(๒๑)
คำเบิกความพยานจำเลย (นำ)

สำหรับศาลใช้

คดีหมายเลขดำที่ พ๓๓๗๐/๒๕๖๖
คดีหมายเลขแดงที่

ศาลแพ่ง

วันที่ ๖ เดือน กันยายน พุทธศักราช ๒๕๖๗

ความแพ่ง

นายจตุภัทร์ บุญภัทรรักษา โจทก์

ระหว่าง

บริษัท เอ็นเอสโอ กรุ๊ป เทคโนโลยี จำกัด (N.S.O. GROUP TECHNOLOGIES LTD.) จำเลย

ข้าพเจ้าพยานได้สาบานตนแล้ว ขอให้คำเบิกความว่า

๑. ข้าพเจ้า ศาตราจารย์ ยูวัล เอลโลวิช
๒. เกิดวันที่ ..... เดือน ..... พ.ศ. อายุ ๕๘ ปี
๓. ตำแหน่งหรืออาชีพ ศาตราจารย์ที่มหาวิทยาลัยเบนกูเรียน หัวหน้าศูนย์วิจัยความปลอดภัยทางไซเบอร์
๔. ตั้งบ้านเรือนอยู่ ๖๕๓ เบียร์เชวา ๘๔๑๐๕ อิสราเอล
๕. เกี่ยวพันกับคู่ความ ไม่เกี่ยวข้อง

และขอให้คำเบิกความต่อไปว่า พยานเป็นชาวอิสราเอลเบิกความเป็นภาษาไทยไม่ได้ ต้องใช้ล่ามโดยฝ่ายจำเลยจัดหามาเอง โดยพยานเบิกความเป็นภาษาอังกฤษผ่านล่ามภาษาอังกฤษ นางสาวอุรุพรรณ สุวรรณประสพ ได้สาบานตัวแล้ว

ตอบทนายจำเลยถาม

ข้าฯ จบชั้นปริญญาตรีสาขาคณิตศาสตร์และปริญญาโททางด้านวิทยาศาสตร์วิศวกรรมไฟฟ้า ระดับปริญญาเอกระบบสารสนเทศ ปรากฏตามปริญญาดุษฎีบัณฑิตที่ทนายจำเลยให้ดูอ้างส่งหมาย ล.๑๑

ข้าฯ เคยทำงานเป็นทหารระดับนายพลชั้นพลตรี ในขณะเดียวกันข้าฯ ก็ศึกษาในระดับชั้นปริญญาเอกด้านระบบสารสนเทศ จากนั้นได้เข้าทำงานมหาวิทยาลัยเบนกูเรียน ตอนเริ่มแรกได้

/ร่วมมือกับ...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

ร่วมมือกับบริษัทเยอรมันชื่อ ดอย เทเลคอม จากนั้นได้ก่อตั้งศูนย์วิจัยความปลอดภัยไซเบอร์ มหาวิทยาลัยเบนกูเรียน

ข้าฯ สอนวิชาความปลอดภัยทางสารสนเทศ วิชาเข้ารหัสประยุกต์ หลักสูตรสำหรับนักศึกษาปริญญาโท

ข้าฯ เป็นอาจารย์ที่ปรึกษาให้กับนักศึกษาระบบชั้นปริญญาเอก มีนักศึกษา ๒๕ คน ที่จบการศึกษาระดับปริญญาเอกไปแล้วและมี ๗ คนที่เป็นสมาชิกและทำงานในมหาวิทยาลัยต่าง ๆ

ประวัติเกี่ยวกับการศึกษาและการทำงานของข้าฯ ปรากฏตามเอกสารหมาย ล.๑๒

หนึ่งในที่ปรึกษาจำเลยในคดีนี้ติดต่อข้าฯ ให้ทำความเห็นและมาเบิกความที่ศาล

ข้าฯ ให้ความเห็นปรากฏตามรายงานเอกสารหมาย ล.๑๓

ทนายจำเลยให้พยานดู Power Point ผ่านหน้าจอประกอบเอกสารหมาย ล.๑๔ พยานเบิกความว่า บทนำอธิบายว่าข้าฯ เป็นใคร หน้าที่ ๓ เป็นประวัติความเป็นมาและที่มาของการโจมตีทางไซเบอร์ การระบุที่มาของการโจมตีทางไซเบอร์เป็นเรื่องที่ยากที่จะแน่ใจ ๑๐๐ เปอร์เซ็นต์ ได้ว่ามีผู้โจมตี เหตุผลหลักคือ ผู้โจมตีจะใช้เทคนิคที่ซับซ้อนเพื่อซ่อนตัวตนของผู้โจมตี อย่างน้อยสิ่งที่ข้าฯ ทราบ ผู้โจมตีจะใช้เทคนิคเดียวกัน คือการโจมตีให้เห็นว่าถูกกระทำโดยประเทศอื่น ทำให้เกิดความเข้าใจผิดเกี่ยวกับที่มาของการโจมตี เป็นการเลียนแบบ Pattern หรือรูปแบบของการโจมตีเพื่อจะทำให้เกิดการสับสนและเข้าใจผิดว่าเป็นการโจมตีจากประเทศอื่น

