กสม. ๒

รายงานผลการตรวจสอบ

การละเมิดสิทธิมนุษยชน

คณะกรรมการสิทธิมนุษยชนแห่งชาติ

วันที่ ๒ เมษายน พ.ศ. ๒๕๖๗

รายงานผลการตรวจสอบ ที่ ๙๖/๒๕๖๗

เรื่อง สิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง อันเกี่ยวเนื่องกับเสรีภาพในการแสดงความคิดเห็น กรณีขอให้ตรวจสอบการใช้สปายแวร์เพกาซัส (Pegasus Spyware)

ผู้ร้อง [redacted]

ผู้ถูกร้อง หน่วยงานของรัฐด้านความมั่นคง

๑. ความเป็นมา

ผู้ร้องยื่นหนังสือร้องเรียนผ่านกรรมการสิทธิมนุษยชนแห่งชาติ ตามคำร้องที่ ๑๖๓/๒๕๖๕ ลงวันที่ ๒๖ กันยายน ๒๕๖๕ ว่า เมื่อวันที่ ๒๔ พฤศจิกายน ๒๕๖๔ ผู้ร้องได้รับไปรษณีย์อิเล็กทรอนิกส์ (อีเมล) แจ้งเตือนจากบริษัทผู้ผลิตโทรศัพท์เคลื่อนที่ ยี่ห้อไอโฟน (iPhone) ว่า โทรศัพท์เคลื่อนที่ของผู้ร้องอาจถูกเจาะระบบเพื่อสอดแนมโดยผู้โจมตีที่ได้รับการสนับสนุนจากองค์กรของรัฐ ผู้ร้องจึงติดต่อไปยังองค์กรที่มีความเชี่ยวชาญด้านเทคโนโลยีคอมพิวเตอร์ในต่างประเทศเพื่อขอให้ตรวจสอบ และพบว่ามีผู้โจมตีเพื่อเจาะระบบโทรศัพท์เคลื่อนที่ของผู้ร้องโดยใช้สปายแวร์ชื่อว่า “เพกาซัส (Pegasus)” ต่อเนื่องกัน ๑๐ ครั้ง ตั้งแต่เดือนพฤศจิกายน ๒๕๖๓ ถึงเดือนพฤศจิกายน ๒๕๖๔ ซึ่งสปายแวร์ดังกล่าวผลิตขึ้นโดยบริษัทในประเทศอิสราเอล ซึ่งได้กำหนดเงื่อนไขว่าจะขายผลิตภัณฑ์ให้แก่เฉพาะหน่วยงานของรัฐเพื่อป้องกันและปราบปรามอาชญากรรมร้ายแรงเท่านั้น เนื่องจากเป็นสปายแวร์ที่มีประสิทธิภาพสูง สามารถเข้าถึงข้อมูลทั้งหมดในโทรศัพท์เคลื่อนที่ของผู้ที่ตกเป็นเป้าหมายได้โดยไม่รู้ตัว ทั้งนี้ จากการตรวจสอบด้วยวิธีการทางเทคนิคคอมพิวเตอร์เพิ่มเติมพบว่า มีนักกิจกรรม นักการเมือง และนักวิชาการที่มีความคิดเห็นแตกต่างจากรัฐบาลอย่างน้อย ๓๕ คน ถูกเจาะระบบโทรศัพท์เคลื่อนที่ด้วยสปายแวร์เพกาซัสเช่นเดียวกัน ทำให้ผู้ร้องเชื่อว่าเป็นการกระทำที่ได้รับการสนับสนุนจากหน่วยงานของรัฐในประเทศไทย และไม่ชอบด้วยกฎหมาย อีกทั้งยังละเมิดต่อสิทธิในความเป็นอยู่ส่วนตัวของประชาชน จึงขอให้ตรวจสอบ

/๒. การตรวจสอบ...

๒. การตรวจสอบ

คณะกรรมการสิทธิมนุษยชนแห่งชาติได้มอบหมายให้พนักงานเจ้าหน้าที่ตรวจสอบตามพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐ และระเบียบคณะกรรมการสิทธิมนุษยชนแห่งชาติว่าด้วยหลักเกณฑ์และวิธีการในการตรวจสอบการละเมิดสิทธิมนุษยชน พ.ศ. ๒๕๖๑ และที่แก้ไขเพิ่มเติม โดยพิจารณาจากข้อเท็จจริงและพยานหลักฐานดังต่อไปนี้

๒.๑ รายการเอกสาร พยานหลักฐานจากการตรวจสอบ และเอกสารที่เกี่ยวข้อง

๒.๑.๑ รายงานวิจัย เรื่อง “GeckoSpy : Pegasus Spyware Used against Thailand’s Pro-Democracy Movement” จัดทำโดยห้องปฏิบัติการ Citizen Lab สังกัดมหาวิทยาลัย Toronto ประเทศแคนาดา เผยแพร่ทางเว็บไซต์เมื่อวันที่ ๑๗ กรกฎาคม ๒๕๖๕

๒.๑.๒ รายงานการประชุมรับฟังข้อเท็จจริงจากผู้แทนหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้อง ได้แก่ สำนักงานตำรวจแห่งชาติ กองบัญชาการตำรวจปราบปรามยาเสพติด สำนักข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ กระทรวงกลาโหม กองทัพบก กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เมื่อวันที่ ๒ ธันวาคม ๒๕๖๕ ณ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๒.๑.๓ รายงานการประชุมรับฟังข้อเท็จจริงเพิ่มเติมจากผู้ร้อง เมื่อวันที่ ๒๒ ธันวาคม ๒๕๖๕ ณ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๒.๑.๔ หนังสือบริษัท [redacted] จำกัด ลงวันที่ ๑๓ กุมภาพันธ์ ๒๕๖๖ ถึงเลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๒.๑.๕ รายงานการประชุมรับฟังความเห็นของ [redacted] ในฐานะพยานผู้เชี่ยวชาญ เมื่อวันที่ ๑๕ กุมภาพันธ์ ๒๕๖๖ ณ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

๒.๑.๖ รายงานความโปร่งใสและความรับผิดชอบ (Transparency and Responsibility Report) [redacted] ๒๕๖๔ และปี ๒๕๖๖

๒.๑.๗ เอกสารประกอบคำของบประมาณประจำปีงบประมาณ พ.ศ. ๒๕๖๖ ของกองบัญชาการตำรวจปราบปรามยาเสพติด เรื่อง “โครงการจัดหาระบบรวบรวมและประมวลผลข่าวกรองชั้นสูง”

๒.๑.๘ รายงานข่าวของสื่อมวลชนที่เกี่ยวข้อง

/๒.๒ ข้อเท็จจริง...

๒.๒ ข้อเท็จจริงจากการตรวจสอบ

๒.๒.๑ ข้อเท็จจริงฝ่ายผู้ร้อง

๑) ผู้ร้องให้ข้อมูลเพิ่มเติมแนบมาพร้อมกับคำร้องว่า เมื่อวันที่ ๒๔ พฤศจิกายน ๒๕๖๔ [redacted] ซึ่งเป็นบริษัทผู้ผลิตโทรศัพท์เคลื่อนที่ยี่ห้อ ไอโฟน ได้ส่งอีเมลแจ้งเตือนผู้ร้อง เรื่อง “แจ้งเตือน: ผู้โจมตีที่ได้รับการสนับสนุนโดยรัฐอาจมุ่งเป้าหมายไปที่ไอโฟนของคุณ [redacted] เนื้อความสรุปได้ว่า [redacted] เชื่อว่าผู้ร้องกำลังตกเป็นเป้าหมายของผู้โจมตีที่ได้รับการสนับสนุนโดยรัฐ ซึ่งพยายามเจาะระบบโทรศัพท์เคลื่อนที่ของผู้ร้องจากระยะไกล โดยอาจเข้าถึงข้อมูลที่อ่อนไหว (sensitive data) ข้อมูลการสื่อสาร หรือสามารถเปิดกล้องและไมโครโฟนได้ ผู้โจมตีที่ได้รับการสนับสนุนโดยรัฐมีเงินทุน มีความซับซ้อนของเทคโนโลยีขั้นสูง และมีการพัฒนาการโจมตีตลอดเวลา ซึ่งบางครั้งเป้าหมายไม่รู้ตัว โดยหลอกให้เป้าหมายกดลิงก์ที่น่าสงสัย เปิดไฟล์แนบในอีเมล ข้อความสั้น หรือข้อความอื่น ๆ รวมทั้งอาจโจมตีอุปกรณ์หรือช่องทางอื่นที่ไม่ได้เกี่ยวข้องกับผลิตภัณฑ์ของบริษัท แอปเปิล ทั้งนี้ [redacted] ไม่สามารถให้ข้อมูลในรายละเอียดการโจมตีมากกว่านี้ได้ เนื่องจากผู้โจมตีอาจปรับเปลี่ยนรูปแบบการโจมตีเพื่อหลีกเลี่ยงการตรวจสอบในอนาคต อย่างไรก็ดี แม้เป็นไปได้ว่าการแจ้งเตือนตามอีเมลนี้อาจเป็นการเตือนที่ผิดพลาด (false alarm) แต่ก็ควรให้ความสำคัญ โดย [redacted] แนะนำให้ผู้ร้องอัปเดตระบบปฏิบัติการ (iOS) ให้เป็นรุ่นล่าสุด และให้ขอความช่วยเหลือจากผู้เชี่ยวชาญ เช่น องค์กร Access Now หากไม่สามารถติดต่อกับผู้เชี่ยวชาญได้ แนะนำเบื้องต้นให้ลงชื่อออก (sign out) จากบัญชีบริการส่งข้อความและคลาวด์ (messaging and cloud services) ตั้งค่าโทรศัพท์เคลื่อนที่กลับคืนสู่การตั้งค่าโรงงาน (factory setting) และเปลี่ยนรหัสผ่านของบัญชีที่ได้ใช้งานบนเว็บไซต์หรือบริการซึ่งเข้าถึงได้จากโทรศัพท์เคลื่อนที่

๒) ผู้ร้องให้ข้อมูลเพิ่มเติมเมื่อวันที่ ๒๒ ธันวาคม ๒๕๖๕ ดังนี้

(๑) หลังจากได้รับอีเมลแจ้งเตือนจาก [redacted] แล้ว ผู้ร้องได้ดำเนินการตามคำแนะนำทั้งหมด และพยายามติดต่อองค์กรผู้เชี่ยวชาญ จนได้รับการตอบรับจากห้องปฏิบัติการสหวิทยาการชื่อ “Citizen Lab” สังกัดมหาวิทยาลัย Toronto ประเทศแคนาดา โดยมี [redacted] นักเทคนิคคอมพิวเตอร์ของห้องปฏิบัติการ เป็นผู้ให้คำปรึกษาโดยไม่มีค่าใช้จ่าย ทำให้ทราบว่าการโจมตีตามที่ผู้ร้องได้รับแจ้งเตือน อาจมาจากสปายแวร์ที่ชื่อว่า “เพกาซัส” โดยการใช้งานสปายแวร์นี้เป็นที่สนใจในระดับโลกมาระยะหนึ่งแล้ว เนื่องจากมีวิธีการทำงานที่สามารถแทรกซึมเข้ามาในโทรศัพท์เคลื่อนที่ของเป้าหมายโดยเจ้าของเครื่องไม่รู้ตัวและไม่ต้องกดรับ หรือที่เรียกว่า “Zero-Click” มีการนำมาใช้กับนักกิจกรรมทางการเมืองหรือผู้ที่เคลื่อนไหวต่อต้านรัฐบาล

/ในหลายประเทศ...

