this may be the case, but they do not know for certain.

The plaintiff's lawyer asked whether the examination to determine if Pegasus spyware was genuinely attacking and whether there was actual tampering would be credible only if conducted on the victim's phone or data from the victim's phone. The witness testified that they do not know.

The plaintiff's lawyer asked whether the examination in documentary evidence Lor.13 was conducted solely using a program and did not involve the plaintiff's phone or data from the plaintiff's phone. The witness testified that this is correct, as the plaintiff's phone was not available for testing.

The plaintiff's lawyer asked whether the methods and the document in documentary evidence Lor.13, as well as the witness's examination, have not been certified by any computer authorities or computer experts. The witness testified that this is irrelevant and not substantial enough to warrant an answer.

Responding to the Defendant's Lawyer's Re-direct Examination:

According to documentary evidence Lor.10, it was only recently published, which relates to what I have testified from the beginning regarding the reuse of vulnerabilities and methodologies among various organizations, as well as the perpetrators in the public sector or different companies. The tools used for lawful data collection also utilize the same methods to exploit vulnerabilities.

The report in documentary evidence Lor.10, which details the testing conducted during the time specified in documentary evidence Lor.10, raises the claim that what is stated in the report, and if one were to look back into the past, asserting that the events that occurred in the past are not true would be quite absurd.

Regarding documentary evidence Lor.10, pages 2 to 3, the first paragraph discusses the watering hole attack and mentions the sharing of knowledge within the data community, indicating that this is an event that has occurred in the past. Companies that collect data and comply with the law, such as the defendant, as well as cybercriminals or perpetrators in the public sector, are involved in this context.

There are individuals who can identify vulnerabilities that are sold on the dark market, with many customers purchasing and using them for attacks. What follows is often the initial capture of the use of such vulnerabilities. The attackers themselves carry out the actions but may try to make it appear as if others are responsible, leading to confusion and misattribution regarding the source of the attack (Domain Attribution).

A watering hole is a type of vulnerability used to attack websites. This method can be linked to mobile phones as one example of an attack used by various attackers. I do not know why this method is specifically called a "watering hole."