ผู้โจมตีซึ่งเป็นอาชญากรทางไซเบอร์ หรือผู้โจมตีที่มาจากรัฐ (State actor) ใช้เทคนิคเดียวกัน คือ หาช่องโหว่ใน Software ที่จะสามารถใช้ประโยชน์ได้ (Exploit) คือการเข้าระบบโดยไม่ได้รับอนุญาตจากผู้ใช้

ยกตัวอย่างเช่น สมมุติว่าบ้านมีหน้าต่างเล็ก ๆ บนหลังคา และไม่มีใครรู้ว่ามีทางเข้าจากหน้าต่างเล็ก ๆ ที่อยู่บนหลังคา จากนั้นก็มีผู้จู่โจมตีเข้ามาในบ้านทางหน้าต่างดังกล่าว

/สิ่งสำคัญ...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

สิ่งสำคัญก็คือ ช่องโหว่ของ Software ที่เรียกว่า ซีโรเดย์ ผู้โจมตีก็อาจจะรู้ถึงช่องโหว่ดังกล่าว ผู้โจมตีที่มีความรู้เกี่ยวกับซีโรเดย์และสามารถเขียนโค้ดขึ้นมาเพื่อใช้ประโยชน์ช่องโหว่ (Exploit) นั้นได้

สไลด์แผ่นที่ ๔ ตรงกับหมาย ล.๑๔ คำแปลหน้าที่ ๔ ข้อกล่าวอ้างของโจทก์ที่ว่ามือถือของโจทก์ถูกโจมตีในเดือนมิถุนายนถึงกรกฎาคม ๒๕๖๔ กล่าวอ้างว่า มีการเจาะเข้าสู่อุปกรณ์โดย Pegasus Software ข้าฯ ขออธิบายถึงความท้าทายและที่มาของการสอดแนมก่อน

วิธีการที่ผู้โจมตีใช้คือ ผู้โจมตีจะใช้เครื่องมือโจมตีและวางแผนโดยจงใจฝังติดลงไปในเครื่องมือหรือในระบบของเป้าหมายทำให้เข้าใจว่าที่มาของการโจมตีเป็นบุคคลอื่น เปรียบเทียบได้กับให้เห็นภาพได้ว่า มีโจรเข้าไปในบ้าน ทิ้งแก้วที่มีลายนิ้วมือของบุคคลอื่นบนแก้วนั้นไว้ในบ้าน

หากผู้โจมตีสามารถเข้าระบบได้ก็สามารถที่จะเปลี่ยนแปลงข้อมูลทุกอย่างที่อยู่ในระบบ เช่น การประทับเวลา (Timestamp) และหลักฐานอื่น ๆ ในระบบที่อยู่ในระบบของเป้าหมาย รวมถึงบันทึก (LOG) ด้วย

ที่โจทก์อธิบายเป็นการทั่วไปว่า มือถือของโจทก์นั้นได้รับการวิเคราะห์อย่างไรนั้น จากข้อกล่าวอ้างของโจทก์ ข้าฯ ไม่สามารถพบรายละเอียดของการวิเคราะห์ที่ Citizen Lab หรือองค์กรอื่นว่าได้ทำการวิเคราะห์อย่างไรและไม่มีวิธีการวิเคราะห์ (Methodology) ที่ชัดเจน ที่ข้าฯ รู้คือมีการใช้ MVT

หลักฐานเดียวที่ข้าฯ เห็นคือ MVT Tool ที่ได้รับการพัฒนาโดย Amnesty International

Amnesty International ได้ดำเนินการโดยใช้วิธีการ (Methodology) ที่ Citizen Lab หรือองค์กรอื่นใช้ แต่ก็ไม่มีการตรวจสอบมือถือของโจทก์อย่างไร ข้าฯ อาศัยข้อมูลที่ Amnesty International ระบุว่ามีการใช้ MVT Tool

MVT Tool เป็นเครื่องมืออย่างเดียวที่ข้าฯ ได้มาทางอินเตอร์เน็ต เครื่องมือที่ข้าฯ สามารถตรวจสอบได้คือ MVT Tool เป็นสิ่งสำคัญ

/ MVT Tool...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

MVT Tool ถูกออกแบบมาเพื่อให้สามารถวิเคราะห์มือถือเพื่อทดสอบว่ามีการถูกโจมตีหรือไม่

MVT Tool มีโค้ดอยู่ใน Website Github ซึ่งเป็น Website ที่ใครก็สามารถเข้าไป Download ได้ และสามารถนำ MVT มาใช้วิเคราะห์ว่า มือถือตัวเองนั้นถูกโจมตีหรือไม่ โดยที่

ใน MVT File จะมีสิ่งที่เป็นสิ่งบ่งชี้หรือ IOCs อาจจะมีใครสักคนที่อ้างว่ามีข้อมูลหลักฐานทางนิติวิทยาศาสตร์ที่เฉพาะเจาะจงที่จะใช้ตรวจสอบว่าใครเป็นผู้โจมตีได้ (Forensic Evidence) ยกตัวอย่างว่า MVT Tool เช่น เหมือนเครื่องทดสอบการตั้งครรภ์ เครื่องมืออุปกรณ์นี้สามารถตรวจสอบการตั้งครรภ์ว่าท้องหรือไม่ แต่ไม่สามารถจะบอกได้ว่าใครเป็นพ่อของเด็ก