ในหลายประเทศ ทั้งนี้ [redacted] แนะนำเบื้องต้นให้หาผู้เชี่ยวชาญที่สามารถทำกระบวนการเก็บรวบรวมและวิเคราะห์หลักฐานทางดิจิทัล หรือ “Digital Forensics” ในประเทศไทย ซึ่งพบว่ามีบริษัทเอกชนเพียงแห่งเดียวที่สามารถดำเนินการได้ แต่ไม่สะดวกที่จะดำเนินการ [redacted] จึงตกลงที่จะให้ความช่วยเหลือแก่ผู้ร้อง ซึ่งจากการตรวจสอบข้อมูลในโทรศัพท์เคลื่อนที่ของผู้ร้องด้วยวิธีการทางเทคนิคคอมพิวเตอร์ ได้พบร่องรอยการถูกเจาะระบบโดยสปายแวร์เพกาซัส

(๒) เมื่อสปายแวร์เพกาซัสถูกติดตั้งในโทรศัพท์เคลื่อนที่ของเป้าหมายแล้ว จะทำการส่งข้อมูลที่ผู้โจมตีต้องการเข้าถึง ผ่านระบบอินเทอร์เน็ตออกไปยังแม่ข่ายหรือเซิร์ฟเวอร์ (server) ของสปายแวร์ กระบวนการทั้งหมดเกิดขึ้นโดยเจ้าของเครื่องไม่รู้ตัว ซึ่งผู้โจมตีอาจเปลี่ยนช่องทางการโจมตีไปเรื่อย ๆ ตามช่องโหว่ที่พบ เพียงแค่ทราบหมายเลขโทรศัพท์เคลื่อนที่หรือที่อยู่อีเมลของเป้าหมาย วิธีการตรวจสอบในเบื้องต้นว่าโทรศัพท์เคลื่อนที่ถูกโจมตีด้วยสปายแวร์หรือไม่ จะตรวจดูจากเลขที่อยู่ไอพี (IP address) และชื่อของเซิร์ฟเวอร์ที่ถูกบันทึกไว้ในโทรศัพท์เคลื่อนที่ หากมีการส่งข้อมูลจากโทรศัพท์เคลื่อนที่ไปยังเซิร์ฟเวอร์ที่ผิดปกติหรือเคยถูกระบุจากงานศึกษาวิจัยแล้วว่าเป็นเซิร์ฟเวอร์ของสปายแวร์เพกาซัส ก็มีความเป็นไปได้ว่ามีการโจมตีเกิดขึ้น

(๓) สปายแวร์เพกาซัสเคยโจมตีด้วยการฝังตัวอยู่ในแอปพลิเคชัน iMessage ซึ่งโทรศัพท์เคลื่อนที่ไอโฟนจะติดตั้งไว้ทุกเครื่อง แต่ [redacted] ได้ทำการอุดช่องโหว่ดังกล่าวแล้ว โดยเมื่อประมาณต้นปี ๒๕๖๕ [redacted] ได้ออกแถลงการณ์ว่าสามารถแก้ไขปัญหาช่องโหว่ที่พบได้แล้ว แต่ไม่ระบุชื่อสปายแวร์ที่โจมตี และแนะนำให้ผู้ใช้งานผลิตภัณฑ์ของ[redacted] อัปเดตระบบปฏิบัติการให้เป็นปัจจุบัน

(๔) ผู้ร้องได้ติดต่อขอความช่วยเหลือจากผู้ที่มีความรู้ทางเทคนิคคอมพิวเตอร์ให้สืบสวนหาข้อมูลการใช้งานสปายแวร์ชนิดนี้ให้ละเอียดยิ่งขึ้น และติดต่อนักกิจกรรมทางการเมืองที่อาจเข้าข่ายถูกโจมตี และผู้ที่ได้รับอีเมลแจ้งเตือนจาก[redacted] อีกหลายคน เพื่อขอความยินยอมในการทำกระบวนการ Digital Forensics โดยใช้เวลาดำเนินการตั้งแต่เดือนมีนาคมถึงเดือนมิถุนายน ๒๕๖๕ พบว่ามีผู้ที่ถูกโจมตีโดยสปายแวร์เพกาซัสอีก ๓๕ คน ทั้งนี้ ห้องปฏิบัติการ Citizen Lab ได้ส่งข้อมูลที่ตรวจพบว่ามีการโจมตีโดยสปายแวร์เพกาซัสในประเทศไทยไปให้ Amnesty Tech ช่วยตรวจทาน โดยมีวิธีการตรวจสอบในอีกรูปแบบ และได้รับการยืนยันว่าเป็นการโจมตีโดยสปายแวร์เพกาซัสเช่นเดียวกัน

(๕) รายงานของห้องปฏิบัติการ Citizen Lab ระบุว่าข้อมูลที่ได้จากการสแกนระบบอินเทอร์เน็ตน่าจะมี ๓ หน่วยงานของรัฐในประเทศไทยที่เป็นผู้ใช้งานสปายแวร์ ได้แก่ กองบัญชาการตำรวจปราบปรามยาเสพติด กองการทหารข่าวกรอง และกองอำนวยการรักษา

ความมั่นคงภายในราชอาณาจักร ผู้ร้องได้สอบถามห้องปฏิบัติการ Citizen Lab ถึงวิธีการตรวจสอบว่าผู้ใดเป็นผู้ใช้งานสปายแวร์เพกาซัสบ้าง แต่ได้รับแจ้งว่าวิธีการตรวจสอบเป็นความลับ หากเปิดเผยจะทำให้ผู้ผลิตสปายแวร์เข้าใจวิธีการตรวจสอบและสามารถซ่อนตัวจากการตรวจสอบได้ อีกทั้งรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ชี้แจงในการอภิปรายไม่ไว้วางใจของสภาผู้แทนราษฎรว่า ประเทศไทยมีหน่วยงานด้านยาเสพติดและหน่วยงานด้านความมั่นคงเป็นผู้ใช้งานสปายแวร์

(๖) ข้อมูลที่บ่งบอกว่า [redacted] ซึ่งผลิตสปายแวร์เพกาซัสจะขายผลิตภัณฑ์ให้แก่หน่วยงานของรัฐเท่านั้น ปรากฏอยู่ในรายงานที่เผยแพร่อยู่บนเว็บไซต์[๑] ของบริษัทเอง ส่วนในประเทศไทย พบกรณีที่อาจเข้าข่ายว่ามีการใช้งานสปายแวร์เพกาซัสโดยหน่วยงานของรัฐปรากฏอยู่ในเอกสารการของบประมาณประจำปีงบประมาณ พ.ศ. ๒๕๖๖ ของกองบัญชาการตำรวจปราบปรามยาเสพติด ระบุรายละเอียดคุณลักษณะของสปายแวร์ที่ขอจัดซื้อคล้ายกับสปายแวร์เพกาซัส คือ สามารถโจมตีเพื่อเข้าถึงข้อมูลต่าง ๆ ได้โดยเจ้าของอุปกรณ์ไม่ต้องกดรับ มูลค่าประมาณ ๓๐๐ ล้านบาท โดยมี [redacted] เป็นผู้เสนอราคา ซึ่งห้องปฏิบัติการ Citizen Lab แจ้งว่าเป็นบริษัทที่มีความเกี่ยวข้องกับ [redacted] ทั้งนี้ เอกสารการของบประมาณยังระบุอีกว่าเป็นการขอจัดสรรงบประมาณต่อเนื่อง เพราะรุ่นเดิมล้าสมัยแล้ว จึงอนุมานได้ว่าอาจมีการจัดซื้อสปายแวร์รุ่นเดิมไว้แล้วในปีงบประมาณก่อน

(๗) ผู้ได้รับผลกระทบหลายรายได้ฟ้องคดี [redacted] ต่อศาลแพ่ง และทราบมาว่า [redacted] ก็ได้ฟ้องคดีต่อ [redacted] ด้วย ซึ่งถือเป็นการยอมรับโดยปริยายว่า [redacted] ถูกโจมตีโดยสปายแวร์เพกาซัส อย่างไรก็ดี จากการศึกษาวิธีการต่อสู้คดีของ [redacted] ในคดีก่อน ๆ ที่ถูกฟ้องต่อศาลในสหรัฐอเมริกาและซาอุดีอาระเบีย พบว่ามักจะเริ่มจากการโต้แย้งก่อนว่าตนเองเป็นบริษัทต่างประเทศ ไม่อยู่ภายในเขตอำนาจศาลของประเทศที่ตนถูกฟ้องคดี จากนั้นจะต่อสู้ว่าได้รับอนุมัติจากกระทรวงกลาโหมของประเทศอิสราเอลแล้ว จึงมีความคุ้มกันในบริบทระหว่างประเทศ ซึ่งคดีที่ [redacted] ยื่นฟ้องยังอยู่ในชั้นการพิจารณาเรื่องความคุ้มกันนี้อยู่

(๘) นอกจากได้รับการแจ้งเตือนจาก [redacted] แล้ว ประมาณเดือนพฤศจิกายน ๒๕๖๕ ก่อนมีการชุมนุมของกลุ่ม “ราษฎรหยุด APEC 2022” ยังพบว่ามีนักกิจกรรมทางการเมืองและนักเคลื่อนไหวในประเด็นต่าง ๆ อีกหลายคน ได้รับการแจ้งเตือนในลักษณะเดียวกัน

/จากแอปพลิเคชัน...

---

๑ [redacted]

จากแอปพลิเคชัน Facebook ด้วย แต่กรณีนี้ได้ปรึกษากับ [redacted] แล้ว ได้รับแจ้งว่าเป็นการโจมตีของสปายแวร์ยี่ห้ออื่น ไม่ใช่สปายแวร์เพกาซัส

๓) ผู้ร้องได้มอบบันทึกรับรองการถูกโจมตีด้วยสปายแวร์เพกาซัสที่ห้องปฏิบัติการ Citizen Lab จัดทำ ให้แก่พนักงานเจ้าหน้าที่ รวม ๘ ฉบับ เพื่อยืนยันอีกชั้นหนึ่งว่ามีการใช้สปายแวร์เพกาซัสโจมตีต่อนักกิจกรรมและนักวิชาการจริง โดยเอกสารดังกล่าวระบุข้อมูลเกี่ยวกับรายชื่อผู้ที่ถูกโจมตี จำนวนครั้งและวันที่ที่ถูกโจมตี (โดยประมาณ) ขีดความสามารถของสปายแวร์เพกาซัส รวมถึงข้อมูลเกี่ยวกับ [redacted] โดยนักกิจกรรมและนักวิชาการที่มีเอกสารรับรองดังกล่าว ประกอบด้วย

- [redacted] ถูกโจมตี ๕ ครั้ง ในระหว่างปี ๒๕๖๓ - ๒๕๖๔
- [redacted] ถูกโจมตี ๑ ครั้ง ในปี ๒๕๖๔
- [redacted] ถูกโจมตี ๓ ครั้ง ในปี ๒๕๖๔
- [redacted] ถูกโจมตี ๑ ครั้ง ในปี ๒๕๖๔
- [redacted] ถูกโจมตี ๔ ครั้ง ในปี ๒๕๖๔
- [redacted] ถูกโจมตี ๕ ครั้ง ในปี ๒๕๖๔
- [redacted] ถูกโจมตี ๑ ครั้ง ในปี ๒๕๖๔
- ผู้ร้อง ถูกโจมตี ๑๐ ครั้ง ในระหว่างปี ๒๕๖๓ - ๒๕๖๔

๒.๒.๒ ข้อเท็จจริงฝ่ายผู้ถูกร้อง

๑) สำนักงานตำรวจแห่งชาติ

๑.๑) กองบัญชาการตำรวจปราบปรามยาเสพติดเป็นหน่วยงานเพียงแห่งเดียวของสำนักงานตำรวจแห่งชาติที่สามารถใช้เครื่องมือพิเศษในการเข้าถึงข้อมูลในโทรศัพท์เคลื่อนที่ของเป้าหมายได้ตามพระราชบัญญัติวิธีพิจารณาคดียาเสพติด พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม มาตรา ๑๑/๕[๒] ส่วนหน่วยงานอื่นในสังกัดไม่ได้จัดซื้อสปายแวร์ เนื่องจากไม่มีอำนาจตามกฎหมาย

/๑.๒) กองบัญชาการ...