สิ่งสำคัญที่ข้าฯ ต้องเน้นคือ Software Pegasus ขายให้รัฐบาลเท่านั้น

MVT Tool อาจจะถูกใช้โดยอาชญากร หรือคนใคร่เด็ก (Pedophile) เพื่อตรวจสอบว่ามีการติดตามโดยตำรวจหรือไม่

หมาย ล.๑๔ คำแปลหน้า ๗ ขั้นตอนการใช้งาน MVT พยานอธิบายว่า ต้องดึงข้อมูลโทรศัพท์มือถือออกมา จากนั้นใช้ MVT ทดสอบกับ File ในโทรศัพท์ที่เรียกว่า Stix Format ที่มีตัวบ่งชี้ช่องโหว่ว่าโทรศัพท์มือถือนั้นถูกโจมตีหรือไม่ MVT Tool ก็จะสังเคราะห์ขึ้นมาได้อย่างชัดเจนว่า IOCs หรือตัวชี้ช่องโหว่ใดที่พบในข้อมูลโทรศัพท์มือถือ ซึ่งเป็นหลักฐานทางนิติวิทยาศาสตร์ (Forensic Evidence)

คำแปลหน้าที่ ๘ หมาย ล.๑๔ พยานอธิบายถึง ปัญหาหรือวิธีการหรือระบุที่มาของการโจมตีที่มีการกล่าวอ้าง Software Pegasus ใน Case นี้ ปัญหาจากการใช้วิธีการตรวจสอบของการโจมตีมีดังนี้

ประการแรก เอกสารที่แนบมาพร้อมฟ้องนั้นตามรายงานของ Citizen Lab Citizen Lab ใช้วิธีการวิเคราะห์ Software Pegasus ตามหมาย จ.๔๑ เมื่ออ่านจบแล้วมีความน่าทึ่ง (ประชดประชัน) มากว่า ถ้าหากเป็นข้าฯ จะไม่เขียนแบบนี้

/ตามหมาย...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

ตามหมาย จ.๔๑ หน้า ๒๘ ที่ไฮไลท์ด้วยปากกาสีเหลือง พยานอ่านข้อความดังกล่าวแล้วเบิกความว่า เมื่อข้าฯ อ่านข้อความดังกล่าวแล้วมีความเห็นว่า สรุปอย่างงั้นได้อย่างไร ข้าฯ ขอยกตัวอย่างว่า ถ้าหากมีใครสักคนหนึ่งที่ใช้ Software Pegasus ส่ง Link ไปให้กับอาชญากรหรือผู้ใคร่เด็ก (Pedophile) แล้วบุคคลเหล่านั้นไม่เปิด Link ที่ส่งให้ แต่ส่ง Link ต่อให้กับบุคคลอื่น และทำให้บุคคลอื่นเปิดลิงค์ดังกล่าวติดเชื้อ Spyware มันง่ายมากที่จะปลอมหรือทำให้เข้าใจได้ว่าเป็น Software Pegasus

ประการที่สองคำแปลหน้า ๙ หมาย ล.๑๔ วิธีการที่ระบุที่มาการโจมตีว่าใครเป็นผู้โจมตีไม่มีทางที่จะแน่ใจได้ ๑๐๐ เปอร์เซ็นต์ ว่าผู้ใดเป็นผู้โจมตี ยกตัวอย่างเรื่องเดิมเรื่องการตั้งครรภ์เครื่องมือทดสอบสามารถตรวจสอบได้ว่าผู้หญิงคนนี้ตั้งครรภ์ และคุณสามารถทดสอบ DNA เพื่อพิสูจน์ว่าผู้ใดเป็นพ่อเด็ก การทดสอบด้วย DNA เป็นวิธีการตรวจสอบที่สามารถมั่นใจได้สูงมาก ๆ

ข้าฯ จะแสดงให้เห็นว่า วิธีการที่ใช้ให้เห็นนั้นไม่ได้เหมือนกับที่ข้าฯ อธิบาย ไม่เหมือนกับการทดสอบ DNA

หน้าที่ ๙ มีการทดลองว่ามีการใช้ MVT Tool ใน File ที่มี IOCs และมีข้อบ่งชี้ว่าโทรศัพท์มือถือนั้นมี Software Pegasus หรือไม่ เราเอามือถือมา แล้วใส่ IOCs เข้าไปในมือถือ และไม่มีการให้ติดเชื้อด้วย Pegasus Spyware จากนั้นนำมาวิเคราะห์ด้วย MVT และ MVT ก็บอกว่ามีการถูกโจมตีด้วย Pegasus Software ทั้ง ๆ ที่ไม่มีการใช้ Software Pegasus เมื่อเปรียบเทียบกับการทดสอบการตั้งครรภ์ว่าไม่มีผลทดสอบว่ามีการตั้งครรภ์ จะบอกว่าพ่อเป็นใครก็ไม่สามารถทำได้

ปัญหาที่เกิดก็คือ วิธีการใช้ทดสอบการโจมตีมือถือของโจทก์วิธีนี้นั้น มันง่ายมากเลยที่จะปลอมแหล่งที่มา ซึ่งเป็นการผิดพลาด ดูที่ File IOCs แล้วก็มาดูว่าใส่อะไรเข้าไป และกล่าวโทษว่าบุคคลอื่นเป็นคนทำ

ประเด็นสุดท้าย การขาดพยานหลักฐาน แม้จะมีรายงานและเอกสารแนบท้ายคำฟ้องมากมาย แต่เอกสารดังกล่าวไม่มีเอกสารไหนเลย หรือพยานหลักฐานใดที่ระบุถึงการวิเคราะห์ในรายละเอียดว่า พบอะไรในมือถือของโจทก์ ข้าฯ ได้ทดสอบโดยการใช้ MVT อยู่ในภาคผนวก A ใน

/เอกสาร...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

เอกสารของข้าฯ จะเป็น Log

ข้าฯ ได้ทำการทดสอบโดยการใช้ MVT ซึ่งจะต้องมี Log ขึ้นมา แต่ไม่ปรากฏตามตัวอย่างดังกล่าวในเอกสารของโจทก์

ถ้าพิจารณาว่าไม่มี Log แม้ข้าฯ เป็นผู้เชี่ยวชาญก็ไม่สามารถที่จะพิสูจน์หรือบอกได้ว่าทำอะไรกับมือถือของโจทก์บ้าง

บทสรุปหน้า ๑๑ เป็นการง่ายที่จะกล่าวหา หรือโทษคนอื่นว่า ผู้อื่นเป็นคนทำ วิธีการทดสอบก็ไม่น่าเชื่อถือ ไม่สามารถที่จะตรวจสอบความถูกต้องได้ เพราะว่าไม่มี Log หรือบันทึกทั้งไม่สามารถบอกได้หรือพิสูจน์ได้ถึงความถูกต้อง หรือไม่ถูกต้องอย่างไร

ทนายจำเลยให้พยานดูเอกสารหมาย ล.๑๐ พยานเบิกความว่า รายงานกล่าวว่า ใช้วิธีการเดียวกันในการโจมตีระบบ

O-day exploits คือ มีการใช้ O-day ไม่จำเป็นที่ต้องมีองค์กรเดียวที่จะรู้เรื่องนี้ อาจจะมีหลายองค์กรหรือหลายหน่วยงานก็รู้เรื่องนี้เช่นเดียวกัน และนำไปใช้ประโยชน์ และอาจจะมีผู้โจมตีรายอื่นก็ใช้วิธีการเดียวกัน

O-day exploits คือ ช่องโหว่ในระบบ ซึ่งไม่เป็นที่ทราบแก่คนทั่วไปหรือสาธารณชนโดยทั่วไป ยกตัวอย่างเช่น หลังคาบ้านมีหน้าต่างเล็ก ๆ ซึ่งอาจจะมีแค่บางคนที่รู้ และบางคนอาจจะไม่รู้ว่ามีหน้าต่างเล็ก ๆ อยู่บนบ้านที่สามารถใช้เข้าบ้านได้

O-day exploits กับ n-day หรือ ๑-day แตกต่างกัน

๑-day คือ เมื่อมีความรู้ที่ถูกเปิดเผยทุกคนทราบทุกคนรู้แล้ว วันนี้มีการค้นพบวันรุ่งขึ้นก็เป็นวันที่สอง (๒ day) จนกระทั่งมีวันที่ n-day หรือวันที่สิ้นสุด คือมีการปิดช่องโหว่

/๑-day...

.....พยาน.....โจทก์

.....จันทมาส.ทนายโจทก์.....ทนายจำเลย

.....นางสาวอุรุพรรณ สุวรรณประสพ ล่ามภาษาอังกฤษ

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

๑-day ไปจนถึงระหว่าง n-day มีช่องโหว่ให้ Attacker หรือผู้โจมตีสามารถเข้ามาใช้ประโยชน์จากช่องโหว่นี้ได้ อาจจะมี Attacker บางคน ผู้โจมตีบางคนที่ฉลาดกว่านี้เสียอีก ที่อาจรู้ก่อนที่จะรู้ถึง n-day

หากไม่มีการถึง n-day หรือไม่มีการปิดช่องโหว่นั้นหรือเจ้าของบริษัท Software ยังไม่แก้ไขในช่องโหว่ได้ ในระหว่างนี้ผู้โจมตีจะใช้ประโยชน์ Software หรือ Exploit Software ได้

<u>ตอบทนายโจทก์ถามค้าน</u>

ทนายโจทก์ถามว่า พยานเคยทำงานกับบริษัทพัฒนา Spyware หรือไม่ พยานเบิกความว่าไม่เคย

ทนายโจทก์ถามว่า ที่พยานเบิกความว่า จำเลยมาติดต่อให้พยานมาเบิกความในคดีนี้นั้น พยานเคยรู้จักกับจำเลยมาก่อนหรือไม่ พยานเบิกความว่า เคยได้ยินชื่อจำเลยจากข่าว

ทนายโจทก์ถามว่า พยานทราบอยู่แล้วใช่หรือไม่ว่า บริษัทของจำเลยผลิต Spyware และเป็น Spyware ที่ใช้ในการสอดแนมใช่หรือไม่ พยานเบิกความว่า วัตถุประสงค์ของผลิตภัณฑ์จำเลยมีเพื่อช่วยบังคับการใช้กฎหมายกับผู้ก่อการร้ายหรือคนใคร่เด็ก ซึ่งไม่สามารถที่จัดการโดยวิธีการอื่นได้