---

[๒] มาตรา ๑๑/๕ ในกรณีจำเป็นและมีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงาน ป.ป.ส. ซึ่งได้รับอนุมัติจากเลขาธิการคณะกรรมการป้องกันและปราบปรามยาเสพติดเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลอาญา เพื่อมีคำสั่งอนุญาตให้เจ้าพนักงาน ป.ป.ส. ได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

การอนุญาตตามวรรคหนึ่ง ให้ศาลพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็น ดังต่อไปนี้

(๑) มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดเกี่ยวกับยาเสพติด

๑.๒) กองบัญชาการตำรวจปราบปรามยาเสพติดจัดซื้อเครื่องมือพิเศษมาตั้งแต่ปี ๒๕๕๗ เนื่องจากมีความคุ้มค่ากับภารกิจในการป้องกันและปราบปรามยาเสพติดที่มีมูลค่าสูง ในส่วนการใช้งานเครื่องมือพิเศษ จะมีคณะกรรมการพิจารณาความจำเป็นก่อนการใช้งาน เพราะเป็นเรื่องที่สำคัญ และไม่สามารถนำไปใช้ในภารกิจอื่นนอกเหนือจากคดีที่เกี่ยวข้องกับยาเสพติดได้ เมื่อได้พยานหลักฐานมาแล้ว จะต้องนำส่งให้ศาลทั้งหมด เจ้าหน้าที่ตำรวจจะขอพยานหลักฐานจากศาลมาใช้ในการจัดทำสำนวนเป็นครั้งคราว อย่างไรก็ดี ตั้งแต่ปี ๒๕๖๓ เป็นต้นมา หน่วยงานไม่ได้รับงบประมาณสนับสนุนในส่วนนี้ จึงไม่ได้อัปเดตซอฟต์แวร์และไม่ได้ใช้งานเครื่องมือพิเศษดังกล่าว

๒) กองบัญชาการตำรวจปราบปรามยาเสพติด

๒.๑) กองบัญชาการตำรวจปราบปรามยาเสพติดได้จัดซื้ออุปกรณ์เข้าถึงข้อมูลพิเศษและข้อมูลอิเล็กทรอนิกส์จากประเทศอิสราเอล เมื่อปี ๒๕๕๗ เนื่องจากมีความจำเป็นในภารกิจสืบสวนเพื่อป้องกันอาชญากรรมที่มีความยากลำบากในการเข้าถึงข้อมูล โดยเฉพาะการเข้าถึงข้อมูลหลักฐานที่อยู่ในโทรศัพท์เคลื่อนที่ของผู้กระทำความผิดเกี่ยวกับยาเสพติด เครื่องมือจะทำงานโดยส่งสปายแวร์เข้าไปในโทรศัพท์เคลื่อนที่เพื่อทำสำเนาข้อมูลส่งมายังระบบ เป้าหมายจะต้องกดรับก่อนจึงจะทำการเจาะข้อมูลสำเร็จ มักจะใช้เป็นกรณีสุดท้ายหากไม่สามารถสืบสวนด้วยวิธีการใด ๆ ได้แล้ว

๒.๒) การใช้อุปกรณ์เช่นนี้อาศัยฐานอำนาจตามพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. ๒๕๑๙ มาตรา ๑๔ จัตวา[๓] โดยเมื่อได้พยานหลักฐานในเบื้องต้นแล้วว่า

/เป้าหมาย...

---

(๒) มีเหตุอันควรเชื่อได้ว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดเกี่ยวกับยาเสพติดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

(๓) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

(ต่อ) การอนุญาตตามวรรคหนึ่ง ให้ศาลสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยกำหนดเงื่อนไขใด ๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายในระยะเวลาที่ศาลกำหนด ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป ให้ศาลมีอำนาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อเจ้าพนักงาน ป.ป.ส. ได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้ศาลทราบ

ฯลฯ ฯลฯ

[๓] มาตรา ๑๔ จัตวา ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญา พิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

(๑) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดเกี่ยวกับยาเสพติด

เป้าหมายมีพฤติการณ์กระทำผิดหรือส่อไปในทางกระทำผิด เจ้าพนักงานผู้มีอำนาจหน้าที่ตามกฎหมายจะขออนุมัติเป็นลายลักษณ์อักษรจากเลขาธิการคณะกรรมการป้องกันและปราบปรามยาเสพติด จากนั้นจึงยื่นคำขอให้อธิบดีผู้พิพากษาศาลอาญามีคำสั่งอนุญาตก่อนปฏิบัติการ โดยจะสั่งอนุญาตได้คราวละไม่เกิน ๙๐ วัน เมื่อดำเนินการแล้ว ต้องรายงานผลต่ออธิบดีผู้พิพากษาศาลอาญาทราบภายใน ๗ วัน หลังจากวันที่สิ้นสุดการอนุญาต หากยังไม่ได้ข้อมูล จะต้องเริ่มกระบวนการขออนุมัติและอนุญาตอีกครั้ง

๒.๓) ไม่มีการกำหนดจำนวนครั้งในการใช้งาน เป็นการซื้อสิทธิใช้งาน (license) แบบปีต่อปี และจำเป็นต้องได้รับการอัปเดตซอฟต์แวร์ในแต่ละปีให้สามารถทำงานได้บนโทรศัพท์เคลื่อนที่หรือระบบปฏิบัติการรุ่นใหม่ เครื่องมือพิเศษที่จัดซื้อมานี้ถูกใช้งานมาจนถึงปี ๒๕๖๒ แต่ตั้งแต่ปี ๒๕๖๓ หน่วยงานไม่ได้รับอนุมัติงบประมาณ จึงไม่สามารถใช้งานต่อได้ และไม่มีการนำเครื่องมืออื่นที่คล้ายกันมาใช้แทน

๓) สำนักข่าวกรองแห่งชาติ

๓.๑) สำนักข่าวกรองแห่งชาติไม่ได้จัดซื้อสปายแวร์เพกาซัส หรือสปายแวร์ยี่ห้ออื่น แต่ทราบว่า [redacted] จากประเทศอิสราเอล ซึ่งเป็นผู้ผลิต เคยนำผลิตภัณฑ์สปายแวร์มาเสนอขายให้แก่หน่วยงานของรัฐด้านความมั่นคง แต่ไม่ทราบว่าหน่วยงานของรัฐแห่งใดจัดซื้อบ้าง [redacted] ได้เสนอขายผลิตภัณฑ์แก่สำนักข่าวกรองแห่งชาติเมื่อปี ๒๕๕๘ แต่ไม่ได้จัดซื้อ เนื่องจากมีมูลค่าสูงกว่าหนึ่งร้อยล้านบาท และเห็นว่ายังมีจุดอ่อนในการนำไปใช้ค่อนข้างมาก ไม่ตอบสนองต่อการทำงานที่มุ่งเน้นเป้าหมายที่กระทำความผิดที่กระทบต่อความมั่นคงของชาติ เช่น อาชญากรข้ามชาติ หรือผู้ก่อการร้ายสากล ซึ่งกลุ่มเหล่านี้มีองค์ความรู้สูง ไม่เปิดเผยหมายเลขโทรศัพท์ จึงไม่น่าจะมีโอกาสได้ใช้บ่อยครั้งและอาจไม่คุ้มค่าต่องบประมาณที่ลงทุนไป

๓.๒) ในด้านข่าวกรอง ที่ผ่านมายังไม่พบว่ามีหน่วยงานใดของรัฐอ้างว่าได้ข่าวกรองมาจากการใช้งานสปายแวร์ ข่าวกรองส่วนใหญ่มักจะมาจากการสืบสวน การสังเกตการณ์

/การรวบรวม...

---

(๒) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดเกี่ยวกับยาเสพติดจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

๓) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

(ต่อ) การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยกำหนดเงื่อนไขใด ๆ ก็ได้และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อเจ้าพนักงานได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

การรวบรวมข้อมูลจากสื่อสังคมออนไลน์ ส่วนการติดตามความเคลื่อนไหวทางการเมือง มีเพียงการเฝ้าดูสถานการณ์ให้อยู่ภายในกรอบของกฎหมายเท่านั้น

๔) สำนักงานสภาความมั่นคงแห่งชาติ

สำนักงานสภาความมั่นคงแห่งชาติไม่ได้จัดซื้อสปายแวร์เพกาซัสหรือสปายแวร์อื่น ๆ เนื่องจากไม่มีอำนาจหน้าที่ตามกฎหมาย อีกทั้งยังมีงบประมาณที่จำกัด จึงไม่มีเหตุผลความจำเป็นที่จะนำมาใช้งาน และที่ผ่านมาไม่พบว่าบริษัทผู้ผลิตสปายแวร์เพกาซัสได้เคยมานำเสนอขายผลิตภัณฑ์ด้วย

๕) กระทรวงกลาโหม

กระทรวงกลาโหมไม่มีการจัดหาสปายแวร์เพกาซัสมาใช้งาน และเท่าที่ทราบหน่วยงานอื่นในสังกัดก็ไม่ได้ใช้งานสปายแวร์ เนื่องจากกระทรวงกลาโหมมีหน้าที่ในเชิงป้องกัน ไม่ได้มีหน้าที่ในเชิงรุกหรือการโจมตีผู้ใด จึงไม่มีเหตุผลความจำเป็นที่จะต้องนำสปายแวร์มาใช้งาน มีเพียงการใช้งานซอฟต์แวร์เพื่อป้องกันสปายแวร์หรือโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (antivirus) เท่านั้น ซึ่งสอดคล้องกับจำนวนงบประมาณที่ได้รับจัดสรร ทั้งนี้ สามารถตรวจสอบการจัดซื้อจัดจ้างหรือการใช้จ่ายงบประมาณได้ว่ากระทรวงกลาโหมหรือกองทัพบกไม่ได้ของบประมาณจัดซื้อจัดจ้างซอฟต์แวร์ประเภทนี้ ที่ผ่านมาไม่มีบริษัทเอกชนมานำเสนอขายสปายแวร์หรือซอฟต์แวร์ในลักษณะเดียวกัน มีเพียงการนำเสนอผลิตภัณฑ์ที่นำมาใช้ในเชิงป้องกันเท่านั้น

๖) กองทัพบก

ภารกิจของหน่วยข่าวกรองทางทหาร กองทัพบก มีหน้าที่ในการป้องกันประเทศ ส่วนใหญ่จะใช้เครื่องมือทางทหารโดยตรง เช่น เครื่องมือดักรับย่านคลื่นแม่เหล็ก เพื่อป้องกันภัยคุกคามและปราบปรามยาเสพติด ไม่มีหน้าที่รับผิดชอบโดยตรงในการติดตามความเคลื่อนไหวของนักกิจกรรมกลุ่มต่าง ๆ ยกเว้นการติดตามบุคคลที่เป็นภัยคุกคามต่อประเทศ จึงขอยืนยันว่าไม่ได้ใช้งานสปายแวร์เพกาซัสหรือสปายแวร์อื่น ๆ

๗) กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรไม่มีการจัดซื้อหรือใช้งานสปายแวร์เพกาซัสรวมถึงสปายแวร์อื่น ๆ มีเพียงการใช้งานโปรแกรมป้องกันไวรัสคอมพิวเตอร์ประจำเครื่องของกำลังพลและข้าราชการเท่านั้น และขอยืนยันว่าหน่วยงานไม่มีส่วนเกี่ยวข้องกับการติดตามเฝ้าระวังนักกิจกรรมทางการเมือง

/๒.๒.๓ ข้อเท็จจริง...