ทนายโจทก์ถามว่า บริษัทจะต้องจัดมาตรการไม่ให้มีการใช้ผลิตภัณฑ์กับบุคคลที่ไม่ใช่ผู้ก่อการร้ายหรือกระทำอาชญากรรมร้ายแรง เช่น คนใคร่เด็กใช่หรือไม่ พยานเบิกความว่าไม่ เท่าที่ทราบ จำเลยไม่ได้ควบคุมการใช้งาน

ทนายโจทก์ถามว่า พยานทราบหรือไม่ว่า จำเลยเคยถูกร้องเรียนว่ามีการใช้ Pegasus Software ละเมิดสิทธิมนุษยชนทั่วโลก รวมถึงสภายุโรปด้วย พยานเบิกความว่า เคยอ่านแต่ไม่ทราบลักษณะของข้อร้องเรียน

ทนายโจทก์ถามว่า การพัฒนา Pegasus Spyware ต้องมีระบบป้องกันการตรวจเจอร่องรอยการโจมตีหรือ Fingerprint ของ Spyware หรือไม่ พยานเบิกความว่า ไม่เห็นด้วยกับคำว่า Spyware เนื่องจาก Spyware เป็นเครื่องมือในการรวบรวมข้อมูลอย่างถูกต้องตามกฎหมายที่ใช้โดยหน่วยงานของรัฐ แต่ไม่สามารถป้องกันการโจมตีได้ ยกตัวอย่างเช่น หากข้าฯ เป็นบริษัทผลิตปืนขายปืน

/ก็ไม่สามารถ...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

ก็ไม่สามารถป้องกันผู้ที่ใช้ปืนในการไปยิงคนได้

ทนายโจทก์ถามว่า Pegasus ออกแบบมาให้ถูกตรวจจับยากใช่หรือไม่ พยานเบิกความว่า Spyware เป็นเครื่องมือในการเก็บรวบรวมข้อมูลโดยชอบด้วยกฎหมาย (lawfully interception) และถูกออกแบบมาเพื่อให้สามารถหลีกเลี่ยงตรวจจับว่าถูกติดตามโดยตำรวจได้

ทนายโจทก์ถามว่า การขาย Pegasus จะต้องได้รับการอนุมัติจากกระทรวงกลาโหมของประเทศอิสราเอลใช่หรือไม่ พยานเบิกความว่า เท่าที่ทราบว่าใช่ แต่ข้าฯ เป็นผู้เชี่ยวชาญ แต่กรุณาอย่าถามคำถามที่ไม่เกี่ยวข้องกับด้านเทคนิค

ทนายโจทก์ถามว่า ตามเอกสารหมาย ล.๑๓ นั้น พยานได้ทดลองกับ MVT ของ Amnesty International ใช่หรือไม่ พยานเบิกความว่า Amnesty International เป็นผู้พัฒนา MVT ขึ้น และให้ทุกคนสามารถ Downlond มาใช้งานได้

ทนายโจทก์ถามว่า Version ของ MVT ที่ไป Downlond มานั้นเป็น Version ของปี ๒๐๒๑ ใช่หรือไม่ พยานเบิกความว่าใช่ ในรายงานหมาย ล.๑๓ นั้น ระบุไว้ว่าใช้ Version ปี ๒๐๒๑ เอกสารเขียนไว้ชัดเจนตามเอกสารหมาย ล.๑๓ ข้อที่ ๓ มันไม่ใช่ประเด็นว่า จะเป็น Version ไหน

ทนายโจทก์ถามว่า ตามเอกสารหมาย ล.๑๓ ข้อ ๙ และข้อ ๙.๒ เป็นการตรวจว่า Pegasus Version ที่เป็นการกด link ใช่หรือไม่ พยานเบิกความว่า ใช่ Citizen Lab อ้างว่ามีการคัดลอก Link และมีการทำให้ติดเชื้อ ซึ่งในข้อ ๙.๒ ก็ระบุว่า ประสบความสำเร็จในการติดเชื้อทำให้โทรศัพท์ที่ทดสอบติดเชื้อ (สหรัฐอเมริกา) Link Pegasus ส่งไปยังนักเคลื่อนไหว UAE Davis Mansu

ทนายโจทก์ถามว่า ตามรายงานหมาย ล.๑๓ นั้นตรงกับเอกสารหมาย จ.๔๑ หน้า ๒๘ แล้วถามว่าเป็นการโจมตีปี ๒๐๑๖ ใช่หรือไม่ พยานเบิกความว่าใช่

ทนายโจทก์ถามว่า Pegasus Spyware มีการพัฒนาเป็น Zero Click ในปี ๒๐๑๙ ใช่หรือไม่ พยานเบิกความว่า เป็นไปได้ ข้าฯ ไม่ทราบ ในทางคู่ขนานกันไปอาจจะมีทั้งการใช้ Link และ

/ไม่ใช้ Link...