๒.๒.๓ ข้อเท็จจริงจากหน่วยงานที่เกี่ยวข้อง

๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑.๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีหน้าที่หลักในการเฝ้าระวังภัยคุกคามทางเทคโนโลยีและรับเรื่องร้องเรียนจากประชาชน โดยเฉพาะการดำเนินการต่อเว็บไซต์ที่ผิดกฎหมาย ไม่มีอำนาจที่จะใช้งานสปายแวร์ ในเรื่องข้อกล่าวหาว่าหน่วยงานของรัฐใช้งานสปายแวร์ รัฐมนตรีว่าการกระทรวงได้ตอบคำถามต่อสภาผู้แทนราษฎรแล้ว

๑.๒) การแจ้งเตือนของ [redacted] เป็นการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งกำหนดให้ผู้ให้บริการมีหน้าที่ต้องแจ้งเตือนผู้ใช้บริการ ซึ่งส่วนใหญ่จะเน้นที่ภาพรวมของระบบว่ามีปัญหาการถูกโจมตี ไม่ระบุเจาะจงว่าใครเป็นผู้โจมตี หากได้รับข้อความแจ้งเตือน ควรนำโทรศัพท์เคลื่อนที่ไปให้หน่วยงานที่มีหน้าที่เกี่ยวข้องช่วยตรวจสอบ เช่น หน่วยพิสูจน์หลักฐานทางคอมพิวเตอร์ เนื่องจากโทรศัพท์เคลื่อนที่หรือคอมพิวเตอร์จะมีการเก็บประวัติข้อมูลหรือ log file ของเครื่องไว้เสมอ จะช่วยทำให้เกิดความกระจ่างมากขึ้นว่าเคยติดตั้งซอฟต์แวร์ที่มีความเสี่ยงไว้หรือไม่ อย่างไรก็ดี การทำงานของสปายแวร์จะมีกระบวนการลบร่องรอยการโจมตี ผู้ใช้หรือบุคคลธรรมดาที่ไม่มีความรู้ทางเทคนิคย่อมไม่สามารถตรวจสอบได้โดยง่าย แต่จำเป็นต้องใช้ผู้เชี่ยวชาญที่มีความรู้ด้านนี้โดยเฉพาะ

๑.๓) จากการติดตามข่าวสารที่เกี่ยวข้องพบว่ากรณีการถูกสปายแวร์โจมตีเกิดขึ้นมานานหลายปีแล้ว อย่างไรก็ดี ต้องมีความชัดเจนก่อนว่า การแจ้งเตือนดังกล่าวไม่ใช่การแจ้งเตือนว่ามีการเข้าถึงที่ผิดปกติบนแอปพลิเคชันสื่อสังคมออนไลน์ อันเกิดขึ้นจากการใช้งานของผู้ใช้เอง เช่น การที่ผู้ใช้งานได้ใช้งานผ่านระบบเครือข่ายส่วนตัวเสมือน (Virtual Private Network - VPN) ซึ่งจะทำให้เกิดการตรวจจับแอปพลิเคชันว่าผู้ใช้งานไม่ได้เข้าถึงหรือใช้งานแอปพลิเคชันในขอบเขตของประเทศไทยตามปกติ หรือการใช้งานแอปพลิเคชันบางประเภท (third party application) ที่เชื่อมโยงการใช้งานกับแอปพลิเคชันสื่อสังคมออนไลน์แบบอัตโนมัติ ทำให้แอปพลิเคชันสื่อสังคมออนไลน์แจ้งเตือนการเข้าถึงหรือการใช้งานที่ผิดปกติได้ ทั้งนี้ มีข้อสังเกตว่าผู้เสียหายตามคำร้องเป็นกลุ่มที่มีความเชื่อมโยงกันบนสื่อสังคมออนไลน์ จึงมีแนวโน้มที่จะติดตั้งแอปพลิเคชันเดียวกันด้วยวิธีการกดรับลิงก์ซึ่งอาจมีความเสี่ยงที่จะถูกโจมตีข้อมูล การแจ้งเตือนที่ได้รับอาจเกิดขึ้นเพราะการติดตั้งแอปพลิเคชันดังกล่าว

๒) [redacted]

๒.๑) [redacted] ได้ออกแบบการแจ้งเตือนมาเพื่อช่วยเหลือผู้ใช้งานที่อาจถูกโจมตีโดยผู้โจมตีที่ได้รับการสนับสนุนจากรัฐ การตรวจจับการโจมตีดังกล่าวอาศัยสัญญาณข่าวกรองภัยคุกคาม (threat intelligence signals) ที่มักไม่สมบูรณ์และไม่ครบถ้วน อาจเป็นไปได้

/ว่าการแจ้งเตือน...

ว่าการแจ้งเตือนบางอย่างของ [redacted] เป็นสัญญาณเตือนที่ผิดพลาดหรือไม่สามารถตรวจพบการโจมตีบางอย่างได้ ทั้งนี้ [redacted] ไม่สามารถตอบได้โดยตรงว่าผู้ใช้งานรายใดรายหนึ่งถูกโจมตีสำเร็จแล้วหรือไม่

๒.๒) [redacted] อาศัยข้อมูลงานวิจัยที่ดำเนินการโดยห้องปฏิบัติการ Citizen Lab ซึ่งเป็นกลุ่มนักวิจัยของมหาวิทยาลัย Toronto ที่ระบุว่ามีการโจมตีผู้ใช้งานโดยสปายแวร์เพกาซัส มาใช้ในการฟ้องคดีต่อ [redacted] เมื่อวันที่ ๒๓ พฤศจิกายน ๒๕๖๔

๒.๓) [redacted] ได้รับข้อมูลทางเทคนิคจากห้องปฏิบัติการ Citizen Lab เกี่ยวกับการใช้ประโยชน์ของ [redacted] ครั้งแรกเมื่อวันที่ ๗ กันยายน ๒๕๖๔ หลังจากการวิจัยและทดสอบอย่างรอบด้านแล้ว [redacted] ได้เปิดตัวระบบปฏิบัติการ iOS รุ่นที่ ๑๔.๘ เมื่อวันที่ ๑๓ กันยายน ๒๕๖๔ โดยได้อัปเดตระบบความปลอดภัยเพื่อแก้ไขปัญหาที่เกิดขึ้น และจะทำการอัปเดตระบบปฏิบัติการเพื่อจัดการปัญหาความปลอดภัยเป็นประจำ ซึ่งรวมถึงปัญหาที่เกี่ยวข้องกับสปายแวร์ต่าง ๆ ด้วย

๒.๒.๔ ความเห็นของพยานผู้เชี่ยวชาญ

[redacted] อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ [redacted] ได้ให้ข้อคิดเห็น ดังนี้

๑) ระบบปฏิบัติการของคอมพิวเตอร์และโทรศัพท์เคลื่อนที่ รวมถึงซอฟต์แวร์ต่าง ๆ มักมีช่องโหว่ (vulnerability) ที่ผู้ผลิตไม่ทราบอยู่เสมอ การโจมตีของสปายแวร์ก็มักโจมตีช่องโหว่ที่ผู้ผลิตยังไม่ทราบหรือที่เรียกว่า Zero-day attack หากผู้ผลิตทราบว่าผลิตภัณฑ์ของตนเองมีช่องโหว่ก็จะทำการอัปเดตเพื่ออุดช่องโหว่ที่เกิดขึ้น แต่การอัปเดตซอฟต์แวร์ทำได้เพียงป้องกันการโจมตีจากสปายแวร์ได้ในระยะหนึ่ง แต่ในอนาคต ผู้ไม่หวังดีอาจหาช่องโหว่อื่นมาใช้โจมตีได้อีก จึงต้องมีการอัปเดตอยู่เสมอ

๒) ในการโจมตีของไวรัสคอมพิวเตอร์ โดยทั่วไปมักจะใช้วิธีหลอกล่อให้ผู้ใช้งานคลิกหรือกดติดตั้งไวรัสก่อน ส่วนการทำงานของสปายแวร์เพกาซัสไม่จำเป็นต้องคลิกหรือกดติดตั้ง เพียงแค่ทราบ IP Address ของอุปกรณ์เป้าหมายหรือหมายเลขโทรศัพท์เคลื่อนที่ก็สามารถโจมตีได้ เมื่อเจาะระบบอุปกรณ์ได้แล้ว จะทำการดักและสำเนาข้อมูลต่าง ๆ ไปยังเซิร์ฟเวอร์ของสปายแวร์ สามารถเปิดกล้องและดักฟังเสียงจากไมโครโฟนได้ การใช้งานสปายแวร์เพกาซัสเพื่อโจมตีจะมีลักษณะของการระบุเป้าหมายโดยเฉพาะ เกิดจากความตั้งใจหรือจงใจ ไม่ใช่การโจมตีแบบสุ่มเลือก หากถูกโจมตีย่อมแสดงว่าเป็นผู้ที่ถูกเพ่งเล็งจากผู้ไม่ประสงค์ดี

/๓) การได้รับ...

๓) การได้รับแจ้งเตือนจาก [redacted] แสดงว่าเป้าหมายถูกโจมตีแล้ว เนื่องจากต้องมีการเก็บหลักฐานพอสมควร โดย [redacted] มีระบบอัตโนมัติคอยเฝ้าระวังการส่งข้อมูลที่ผิดปกติจากการใช้งานทั่วไปของผู้ใช้งานผลิตภัณฑ์ อย่างไรก็ดี การทำงานของสปายแวร์มีความไหวตัวสูง สามารถฝังตัวและหลบหลีกการตรวจจับได้ง่าย เพียงแค่เปิดหรือปิดเครื่องก็ทำให้ไม่พบสปายแวร์ในเครื่องแล้ว สปายแวร์มีวิธีการทางเทคนิคที่ทำให้ไม่สามารถตรวจสอบได้ว่าผู้โจมตีคือใคร การเก็บพยานหลักฐานของการเจาะระบบจึงเป็นไปได้ยาก ดังนั้น ในฐานะผู้ให้บริการ การกระทำใด ๆ ของ [redacted] ซึ่งมีความรับผิดชอบในทางกฎหมาย จึงทำได้เพียงแจ้งเตือนในลักษณะที่ไม่ยืนยันข้อเท็จจริง แต่เลี่ยงไปใช้คำว่า “อาจจะ” แทน อย่างไรก็ดี สามารถตรวจสอบการโจมตีได้จากบันทึกข้อมูลการติดต่อสื่อสารของระบบคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ หรือที่เรียกว่า log file จะพบว่ามีคนกลาง (man in the middle) คอยดักข้อมูลจากโทรศัพท์เคลื่อนที่หรือคอมพิวเตอร์ของเหยื่อ ซึ่งสังเกตได้จาก IP Address ที่ผิดปกติ

๔) ผู้ผลิตสปายแวร์เพกาซัสอาจขายให้ผู้ใดก็ได้ที่ต้องการนำไปใช้โจมตีเพื่อสอดแนมข้อมูล ผู้ใช้งานสปายแวร์เพกาซัสอาจนำไปใช้ทั้งในทางที่เป็นประโยชน์ เช่น การป้องกันและปราบปรามอาชญากรรม หรือในทางที่ก่อให้ผลร้ายก็ได้ ทั้งนี้ มีความเป็นไปได้อย่างมากที่หน่วยงานของรัฐจะใช้งานสปายแวร์ แต่ไม่แน่ชัดว่าเป็นสปายแวร์เพกาซัสหรือไม่ ต้องตรวจสอบการใช้งบประมาณ แต่มีความเป็นไปได้ว่าจะไม่สามารถตรวจสอบได้โดยง่าย เนื่องจากเป็นงบประมาณลับ ไม่เปิดเผยต่อสาธารณะ โดยเมื่อหน่วยงานของรัฐได้จัดซื้อมาแล้ว จะได้รับบัญชีผู้ใช้งาน (account) และรหัสผ่านในการเข้าใช้งาน รวมถึงมีการคิดค่าบริการเป็นรายเดือน

๕) บุคคลทั่วไปไม่สามารถทราบเลยว่าอุปกรณ์สื่อสารของตนเองถูกโจมตีจากสปายแวร์ ทำได้เพียงแนะนำให้ใช้งานเฉพาะแอปพลิเคชันที่ไม่มีความเสี่ยงเท่านั้น อย่างไรก็ดี อาจสังเกตจากความผิดปกติของอุปกรณ์สื่อสารของตนเองได้ เช่น แบตเตอรี่ร้อนและหมดเร็วกว่าปกติทั้งที่ไม่ค่อยได้ใช้งาน ซึ่งอาจเกิดจากการที่อุปกรณ์ส่งข้อมูลอยู่ตลอดเวลา หรืออุปกรณ์มีการใช้งานโปรแกรมหรือแอปพลิเคชันบางอย่างอยู่

๖) การตรวจสอบของห้องปฏิบัติการ Citizen Lab มีความน่าเชื่อถือ เพราะเป็นหน่วยงานวิจัยทางวิชาการของสถาบันการศึกษาที่มีความรู้ในเรื่องนี้โดยเฉพาะ ส่วนในประเทศไทยยังไม่พบว่ามีห้องปฏิบัติการที่สามารถดำเนินการตรวจสอบในลักษณะเดียวกันได้ แต่อาจมีผู้เชี่ยวชาญที่มีความรู้ในเรื่องนี้จำนวนหนึ่ง

๒.๒.๕ การแสวงหาข้อเท็จจริงของพนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่ได้สืบค้นข้อมูลที่เกี่ยวข้องแล้ว ปรากฏข้อเท็จจริงดังนี้

๑) รายงานวิจัยที่จัดทำโดยห้องปฏิบัติการ Citizen Lab เรื่อง “GeckoSpy : Pegasus Spyware Used against Thailand’s Pro-Democracy Movement”[๔] ซึ่งเผยแพร่บนเว็บไซต์เมื่อวันที่ ๑๗ กรกฎาคม ๒๕๖๕ ได้ระบุข้อค้นพบการใช้งานสปายแวร์เพกาซัสต่อขบวนการเรียกร้องประชาธิปไตยในประเทศไทย สรุปได้ดังนี้

๑.๑) ในปี ๒๕๕๖ และปี ๒๕๕๘ ปรากฏข่าวว่ารัฐบาลไทยได้จัดซื้อเทคโนโลยีสอดแนมข้อมูลจาก [redacted] ของประเทศอิตาลี และจากรายงานวิจัย[๕] ที่เผยแพร่เมื่อปี ๒๕๖๓ ของห้องปฏิบัติการ Citizen Lab ระบุว่า หน่วยงานของรัฐในประเทศไทยอย่างน้อย ๓ แห่ง ได้แก่ กองบัญชาการตำรวจปราบปรามยาเสพติด กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร และหน่วยข่าวกรองทางทหาร กองทัพบก ได้ทำสัญญากับ [redacted] ซึ่งขายผลิตภัณฑ์สนับสนุนการทำงานของสปายแวร์เพกาซัส โดยมีความสามารถในการดักฟังข้อมูลการโทร ข้อความสั้น และติดตามตำแหน่งของโทรศัพท์เคลื่อนที่

๑.๒) การจัดทำรายงานวิจัยฉบับนี้ได้รับความร่วมมือจากองค์กรภาคประชาสังคม คือ iLaw และ DigitalReach ในการเก็บรวบรวมข้อมูลและหลักฐานทางดิจิทัลจากผู้ตกเป็นเป้าหมายการโจมตีในประเทศไทย จากนั้นได้วิเคราะห์ในทางเทคนิคคอมพิวเตอร์ต่อหลักฐานที่ได้มา เพื่อจำแนกว่ามีการโจมตีด้วยสปายแวร์เพกาซัสหรือสปายแวร์อื่น ๆ หรือไม่ จึงได้ทราบว่ามีผู้ถูกโจมตีด้วยสปายแวร์เพกาซัสอย่างน้อย ๓๐ คน ประกอบด้วยนักกิจกรรม นักวิชาการ นักกฎหมาย และผู้ทำงานในองค์กรภาคประชาสังคม การโจมตีเกิดขึ้นตั้งแต่เดือนตุลาคม ๒๕๖๓ ถึงเดือนพฤศจิกายน ๒๕๖๔ ซึ่งเป็นช่วงที่มีการจัดกิจกรรมหรือการชุมนุมเรียกร้องในประเด็นต่าง ๆ เป็นวงกว้างในประเทศไทย การโจมตีส่วนใหญ่เกิดขึ้นกับผู้ที่เป็นแกนนำสำคัญ โดยบางคนถูกโจมตีหลายครั้งในช่วงดังกล่าว

๑.๓) การตรวจสอบอาศัยวิธีการเก็บรวบรวมหลักฐานทางนิติวิทยาศาสตร์ (forensic evidence) จากโทรศัพท์เคลื่อนที่ยี่ห้อไอโฟน โดยใช้การสุ่มตัวอย่างแบบอ้างอิงด้วยบุคคลและ

/ผู้เชี่ยวชาญ...

---

[๔] จาก GeckoSpy: Pegasus Spyware Used against Thailand’s Pro-Democracy Movement, โดย [redacted] ๑๗ กรกฎาคม ๒๕๖๕, สืบค้นจาก https://[redacted]2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement, เมื่อวันที่ ๗ พฤศจิกายน ๒๕๖๖

[๕] จาก Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles, โดย [redacted] ๑ ธันวาคม ๒๕๖๓, สืบค้นจาก https://[redacted]/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles, เมื่อวันที่ ๗ พฤศจิกายน ๒๕๖๖

ผู้เชี่ยวชาญ (snowball-sampling method) ซึ่งในชั้นแรกจะตรวจสอบจากบุคคลที่ได้รับการแจ้งเตือนจาก [redacted] จากนั้นจะขยายการตรวจสอบเพิ่มเติมไปถึงบุคคลอื่นที่อยู่ในบัญชีรายชื่อติดต่อของบุคคลกลุ่มแรก โดยทั่วไปจะทำการเก็บรวบรวมและวิเคราะห์หลักฐานโดยจำแนกหลักฐานที่มีความเชื่อมโยงกับสปายแวร์เพกาซัส ทั้งลักษณะกระบวนการทำงานและหลักฐานที่อยู่ในบันทึกประวัติการทำงานของโทรศัพท์เคลื่อนที่ (phone logs) โดยใช้ตัวชี้วัด (indicators) ที่ได้มาจากการติดตามการโจมตีด้วยสปายแวร์เพกาซัสตลอด ๖ ปี ซึ่งรวมถึงตัวอย่างรหัสของสปายแวร์เพกาซัสที่รวบรวมได้จากอุปกรณ์ที่ถูกโจมตี ในบางกรณี หลักฐานที่ได้จากกระบวนการวิเคราะห์จะถูกระบุช่วงเวลาที่เกี่ยวข้อง (associated timestamp) ไว้ ทำให้สามารถรู้วันที่ที่มีการโจมตีได้แน่ชัด แต่โดยทั่วไปแล้ว จะทำได้เพียงคาดการณ์ช่วงเวลาที่มีการโจมตี โดยจะทำการระบุเป็นห้วงระยะเวลาไว้แทน ทั้งนี้ ข้อค้นพบว่ามีการโจมตีเกิดขึ้นชี้ให้เห็นว่า ผู้วิจัยได้ทำการตรวจสอบด้วยความมั่นใจเป็นอย่างมากว่าโทรศัพท์เคลื่อนที่ดังกล่าวถูกเจาะระบบด้วยสปายแวร์เพกาซัสจนสำเร็จ และไม่เชื่อว่าจะมีแนวทางที่น่าเชื่อถืออื่นมาโต้แย้งข้อค้นพบได้

๑.๔) ผู้วิจัยจะไม่เผยแพร่ตัวชี้วัดสำหรับการตรวจสอบการโจมตีด้วยสปายแวร์ที่กำลังเกิดขึ้นไว้ทั้งหมด เพื่อที่จะยังคงทำให้สามารถตรวจสอบการโจมตีที่อาจเกิดขึ้นได้อีกในอนาคต ทั้งนี้ ผู้วิจัยได้ส่งข้อมูลหลักฐานที่ได้จากกระบวนการวิเคราะห์บางส่วนไปให้ห้องปฏิบัติการด้านความปลอดภัยทางไซเบอร์ขององค์กรแอมเนสตี้ อินเตอร์เนชั่นแนล (Amnesty International's Security Lab) ตรวจสอบด้วยอีกทางหนึ่ง แต่ไม่ได้เปิดเผยผลการค้นพบ โดยจากกระบวนการวิเคราะห์ที่มีความแตกต่างกัน ยังคงยืนยันผลเช่นเดิมว่ามีการโจมตีด้วยสปายแวร์เพกาซัสเกิดขึ้น

๑.๕) หลักฐานที่ได้จากกระบวนการตรวจสอบโทรศัพท์เคลื่อนที่ที่ถูกโจมตีพบว่า สปายแวร์เพกาซัสมีการใช้ระบบการโจมตีแบบไม่ต้องคลิก หรือ Zero-click exploit เพื่อโจมตีช่องโหว่ของระบบปฏิบัติการที่ผู้ผลิตยังไม่ทราบหรือยังไม่สามารถแก้ไขได้ โดยที่ไม่พบหลักฐานว่ามีการโจมตีแบบคลิกหนึ่งครั้ง

๑.๖) ผู้วิจัยพบการใช้งานสปายแวร์เพกาซัสในประเทศไทยครั้งแรกเมื่อเดือนพฤษภาคม ๒๕๕๗ โดยพบข้อมูลที่ส่งเข้ามายังกลุ่มของเซิร์ฟเวอร์สปายแวร์เพกาซัสจากชื่อที่อยู่เว็บไซต์ (domain name) ซึ่งมีความเกี่ยวข้องกับประเทศไทย เช่น [redacted] แต่ไม่สามารถจำแนกได้ว่ามาจากหน่วยงานใดของรัฐ และเมื่อปี ๒๕๕๙ ผู้วิจัยพบข้อมูลที่ถูกส่งจากชื่อที่อยู่เว็บไซต์ที่จดทะเบียนในประเทศไทยไปยังกลุ่มของเซิร์ฟเวอร์สปายแวร์เพกาซัสโดยใช้อีเมล ๒ บัญชี คือ (๑) "(ปกปิด)[redacted] และ (๒) อีเมลที่ใช้เพื่อเปิดบัญชีแอปพลิเคชัน Facebook ชื่อบัญชีว่า [redacted] โดยที่ตัวย่ออักษรภาษาอังกฤษ [redacted] นี้ อาจหมายถึงกองบัญชาการตำรวจปราบปรามยาเสพติด (Narcotics Suppression Bureau: NSB) นอกจากนี้ ในปี ๒๕๖๑

/ผู้วิจัย...

ผู้วิจัยได้ตรวจพบผู้ใช้งานสปายแวร์เพกาซัส ซึ่งจากการวิเคราะห์ด้วยวิธีการทางเทคนิคพบว่า ผู้ใช้งานดังกล่าวดำเนินการอยู่เฉพาะในประเทศไทย จึงได้ตั้งชื่อว่า [redacted] นอกจากนี้ผู้วิจัยพบว่า ยังมีผู้ใช้งานสปายแวร์เพกาซัสดำเนินการอยู่ในประเทศไทยในวันที่มีการเผยแพร่รายงานนี้อย่างน้อย ๑ ราย แต่ไม่สามารถระบุได้ว่าเป็นหน่วยงานใดของรัฐ หรือเป็นหน่วยงานเดียวกับที่เคยตรวจพบว่ามีการใช้งานเมื่อปี ๒๕๕๗ - ๒๕๖๑ หรือไม่

๑.๗) ผู้วิจัยไม่สามารถระบุได้อย่างชัดเจนว่าการโจมตีด้วยสปายแวร์เพกาซัสตามรายงานนี้เป็นการดำเนินงานของหน่วยงานใดของรัฐ แต่ [redacted] ที่เป็นผู้ผลิตมักอ้างอยู่เสมอว่าจะขายผลิตภัณฑ์ให้แก่รัฐบาลเท่านั้น ซึ่งข้อเท็จจริงนี้ มีความสอดคล้องกับข้อมูลจากรายงานการวิจัยหลายฉบับและการรายงานข่าวของสื่อมวลชนหลายแห่งในช่วงเวลาที่ผ่านมา จึงอาจสรุปได้ว่า การค้นพบสปายแวร์เพกาซัสมีความเกี่ยวข้องกับหน่วยงานของรัฐ อย่างไรก็ดี ห้องปฏิบัติการ Citizen Lab ได้เผยแพร่รายงานหลายฉบับว่ามีการใช้สปายแวร์เพกาซัสโดยไม่ชอบต่อผู้เสียหายจำนวนมากในหลายประเทศ ไม่ว่าจะเป็นนักวิทยาศาสตร์ สื่อมวลชน และทนายความ แต่ [redacted] มักจะตอบโต้รายงานดังกล่าวด้วยการอ้างว่ามีกระบวนการสอบสวนภายในของบริษัทแล้ว และไม่พบกรณีตามที่มีการกล่าวอ้าง