.....พยาน.....โจทก์

.....ผู้ชำนาญทนายโจทก์.....ทนายจำเลย

.....นางสาวอุรุพรรณ สุวรรณประสพ ล่ามภาษาอังกฤษ

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชี)

ไม่ใช้ Link ก็ได้

ทนายโจทก์ถามว่า การตรวจโทรศัพท์มือถือของโจทก์นั้นจะเป็นการมี Link หรือไม่มี Link พยานทราบหรือไม่ พยานเบิกความว่าไม่ทราบ จะทราบได้อย่างไร เนื่องจากไม่เคยได้รับมือถือของโจทก์มาทำการตรวจสอบ

ทนายโจทก์ให้พยานดูเอกสารหมาย ล.๑๓ ภาคผนวก A หน้าที่ ๙ แล้วถามว่า โทรศัพท์ที่พยานตรวจสอบคือโทรศัพท์ iPhone ๑๔ IOS ๑๖.๖ ใช่หรือไม่ พยานเบิกความว่าใช่

แล้วทนายโจทก์ถามว่า โจทก์ในคดีนี้จะใช้โทรศัพท์ IOS เดียวกันหรือไม่ พยานทราบหรือไม่ พยานเบิกความว่า ไม่ใช่ประเด็น เพราะสิ่งที่ต้องการที่จะพิสูจน์ คือ วิธีการใช้หรือ Methodology ข้าฯ ไม่สามารถเอามือถือของโจทก์มาตรวจสอบได้ จึงไม่สามารถตรวจสอบมือถือจริง ๆ ของโจทก์ได้

ทนายโจทก์ให้พยานดูเอกสารหมาย ล.๑๓ หน้า ๗ ข้อ ๑๑.๖ แล้วถามว่า IOCs หรือ Indicators of Compromise ถ้าบริษัทที่ตรวจการถูกโจมตีโดย Pegasus Spyware เปิดเผย IOCs เช่น Citizen Lab หรือ Amnesty International ในฐานะผู้ผลิตสามารถเอาข้อมูลไปพัฒนาข้อด้อยของ Pegasus Spyware ของตนเองได้ใช่หรือไม่ พยานเบิกความว่า อาจจะเป็นไปได้ว่าถูกต้อง แต่ก็ต้องมีหลักฐานที่พิสูจน์ถึงวิธีการที่หน่วยงานดังกล่าวใช้ หากมีการถูกโจมตีจะพูดแค่นี้มันไม่เพียงพอ จะต้องมีหลักฐานที่มาประกอบด้วย ข้าฯ ทราบว่า Amnesty International เปิดเผย IOCs เพียงแต่ว่าไม่มีรายงาน แต่มั่นใจว่าทุกคนใช้ IOCs และข้อมูลเหล่านี้ทุกคนก็ Download ได้ และยังมีการ Update อย่างต่อเนื่อง

ทนายโจทก์ถามว่า ที่มั่นใจว่า คนอื่นก็ใช้เหมือนกัน พยานได้เคยติดต่อไปยัง Citizen Lab หรือ Amnesty International หรือองค์กรอื่นด้วยตนเองหรือไม่ พยานเบิกความว่าไม่เคย องค์กรเหล่านี้ซ่อนหรือปกปิดวิธีการที่องค์กรเหล่านี้ทำการทดสอบ

ทนายโจทก์ถามว่า หากองค์กรเหล่านี้มีการเปิดเผยวิธีการตรวจสอบหรือเปิดเผย IOCs ทั้งหมด จำเลยสามารถเอาไปพัฒนา Spyware เพื่อหลีกเลี่ยงในการตรวจจับหรือค้นพบทำให้ยากขึ้นใช่หรือไม่ พยานเบิกความว่า หากมือถือนั้นถูกนำข้อมูลออกมา และนำมาทดสอบ IOCs แล้ว แม้จะไม่มี

/การเปิดเผย...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชี)

การเปิดเผย IOCs หากมีการถูกโจมตีด้วย Pegasus จำเลยก็น่าจะต้องรู้ข้อมูลแล้วว่ามีคนรู้แล้วว่ามีการตรวจจับได้ว่ามีการใช้ บริษัทก็คงจะไปหาทางในการเปลี่ยนแปลง Software ของตนเองได้

Amnesty International จะ Update รายการ IOCs และมีบทความที่ตีพิมพ์อยู่แล้ว แม้จะมีการเปิดเผย IOCs แล้วบริษัททราบว่ามีการตรวจจับหรือตรวจพบ Software ของตนเองก็ต้องมีการพัฒนาหรือ Update Software ของตัวเองอยู่แล้ว

ทนายโจทก์ถามพยานว่า พยานทราบหรือไม่ว่า กระบวนการทดสอบว่ามีการปลอมแปลงว่าเป็น Pegasus หรือไม่ เป็นวิธีการไม่ให้ถูกเปิดเผยและคนทั่วไปไม่สามารถทราบได้ พยานเบิกความว่า ถ้าไม่มีความรู้คอมพิวเตอร์ก็ไม่สามารถทำได้ แต่หากเป็นบุคคลในวงการ เช่น เป็นผู้ผลิต Software ก็สามารถทำได้

ช่วงบ่าย (พยานเบิกความต่อจากช่วงเช้า)

ทนายโจทก์ถามว่า หมาย ล.๑๓ ย่อหน้าที่ ๑ ในการทดลองตามเอกสารหมาย ล.๑๓ พยานไม่ได้เป็นคนทำเองใช่หรือไม่ พยานเบิกความว่า ใช่ วิศวกรเป็นผู้ทำให้แก่ข้าฯ