๑.๘) แม้หลักฐานที่ได้จากการตรวจวิเคราะห์ข้อมูลที่รวบรวมจากอุปกรณ์ที่ถูกโจมตี ยังไม่สามารถยืนยันหรือระบุตัวตนของผู้ใช้งานได้อย่างชัดเจน แต่ก็ถือเป็นหลักฐานแวดล้อมที่ชี้ให้เห็นว่า หน่วยงานของรัฐในประเทศไทยเป็นผู้ใช้งานสปายแวร์เพกาซัส เนื่องจากรัฐบาลไทยได้ประโยชน์อย่างมากจากการโจมตีผู้เสียหายที่เป็นนักกิจกรรม นักเคลื่อนไหวทางการเมือง นักวิชาการที่มีความคิดเห็นแตกต่างจากรัฐบาล ซึ่งทำให้ทราบถึงความเคลื่อนไหวของกลุ่ม วิธีการระดมทุน และบทบาทที่แต่ละคนมีในการเคลื่อนไหวทำกิจกรรม ประกอบกับช่วงเวลาที่ผู้เสียหายถูกโจมตีมีความเชื่อมโยงอย่างใกล้ชิดกับเหตุการณ์ทางการเมืองในประเทศไทย โดยเฉพาะในช่วงเวลาไม่นานก่อนการนัดหมายชุมนุมประท้วงหรือการจัดกิจกรรมทางการเมือง อีกทั้ง มีการค้นพบหลักฐานการใช้งานสปายแวร์เพกาซัสในประเทศไทยมาเป็นเวลานานแล้ว ซึ่งบ่งชี้ว่ารัฐบาลไทยน่าจะเข้าถึงการใช้งานสปายแวร์เพกาซัสในช่วงดังกล่าว

๑.๙) ผู้วิจัยเห็นว่ามีความเป็นไปได้น้อยมากที่ผู้ใช้งานสปายแวร์เพกาซัสตามรายงานวิจัยนี้จะเป็นหน่วยงานอื่นที่ไม่ได้อยู่ในประเทศไทย เนื่องจากการโจมตีอย่างเป็นระบบและเป็นวงกว้างต่อบุคคลที่มีชื่อเสียงในประเทศอื่น เป็นภารกิจที่มีความเสี่ยงและมีความเป็นไปได้ที่จะถูกเปิดโปง ซึ่งที่ผ่านมาก็เคยพบว่ามีการเปิดโปงการใช้งานสปายแวร์เพกาซัสมาก่อนหน้านี้แล้ว

/๒) รายงาน...

๒) รายงานความโปร่งใสและความรับผิดชอบ (Transparency and Responsibility Report) ของ [redacted] ที่เผยแพร่เมื่อปี ๒๕๖๔[๖] และปี ๒๕๖๖[๗] ระบุข้อมูลที่เกี่ยวข้องกับ [redacted] และสปายแวร์เพกาซัส สรุปได้ดังนี้

๒.๑) [redacted] ก่อตั้งเมื่อปี ๒๕๕๓ ที่ประเทศอิสราเอล เป็นบริษัทผู้พัฒนาผลิตภัณฑ์ทางเทคโนโลยีหลายประเภท และขายสิทธิการใช้งานผลิตภัณฑ์ (license) ให้แก่ผู้ซื้อ โดยมีสปายแวร์เพกาซัสเป็นผลิตภัณฑ์ที่มีชื่อเสียงมากที่สุด ทั้งนี้ บริษัทไม่ได้เป็นผู้ใช้งานสปายแวร์เพกาซัสด้วยตัวเอง แต่จะขายสิทธิการใช้งานให้แก่หน่วยงานด้านข่าวกรองและหน่วยงานบังคับใช้กฎหมายของประเทศต่าง ๆ เพื่อการสืบสวนและป้องกันภัยคุกคามต่อความมั่นคงของรัฐ การก่อการร้าย และการก่ออาชญากรรมที่มีความร้ายแรงตามที่กฎหมายได้ให้อำนาจไว้ เช่น การค้ามนุษย์ การค้าอาวุธโดยผิดกฎหมาย การค้ายาเสพติด สื่อลามกอนาจารเด็ก หรืออาชญากรรมทางการเงิน อย่างไรก็ดี บริษัทจะไม่ทราบข้อมูลเกี่ยวกับบุคคลที่เป็นเป้าหมายหรือแผนการที่หน่วยงานของรัฐจะนำผลิตภัณฑ์ไปใช้ช่วยเหลือในการสืบสวนหรือการปฏิบัติงาน เนื่องจากเป็นข้อมูลที่เป็นความลับ

๒.๒) บริษัทมีกระบวนการกลั่นกรองประเมินความเสี่ยงและความเหมาะสมของผู้ซื้อก่อนการซื้อขาย เพื่อป้องกันการใช้ผลิตภัณฑ์ของบริษัทไปในทางที่ไม่ชอบ และเนื่องจากสปายแวร์เพกาซัสเป็นผลิตภัณฑ์ที่ถูกจัดอยู่ในหมวดหมู่ “อุปกรณ์ทางทหาร (Defense Article)” ที่ต้องควบคุมการส่งออกอย่างเข้มงวด บริษัทจึงต้องได้รับใบอนุญาตการส่งออกจากหน่วยงานควบคุมการส่งออกของกระทรวงกลาโหมอิสราเอล (the Israeli Ministry of Defense’s Defense Exports Control Agency: “DECA”) ก่อนที่จะมีการซื้อขายผลิตภัณฑ์ทุกครั้ง นอกจากนี้บริษัทจะตรวจสอบโดยทันที หากมีการกล่าวอ้างว่ามีการใช้งานสปายแวร์เพกาซัสไปในทางที่ไม่ชอบ โดยเมื่อตรวจสอบแล้วพบว่ามีการใช้งานลักษณะดังกล่าวจริง บริษัทจะดำเนินการตามความร้ายแรงที่พบ ซึ่งรวมถึงการยกเลิกสัญญาการขายสิทธิใช้งานผลิตภัณฑ์

๒.๓) สปายแวร์เพกาซัสไม่ใช่เครื่องมือสอดแนมข้อมูลในวงกว้าง (mass surveillance tool) แต่ใช้กับเป้าหมายเฉพาะรายและใช้ได้เพียงครั้งละ ๑ เป้าหมาย ซึ่งจะอาศัยหมายเลขโทรศัพท์เคลื่อนที่ที่ได้จำแนกแล้วว่าเป็นของอาชญากรหรือผู้ต้องสงสัยที่มีความเกี่ยวข้องกับการก่อการร้าย สปายแวร์เพกาซัสไม่สามารถควบคุมอุปกรณ์ที่เป็นเป้าหมายได้อย่างเบ็ดเสร็จ และไม่

/สามารถ...

---

[๖] จาก Transparency and Responsibility Report 2021, โดย [redacted] วันที่ ๓๐ มิถุนายน ๒๕๖๔, สืบค้นจาก https://www.[redacted]/wp-content/uploads/2021/06/ReportBooklet.pdf, เมื่อวันที่ ๒๓ พฤศจิกายน ๒๕๖๖

[๗] จาก Transparency and Responsibility Report 2023, โดย [redacted] วันที่ ๓๑ ธันวาคม ๒๕๖๖, สืบค้นจาก https://www.[redacted]/wp-content/uploads/2023/12/2023-Transparency-and-Responsibility-Report.pdf, เมื่อวันที่ ๑๐ มกราคม ๒๕๖๗

สามารถจัดการข้อมูลต่าง ๆ ที่อยู่ในอุปกรณ์ได้ ไม่ว่าจะเป็นการเพิ่ม เปลี่ยนแปลง หรือลบข้อมูล ทำได้เพียงแค่เฝ้าดูและจำแนกแยกแยะข้อมูลเฉพาะบางอย่าง โดยจะทำงานในลักษณะคล้ายกับการดักฟังแบบดั้งเดิม อีกทั้งยังไม่สามารถเจาะเข้าไปในเครือข่ายคอมพิวเตอร์ (computer networks) ระบบปฏิบัติการ (operating systems) ของคอมพิวเตอร์ หรือข้อมูลเครือข่าย (data networks) ทำได้เพียงการติดตั้งบนโทรศัพท์เคลื่อนที่เท่านั้น

๒.๔) ในปี ๒๕๖๔ มีผู้ใช้งานสปายแวร์เพกาซัส จำนวน ๖๐ ราย ใน ๔๐ ประเทศทั่วโลก โดยร้อยละ ๓๘ เป็นหน่วยงานด้านการบังคับใช้กฎหมาย (Law Enforcement Agencies) ร้อยละ ๕๑ เป็นหน่วยงานด้านข่าวกรอง (Intelligence Agencies) และร้อยละ ๑๑ เป็นหน่วยงานด้านการทหาร ส่วนในปี ๒๕๖๖ มีผู้ใช้งานสปายแวร์เพกาซัส จำนวน ๕๖ ราย ใน ๓๑ ประเทศ โดยร้อยละ ๔๖ เป็นหน่วยงานด้านการบังคับใช้กฎหมาย ร้อยละ ๔๖ เป็นหน่วยงานด้านข่าวกรอง และร้อยละ ๙ เป็นหน่วยงานด้านการทหาร

๓) ข้อมูลเกี่ยวกับการดำเนินคดี การสอบสวน และการจัดทำรายงาน อันเนื่องมาจากการใช้งานสปายแวร์เพกาซัสโดยมิชอบ สรุปได้ ดังนี้

๓.๑) เมื่อวันที่ ๒๓ พฤศจิกายน ๒๕๖๔ [redacted] ได้ฟ้อง [redacted] และ [redacted] เป็นคดีต่อศาลในมลรัฐแคลิฟอร์เนีย สหรัฐอเมริกา[๘] เพื่อเรียกร้องให้แสดงความรับผิดชอบต่อการสอดส่องและการเจาะจงกลุ่มเป้าหมายมายังผู้ใช้ผลิตภัณฑ์ของ [redacted] จากการฟ้องคดีทำให้ทราบข้อมูลใหม่เกี่ยวกับวิธีการที่เรียกว่า “FORCEDENTRY” ซึ่ง [redacted] ได้นำมาใช้ในการทำให้อุปกรณ์ของผู้เสียหายถูกเจาะด้วยสปายแวร์เพกาซัส เพื่อเข้าถึงไมโครโฟน กล้อง และข้อมูลสำคัญอื่น ๆ บนอุปกรณ์ของผู้ใช้งาน โดยวิธีการดังกล่าวได้ถูกตรวจพบครั้งแรกโดยห้องปฏิบัติการ Citizen Lab อีกทั้งยังพบว่าเมื่อปี ๒๕๖๒ [redacted] ผู้พัฒนาแอปพลิเคชันการสื่อสาร [redacted] ได้ยื่นฟ้อง [redacted] ต่อศาลในสหรัฐอเมริกาด้วยเช่นกัน โดยกล่าวหาว่าเป็นผู้อยู่เบื้องหลังการโจมตีทางไซเบอร์ ด้วยการใช้สปายแวร์เพกาซัสฝังตัวในโทรศัพท์เคลื่อนที่ของผู้ใช้งานประมาณ ๑,๔๐๐ ราย[๙] ขณะจัดทำรายงานฉบับนี้ คดีทั้งสองยังอยู่ระหว่างการพิจารณาคดีของศาล

/๓.๒) ตั้งแต่...

---

[๘] [redacted] เพื่อระงับการใช้สปายแวร์ที่ได้รับการสนับสนุนจากรัฐ, โดย [redacted] วันที่ ๒๔ พฤศจิกายน ๒๕๖๔, สืบค้นจาก [redacted] เมื่อวันที่ ๒๕ ตุลาคม ๒๕๖๖

[๙] จาก เพกาซัส สปายแวร์ : ไอลอว์เปิดรายงานพบ 30 นักวิชาการ-นักกิจกรรมการเมืองไทยถูกสปายแวร์สอดแนม, โดย [redacted] วันที่ ๑๘ กรกฎาคม ๒๕๖๕, สืบค้นจาก [redacted] เมื่อวันที่ ๒๗ ตุลาคม ๒๕๖๖

๓.๒) ตั้งแต่ปี ๒๕๖๐ เป็นต้นมา มีการฟ้องร้องเป็นคดีต่อศาล รวมถึงการตั้งคณะกรรมการขึ้นมาเป็นการเฉพาะเพื่อสอบสวนการใช้งานสปายแวร์เพกาซัสโดยมิชอบในประเทศต่าง ๆ อีก ๓๐ กรณี[๑๐] โดยพบว่าเหยื่อที่ถูกโจมตี ได้แก่ ผู้สื่อข่าว ผู้ที่มีความคิดเห็นแตกต่างจากรัฐบาล ผู้นำขององค์กรภาคประชาสังคม นักกิจกรรม นักปกป้องสิทธิมนุษยชน นักวิชาการ ไปจนถึงนักการเมือง ขณะที่เมื่อเดือนพฤศจิกายน ๒๕๖๔ สำนักอุตสาหกรรมและความปลอดภัย (Bureau of Industry and Security: BIS) ภายใต้กระทรวงพาณิชย์ สหรัฐอเมริกา ได้เพิ่มรายชื่อ [redacted] เข้าไปในบัญชีรายชื่อบริษัทที่เข้าไปมีส่วนร่วมในกิจกรรมที่ขัดต่อความมั่นคงของชาติและผลประโยชน์ด้านนโยบายต่างประเทศของสหรัฐอเมริกา เนื่องจากมีหลักฐานว่ามีการพัฒนาและจัดหาสปายแวร์ให้แก่รัฐบาลหลายประเทศ เพื่อใช้โจมตีเป้าหมายที่เป็นเจ้าหน้าที่ของรัฐ ผู้สื่อข่าว นักธุรกิจ นักกิจกรรม และนักวิชาการ ซึ่งส่งผลให้เกิดการปราบปรามผู้เห็นต่างโดยไม่จำกัดพรมแดน อันเป็นการกระทำที่ขัดกับกฎระเบียบในทางระหว่างประเทศ[๑๑]

๓.๓) เมื่อปี ๒๕๖๕ สำนักงานข้าหลวงใหญ่เพื่อสิทธิมนุษยชนแห่งสหประชาชาติ (Office of the United Nations High Commissioner for Human Rights) ได้เสนอรายงาน เรื่อง “สิทธิในความเป็นอยู่ส่วนตัวในโลกยุคดิจิทัล (The right to privacy in the digital age)”[๑๒] ต่อที่ประชุมคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ (United Nations Human Rights Council: UNHRC) เพื่อมีมติรับรอง โดยในรายงานดังกล่าวได้กล่าวถึงภัยคุกคามของสปายแวร์เพกาซัสไว้เป็นการเฉพาะดังนี้

(๑) สปายแวร์เพกาซัสเป็นสปายแวร์ที่สามารถติดตั้งบนโทรศัพท์เคลื่อนที่ได้โดยที่เป้าหมายไม่รู้ตัว หรือที่เรียกว่า “Zero-click attack” เมื่อถูกติดตั้งแล้วจะสามารถเข้าถึงข้อมูลในโทรศัพท์เคลื่อนที่ได้อย่างทั่วถึงและไม่จำกัด ไม่ว่าจะเป็นกล้อง ไมโครโฟน ข้อมูลระบุตำแหน่ง อีเมล ข้อความ รูปภาพ วิดีโอ หรือแอปพลิเคชันต่าง ๆ โดยเปลี่ยนให้โทรศัพท์เคลื่อนที่

/ของเป้าหมาย...

---

[๑๐] จาก Litigation and other formal complaints related to mercenary spyware, โดย [redacted] ๑๒ ธันวาคม ๒๕๖๑, สืบค้นจาก https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/, เมื่อวันที่ ๑ กุมภาพันธ์ ๒๕๖๗

[๑๑] จาก Commerce Adds [redacted] and Other Foreign Companies to Entity List for Malicious Cyber Activities, โดย U.S. Department of Commerce, ๓ พฤศจิกายน ๒๕๖๔, สืบค้นจาก https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-[redacted]-and-other-foreign-companies-entity-list, เมื่อวันที่ ๑๗ มกราคม ๒๕๖๗

[๑๒] จาก The right to privacy in the digital age, โดย Office of the United Nations High Commissioner for Human Rights, ๔ สิงหาคม ๒๕๖๕, สืบค้นจาก https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age, เมื่อวันที่ ๑๘ ธันวาคม ๒๕๖๖

ของเป้าหมายกลายเป็นเครื่องมือสอดแนมตลอด ๒๔ ชั่วโมง ด้วยความสามารถเช่นนี้ของสปายแวร์เพกาซัส จึงแทบเป็นไปไม่ได้ที่เหยื่อจะหลีกเลี่ยงการถูกโจมตีได้

(๒) แม้สปายแวร์เพกาซัสจะถูกพัฒนาขึ้นเพื่อต่อสู้กับการก่อการร้ายและอาชญากรรม แต่ก็พบว่ามีการใช้งานที่ผิดวัตถุประสงค์บ่อยครั้ง โดยเฉพาะการถูกใช้เพื่อจำกัดควบคุมผู้ที่วิพากษ์วิจารณ์หรือมีความคิดเห็นแตกต่างจากรัฐบาล รวมถึงนักปกป้องสิทธิมนุษยชน

(๓) จากข้อมูลการรายงานข่าวของสื่อมวลชนและรายงานการวิจัยของห้องปฏิบัติการ Citizen Lab หลายฉบับ พบว่ามีผู้ได้รับผลกระทบจากสปายแวร์นี้หลายส่วน เช่น ผู้สื่อข่าวไม่น้อยกว่า ๑๘๙ คน นักปกป้องสิทธิมนุษยชนไม่น้อยกว่า ๘๕ คน ผู้อยู่ในแวดวงการเมืองกว่า ๖๐๐ คน และจากการสืบสวนเพิ่มเติมยังพบว่ามีการสอดแนมผู้พิพากษา ทนายความ แพทย์ และนักวิชาการด้วย

(๔) ในระหว่างการให้ข้อเท็จจริงต่อคณะกรรมการเฉพาะกิจ[๑๓] ที่รัฐสภายุโรป (European Parliament) แต่งตั้งขึ้นเพื่อสอบสวนการใช้งานสปายแวร์เพกาซัส เมื่อปี ๒๕๖๕ [redacted] ยอมรับว่า มีผู้ที่ถูกกำหนดเป็นเป้าหมายของการโจมตีด้วยสปายแวร์เพกาซัส ปีละประมาณ ๑๒,๐๐๐ - ๑๓,๐๐๐ คน

๓.๔) เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๖๕ ผู้ร้องรวมถึงผู้เสียหายที่ถูกโจมตีด้วยสปายแวร์เพกาซัส รวม ๘ คน ได้ยื่นฟ้อง [redacted] ต่อศาลแพ่ง ในคดีละเมิดเพื่อให้ศาลมีคำบังคับให้บริษัทระงับการกระทำที่เป็นการสอดแนมและเข้าถึงข้อมูล รวมทั้งเรียกค่าเสียหาย แต่เมื่อวันที่ ๒๖ พฤศจิกายน ๒๕๖๕ ศาลแพ่งมีคำสั่งให้จำหน่ายคดี เนื่องจากเหตุแห่งการละเมิดของผู้เสียหายแต่ละคนเกิดขึ้นต่างวาระกัน จึงคืนคำฟ้องเพื่อให้ผู้เสียหายยื่นฟ้องคดีใหม่แยกกัน ต่อมาเมื่อวันที่ ๑๓ กรกฎาคม ๒๕๖๖ [redacted] หนึ่งในผู้เสียหายที่ถูกโจมตี ได้ยื่นฟ้องคดี [redacted] ต่อศาลแพ่งอีกครั้ง ศาลมีคำสั่งรับฟ้องและคดียังอยู่ระหว่างการพิจารณา นอกจากนี้ เมื่อวันที่ ๒๐ มิถุนายน ๒๕๖๖ ผู้ร้องและ [redacted] ผู้เสียหายที่ถูกโจมตี ได้ยื่นฟ้องหน่วยงานของรัฐ ๙ หน่วยงาน ต่อศาลปกครอง เนื่องจากอาจมีส่วนเกี่ยวข้องกับการใช้งานสปายแวร์เพกาซัสในประเทศไทย แต่ศาลมีคำสั่งไม่รับฟ้องและจำหน่ายคดีออกจาก

/สารบบความ...

---

[๑๓] Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA)

สารบบความ[๑๔] โดยขณะจัดทำรายงานผลการตรวจสอบฉบับนี้ คดีอยู่ระหว่างการอุทธรณ์ขอให้ศาลปกครองรับฟ้องไว้พิจารณา[๑๕]

๔) ข้อมูลเกี่ยวกับการจัดซื้อสปายแวร์โดยหน่วยงานของรัฐในประเทศไทย สรุปได้ดังนี้

๔.๑) ในระหว่างการพิจารณางบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๖ สมาชิกสภาผู้แทนราษฎรจากพรรคก้าวไกล ซึ่งทำหน้าที่กรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๖ ได้ตั้งข้อสังเกตและขอทราบรายละเอียดเกี่ยวกับ “โครงการจัดหาระบบรวบรวมและประมวลผลข่าวกรองชั้นสูง” ซึ่งเสนอโดยกองบัญชาการตำรวจปราบปรามยาเสพติด สำนักงานตำรวจแห่งชาติ วงเงินงบประมาณ ๓๕๐ ล้านบาท โดยจากการพิจารณาเอกสารในรายละเอียดพบว่า[๑๖] กองบัญชาการตำรวจปราบปรามยาเสพติดได้เคยจัดหา “ระบบเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์” ซึ่งมีคุณสมบัติการทำงานคล้ายกับสปายแวร์มาแล้ว ๔ ครั้ง ได้แก่

(๑) ระบบเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์แบบ ๓ จัดหาเมื่อปี ๒๕๕๗ มีคุณสมบัติในการส่ง Application Agent ไปติดตั้งยังโทรศัพท์เคลื่อนที่ของเป้าหมายเพื่อเข้าถึงข้อมูลข่าวสาร ซึ่งตามเอกสารการของบประมาณระบุว่ายังมีการใช้งานระบบนี้อยู่

(๒) ระบบเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์แบบ ๔ จัดหาเมื่อปี ๒๕๖๒ มีคุณสมบัติในการเข้าถึงข้อมูลเสียงและข้อความสั้นในโทรศัพท์เคลื่อนที่เป้าหมาย

/ในเครือข่าย...

---

[๑๔] จากการสืบค้นข้อมูลเกี่ยวกับการฟ้องคดีต่อศาลปกครองดังกล่าวบนเว็บไซต์ของ iLaw พบว่า เมื่อวันที่ ๒๑ สิงหาคม ๒๕๖๖ ศาลปกครองมีคำสั่งไม่รับฟ้อง เนื่องจากคำฟ้องของผู้ฟ้องคดี เป็นการบรรยายฟ้องที่มีเจตนากล่าวอ้างว่าเจ้าหน้าที่ในสังกัดของผู้ถูกฟ้องคดีกระทำละเมิดเพื่อแสวงหาประโยชน์ในการแสวงหาข้อเท็จจริงและหลักฐานเกี่ยวกับการกระทำความผิดหรือหาตัวผู้กระทำความผิดที่มีโทษทางอาญา ดังนั้น การเข้าถึงข้อมูลคอมพิวเตอร์ดังกล่าว จึงเป็นขั้นตอนการสอบสวนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่มีการบัญญัติโทษทางอาญาให้อำนาจไว้โดยตรง การกระทำละเมิดตามฟ้องจึงเป็นการกระทำละเมิดอันเนื่องมาจากการดำเนินกระบวนการยุติธรรมทางอาญาโดยมิชอบด้วยประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายพิเศษของฝ่ายปกครองที่มีการบัญญัติโทษทางอาญาไว้ กรณีนี้จึงไม่ใช่การคดีพิพาทที่ศาลปกครองมีอำนาจรับฟ้อง

[๑๕] จาก อัพเดทเส้นทางเปิดโปงผู้ใช้เพกาซัส สปายแวร์ปราบชุมนุมในไทย, โดย โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน, วันที่ ๓๐ ตุลาคม ๒๕๖๖, สืบค้นจาก https://www.ilaw.or.th/articles/6266, เมื่อวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๗