ทนายโจทก์ถามว่า การทดลองตามภาคผนวก A ของเอกสารหมาย ล.๑๓ ทำการทดสอบกับโทรศัพท์ที่ไม่ได้มีการถูกจู่โจมโดย Pegasus Spyware ใช่หรือไม่ พยานเบิกความว่าใช่

ทนายโจทก์ถามว่า โดยปกติแล้วในเครื่องที่ถูกปลอมแปลงโดย Spyware Pegasus จะตรวจสอบพบว่ามีการปลอมแปลงใช่หรือไม่ พยานเบิกความว่า ข้าฯ ไม่ทราบ เพราะข้าฯ ไม่ได้ตรวจสอบ

ทนายโจทก์ถามว่า การตรวจของโจทก์ตามเอกสารหมาย จ.๔๒ การตรวจตามรายงานดังกล่าวจะถูกตรวจโดยวิธีการอย่างไร ขั้นตอน และรายละเอียดการตรวจเป็นอย่างไร พยานทราบหรือไม่ พยานเบิกความว่า ข้าฯ ไม่ทราบ จะตอบว่าใช่หรือไม่ใช่นั้นไม่เพียงพอ จากเอกสารของโจทก์นั้น Amnesty International ใช้วิธีการเดียวกัน สันนิษฐานว่าหรือเข้าใจว่าก็ต้องมีวิธีการเดียวกันที่มีการใช้กับมือถือของโจทก์เช่นเดียวกัน

/ทนายโจทก์...

.....พยาน .....โจทก์

.....ทนายโจทก์ .....ทนายจำเลย

.....นางสาวอุรุพรรณ สุวรรณประสพ ล่ามภาษาอังกฤษ

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

ทนายโจทก์ถามว่า ที่พยานอ้างว่า MVT สามารถปลอมแปลงได้ ข้อต่อสู้นี้พยานเคยให้การในศาลอื่นในประเทศฮังการีและโปร์แลนด์ ว่า จำเลยใช้ Pegasus Spyware กับผู้เสียหายโดยใช้วิธี MVT พยานเคยไปให้การในคดีดังกล่าวใช่หรือไม่ พยานเบิกความว่าไม่เคย

ทนายโจทก์ถามว่า พยานเคยเขียนบทความหรืองานวิชาการโต้แย้ง MVT หรือไม่ พยานเบิกความว่าไม่เคย แต่ข้าฯ ทำวิจัยการตรวจสอบมือถือ

ทนายโจทก์ถามว่า เคยตรวจโทรศัพท์มือถือที่ถูกโจมตีโดย Pegasus Spyware มาก่อนหรือไม่ พยานเบิกความว่าไม่เคย

ทนายโจทก์ถามพยานว่า พยานเคยตรวจเจอเครื่องที่มีการปลอมแปลง Pegasus Spyware เช่นเดียวกับที่พยานรายงานในเอกสารหมาย ล.๑๓ หรือไม่ พยานเบิกความว่า ไม่ การทดลองนี้ตามเอกสารหมาย ล.๑๓ ทำเฉพาะการทดสอบ ชุดทดสอบขององค์กรที่มีกรอบการทำงานขององค์กรเป็นการทดสอบ MVT ว่าจะสามารถเชื่อถือผลการทดสอบได้แค่ไหน

ทนายโจทก์ถามว่า ตามเอกสารหมาย ล.๑๓ ไม่มีการเปรียบเทียบระหว่าง Pegasus Spyware ตัวจริงและผลการตรวจ Pegasus Spyware ตัวเท็จนั้นเป็นอย่างไร พยานเบิกความว่า ไม่สามารถตอบได้ว่าได้หรือไม่ได้ ที่ทำการทดสอบทดลองตามหมาย ล.๑๓ เพื่อตรวจสอบว่า MVT Tool นั้น สามารถที่จะหลอกลวงระบบได้ง่าย

ทนายโจทก์ถามว่า เอกสารหมาย ล.๑๓ ไม่มีการตรวจสอบหรือ Peer Review โดยนักคอมพิวเตอร์คนอื่นหรือไม่ พยานเบิกความว่าไม่มี

ทนายโจทก์ถามพยานว่า ตามเอกสารหมาย ล.๑๐ หน้าที่ ๒ เป็นการตรวจสอบการโจมตีในช่วงเดือนพฤศจิกายน ๒๐๒๓ ถึงกรกฎาคม ๒๐๒๔ พยานเบิกความว่า เป็นวันที่ตามที่เขียนไว้ แล้วถามว่า รายงานได้มีการทำขึ้นในเดือนสิงหาคม ๒๐๒๔ ใช่หรือไม่ พยานเบิกความว่าใช่ แล้วถามว่า รายงานนี้ทำขึ้นภายหลังจากที่โจทก์ถูกโจมตีในปี ๒๕๖๓ ใช่หรือไม่ พยานเบิกความว่า ใช่ เป็นการพิสูจน์หลักการ

/ทนายโจทก์...

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

ทนายโจทก์ถามว่า เอกสารหมาย ล.๑๐ หน้าที่ ๒ และหน้าที่ ๓ ย่อหน้าแรกเป็นการโจมตีแบบ Wateringhole ใช่หรือไม่ พยานเบิกความว่า อาจจะเป็นไปได้ แล้วถามว่า การโจมตีแบบ Wateringhole เป็นการโจมตีที่เจาะ Website ซึ่งแตกต่างจากการโจมตีโทรศัพท์ของโจทก์ใช่หรือไม่ พยานเบิกความว่า อาจจะเป็นไปได้ แต่ไม่ทราบ

ทนายโจทก์ถามว่า การตรวจว่ามี Pegasus Spyware โจมตีจริงหรือไม่ และมีการปลอมแปลงจริงหรือไม่ ผลการตรวจจะน่าเชื่อถือก็ต่อเมื่อตรวจจากโทรศัพท์หรือข้อมูลจากโทรศัพท์ของผู้เสียหายใช่หรือไม่ พยานเบิกความว่าไม่ทราบ

ทนายโจทก์ถามว่า การตรวจตามหมาย ล.๑๓ เป็นการตรวจจากโปรแกรมเฉย ๆ ไม่มีโทรศัพท์หรือข้อมูลจากโทรศัพท์ของโจทก์หรือโทรศัพท์ของโจทก์ใช่หรือไม่ พยานเบิกความว่าใช่ เนื่องจากไม่มีโทรศัพท์ของโจทก์มาทำการทดสอบ

ทนายโจทก์ถามว่า เอกสารหมาย ล.๑๓ และวิธีการตรวจของพยาน ยังไม่มีการรับรองจากหน่วยงานด้านคอมพิวเตอร์หรือผู้เชี่ยวชาญด้านคอมพิวเตอร์ใด ๆ ใช่หรือไม่ พยานเบิกความว่าไม่เกี่ยวข้อง ไม่เป็นสาระที่จะตอบคำถามดังกล่าว

<u>ตอบทนายจำเลยถามติง</u>

ตามเอกสารหมาย ล.๑๐ เพิ่งได้รับการตีพิมพ์เผยแพร่เมื่อไม่กี่วันที่ผ่านมา เกี่ยวข้องกับที่ข้าฯ เบิกความมาตั้งแต่ต้นว่า มีการใช้ช่องโหว่หรือช่องว่าง (Reuse of vulnerability) และวิธีการ (Methodology) ระหว่างองค์กรต่าง ๆ กับผู้กระทำในภาครัฐหรือบริษัทต่าง ๆ เครื่องมือที่ใช้สำหรับการเก็บข้อมูลโดยชอบด้วยกฎหมาย มีการนำช่องโหว่กลับมาใช้ด้วยวิธีการเดียวกัน

รายงานตามหมาย ล.๑๐ ที่มีการทดสอบในช่วงเวลาตามเอกสารหมาย ล.๑๐ นั้นแล้ว จะกล่าวอ้างว่าสิ่งที่เกิดขึ้นตามรายงานและหากย้อนกลับในอดีตแล้วจะบอกว่า สิ่งที่เกิดขึ้นในอดีตนั้นไม่จริงนั้นก็เป็นเรื่องที่ตลก

/เกี่ยวกับ...

.....พยาน.....โจทก์

.....ทนายโจทก์.....ทนายจำเลย

.....นางสาวอุรุพรรณ สุวรรณประสพ ล่ามภาษาอังกฤษ

(คำเบิกความพยานศาตราจารย์ ยูวัล เอลโลวิชิ)

เกี่ยวกับเอกสารหมาย ล.๑๐ หน้าที่ ๒ ถึงหน้าที่ ๓ ย่อหน้าแรกเกี่ยวกับการโจมตี Wateringhole มีการแบ่งปันความรู้ Data Community ว่าเป็นเหตุการณ์ที่เกิดขึ้นมาในอดีต บริษัทที่เก็บรวบรวมการใช้ข้อมูลและกฎหมาย อย่างเช่น จำเลย อาชญากรทางไซเบอร์ หรือผู้กระทำในภาครัฐ

มีคนที่จะสามารถระบุช่องโหว่ มีการขายในตลาดมืดและมีลูกค้าหลายรายจำนวนมากที่ซื้อและใช้ที่เป็นการโจมตี สิ่งที่เกิดขึ้นจากนั้นเป็นสิ่งแรกที่จะจับการใช้ช่องว่างดังกล่าว ผู้ที่โจมตีเป็นผู้ที่เป็นคนทำ แต่จะให้คิดว่าคนอื่นนั้นเป็นคนทำ ทำให้เกิดความสับสน หลงผิดถึงการระบุที่มาของการโจมตี (Domain Attribution)

Wateringhole คือช่องโหว่ประเภทหนึ่งที่มีการใช้เพื่อโจมตี Website

วิธีการดังกล่าวเชื่อมโยงกับมือถือ เป็นตัวอย่างประเภทหนึ่งของการโจมตี ซึ่งมีการใช้โดยผู้โจมตีต่าง ๆ

ข้าฯ ไม่ทราบว่าทำไมถึงเรียกวิธีการดังกล่าวว่า Wateringhole./อ่านแล้ว

(นายบัญชา สุวรรณน้อย) (นางสาวณัฐดา อินฉัตร) บันทึก/อ่าน

.....พยาน

.....โจทก์

.....ทนายโจทก์

.....ทนายจำเลย

.....นางสาวอุรุพรรณ สุวรรณประสพ ล่ามภาษาอังกฤษ