[๑๖] จาก แฉ! เอกสารของบฯ ซื้อเพกาซัสจาก สตช. ยอมรับเต็มๆ ใช้มาตั้งแต่ปี 57 ตอนนี้ล้าสมัยขออัพเดทเป็นตัวใหม่, โดย พรรคก้าวไกล, วันที่ ๒๗ กรกฎาคม ๒๕๖๕, สืบค้นจาก https://www.moveforwardparty.org/news/14287, เมื่อวันที่ ๒๐ พฤศจิกายน ๒๕๖๖

ในเครือข่าย 3G และ 4G โดยการจำลองเป็นสถานีฐานและตัวกระจายสัญญาณ รวมถึงสามารถระบุตำแหน่งเป้าหมายได้อย่างแม่นยำ ตามเอกสารการของบประมาณระบุว่ายังมีการใช้งานระบบนี้อยู่

(๓) ระบบเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์แบบ ๓๑ จัดหาเมื่อปี ๒๕๖๓ มีคุณสมบัติในการทำงานร่วมกับชุดเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์แบบ ๓ โดยการส่ง Application Agent ไปติดตั้งบนโทรศัพท์เคลื่อนที่เป้าหมายอย่างลับ ๆ โดยผู้ใช้ไม่จำเป็นต้องเปิดอ่านข้อความ ตามเอกสารการของบประมาณระบุว่ายังมีการใช้งานระบบนี้อยู่

(๔) ระบบเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์ในระบบเครือข่าย Cyber Intelligence จัดหาเมื่อปี ๒๕๖๔ มีคุณสมบัติในการเข้าถึงข้อมูลข่าวสารของอุปกรณ์ต่าง ๆ ที่ต่อผ่านอุปกรณ์ค้นหาเส้นทางเครือข่าย (Router) ของเป้าหมาย และสามารถเข้าถึงข้อมูลภาพของกล้องวงจรปิดระบบ Analog ได้ ตามเอกสารการของบประมาณระบุว่ายังมีการใช้งานระบบนี้อยู่

๔.๒) “ระบบรวบรวมและประมวลผลข่าวกรองชั้นสูง” ที่กองบัญชาการตำรวจปราบปรามยาเสพติดขอจัดซื้อใหม่ในปีงบประมาณ พ.ศ. ๒๕๖๖ นั้น มีคุณสมบัติในการส่ง Application Agent เข้าไปติดตั้งในโทรศัพท์เคลื่อนที่ได้โดยที่เป้าหมายไม่รู้ตัว สามารถรวบรวมข้อมูลข่าวสารจากระยะไกล เป้าหมายไม่จำเป็นต้องอยู่ในพื้นที่เดียวกับเจ้าหน้าที่ สามารถทำงานในระบบปฏิบัติการ iOS และระบบปฏิบัติการ Android ตั้งแต่รุ่นล่าสุดลงไป และจะมีการพัฒนาให้ทันตามการปรับปรุงระบบปฏิบัติการของโทรศัพท์เคลื่อนที่ ภายใน ๔๕ วัน รวมถึงสามารถติดตั้งและรวบรวมข้อมูลเป้าหมายได้ ๑๐ เครื่องพร้อมกัน และรองรับผู้ใช้งานได้ ๕ ผู้ใช้งานพร้อมกัน ทั้งนี้การจัดหาระบบดังกล่าวมีผู้เสนอราคา ๓ ราย โดยพบว่ามีผู้เสนอราคารายหนึ่ง จะทำการจัดหาผลิตภัณฑ์ ยี่ห้อ [redacted] รุ่น [redacted] จากประเทศอิสราเอลด้วย

๕) กฎหมายอื่นที่มีเนื้อหาในลักษณะเดียวกับพระราชบัญญัติวิธีพิจารณาคดียาเสพติด พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม มาตรา ๑๑/๕ ซึ่งเปิดช่องให้เจ้าหน้าที่ของรัฐสามารถใช้งานสปายแวร์หรือเทคโนโลยีสอดแนมเพื่อเข้าถึงข้อมูลในอุปกรณ์สื่อสารซึ่งถูกต้องสงสัยว่ามีการกระทำความผิดตามกฎหมายว่าด้วยยาเสพติด ได้แก่ (๑) พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ มาตรา ๔๖ (๒) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗ มาตรา ๒๕ (๓) พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. ๒๕๕๑ มาตรา ๓๐ และ (๔) พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. ๒๕๕๖ มาตรา ๑๗ และมาตรา ๒๐ โดยกฎหมายเหล่านี้กำหนดเนื้อหาในรูปแบบที่คล้ายกัน กล่าวคือ เจ้าหน้าที่ของรัฐที่มีอำนาจตามกฎหมายแต่ละฉบับสามารถยื่นคำขอฝ่ายเดียวต่อศาลที่มีเขตอำนาจ เพื่อขอให้ศาลมีคำสั่งให้ได้มาซึ่งข้อมูลข่าวสารที่ถูกส่งทางอุปกรณ์สื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อเทคโนโลยี

ทุกรูปแบบที่มีเหตุอันควรเชื่อว่าถูกใช้หรืออาจถูกใช้เพื่อกระทำความผิดตามกฎหมายข้างต้น โดยศาลต้องพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคล สิทธิอื่น ประกอบกับเหตุผลและความจำเป็น และสามารถสั่งอนุญาตได้คราวละไม่เกิน ๙๐ วัน เมื่อเจ้าหน้าที่ของรัฐดำเนินการตามที่ได้รับอนุญาตแล้ว จะต้องรายงานการดำเนินการให้ศาลทราบด้วย

๓. ความเห็นคณะกรรมการสิทธิมนุษยชนแห่งชาติ

กรณีตามคำร้องมีประเด็นที่ต้องพิจารณาว่าผู้ถูกร้องได้กระทำหรือละเลยการกระทำอันเป็นการละเมิดสิทธิมนุษยชนต่อผู้ร้อง ด้วยการใช้งานสปายแวร์เพกาซัสโจมตีระบบโทรศัพท์เคลื่อนที่เพื่อสอดแนมข้อมูลของผู้ร้อง หรือไม่ โดยมีข้อพิจารณาดังนี้

๓.๑ สิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว และเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ ของประชาชน ได้รับการบัญญัติรับรองและคุ้มครองไว้ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองในฐานะสิทธิและเสรีภาพขั้นพื้นฐาน การจำกัดสิทธิและเสรีภาพดังกล่าวจะทำได้เฉพาะแต่กรณีที่มีกฎหมายให้อำนาจไว้เท่านั้น และต้องเป็นไปโดยสอดคล้องกับหลักความจำเป็นและหลักความได้สัดส่วน นอกจากนี้ ตามหลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน (United Nations Guiding Principles on Business and Human Rights: UNGPs) ซึ่งประเทศไทยรับหลักการมาปรับใช้อย่างเป็นทางการเมื่อปี ๒๕๕๙ ได้กำหนดหน้าที่พื้นฐานให้แก่รัฐว่า จะต้องคุ้มครองไม่ให้มีการละเมิดสิทธิมนุษยชนภายในดินแดนหรือเขตอำนาจของรัฐ อันเป็นผลมาจากการกระทำของบุคคลอื่น รวมถึงองค์กรธุรกิจ[๑๗] โดยรัฐควรจัดให้มีกลไกนอกกระบวนการยุติธรรมที่มีประสิทธิภาพและเหมาะสม ควบคู่ไปกับกระบวนการยุติธรรมปกติ เพื่อเยียวยาผลจากการละเมิดสิทธิมนุษยชนดังกล่าวอย่างครอบคลุมด้วย[๑๘]

๓.๒ จากการตรวจสอบข้อเท็จจริงปรากฏว่า

๓.๒.๑ รายงานวิจัยที่จัดทำโดยห้องปฏิบัติการ Citizen Lab เรื่อง “GeckoSpy : Pegasus Spyware Used against Thailand’s Pro-Democracy Movement” ได้ระบุข้อค้นพบจาก

/การตรวจ...

---

[๑๗] หลักการข้อที่ ๑ กำหนดว่า “รัฐต้องคุ้มครองสิทธิมนุษยชนของประชาชนให้พ้นจากการกระทำที่ไม่ชอบภายในดินแดนของตน และ/หรือการกระทำของบุคคลภายนอก รวมถึงองค์กรธุรกิจในเขตอำนาจของตน การคุ้มครองกำหนดให้ใช้ขั้นตอนที่เหมาะสมในการป้องกัน สืบสวน ลงโทษ และเยียวยาผลของการกระทำที่ไม่ชอบ โดยใช้นโยบาย กฎหมาย ข้อบังคับ และการพิจารณาตัดสินคดีที่มีประสิทธิภาพ”

[๑๘] หลักการข้อที่ ๒๗ กำหนดว่า “รัฐควรจัดให้มีกลไกการร้องทุกข์นอกกระบวนการยุติธรรมที่มีประสิทธิผลและเหมาะสม ควบคู่ไปกับกลไกทางกระบวนการยุติธรรม โดยให้ถือเป็นส่วนหนึ่งของระบบอันครอบคลุมที่อาศัยรัฐเพื่อการเยียวยาสำหรับการละเมิดสิทธิมนุษยชนที่เกี่ยวข้องกับธุรกิจ”

การตรวจวิเคราะห์ด้วยวิธีการทางนิติวิทยาศาสตร์ว่า ในช่วงเดือนตุลาคม ๒๕๖๓ ถึงเดือนพฤศจิกายน ๒๕๖๔ มีผู้ถูกเจาะระบบโทรศัพท์เคลื่อนที่ด้วยสปายแวร์เพกาซัสในประเทศไทยอย่างน้อย ๓๐ คน ประกอบด้วยนักกิจกรรม นักวิชาการ ผู้ที่ทำงานในองค์กรภาคประชาสังคม ซึ่งรวมถึงผู้ร้อง โดยข้อค้นพบที่ปรากฏนี้ได้รับการยืนยันผลการตรวจวิเคราะห์จากองค์กรที่มีความเชี่ยวชาญด้านการรักษาความปลอดภัยไซเบอร์อีกแห่งหนึ่งด้วย คือ ห้องปฏิบัติการด้านความปลอดภัยทางไซเบอร์ขององค์กรแอมเนสตี้ อินเตอร์เนชั่นแนล

๓.๒.๒ [redacted] ในฐานะพยานผู้เชี่ยวชาญของคณะกรรมการสิทธิมนุษยชนแห่งชาติมีความเห็นสอดคล้องว่า ผลการตรวจวิเคราะห์ของห้องปฏิบัติการ Citizen Lab มีความน่าเชื่อถือ

๓.๒.๓ เมื่อปี ๒๕๖๔ [redacted] ได้ฟ้อง[redacted] ในฐานะผู้พัฒนาสปายแวร์เพกาซัส โดยเรียกร้องให้แสดงความรับผิดชอบต่อการใช้สปายแวร์เพกาซัสพุ่งเป้าการสอดแนมมายังผู้ใช้งานผลิตภัณฑ์ของ[redacted] ซึ่งเป็นช่วงเวลาเดียวกันกับที่[redacted] ส่งอีเมลแจ้งเตือนให้ผู้ร้องและผู้ใช้งานผลิตภัณฑ์ของบริษัทรายอื่น ๆ ระมัดระวังการถูกเจาะระบบโทรศัพท์เคลื่อนที่จากผู้โจมตีที่ได้รับการสนับสนุนโดยรัฐ

๓.๒.๔ นับตั้งแต่ปี ๒๕๖๐ เป็นต้นมา มีการฟ้องร้องเป็นคดีต่อศาลและมีการตั้งคณะกรรมการขึ้นมาเป็นการเฉพาะเพื่อสอบสวนการใช้งานสปายแวร์เพกาซัสโดยมิชอบในประเทศต่าง ๆ อีก ๓๐ กรณี โดยพบว่าเหยื่อที่ถูกโจมตีมักเป็นผู้สื่อข่าว ผู้ที่มีความคิดเห็นแตกต่างจากรัฐบาล ผู้นำองค์กรภาคประชาสังคม นักกิจกรรม นักปกป้องสิทธิมนุษยชน นักวิชาการ ไปจนถึงนักการเมือง ซึ่งเป็นกลุ่มในบริบทเดียวกันกับผู้ที่ถูกโจมตีในประเทศไทยตามข้อค้นพบจากรายงานวิจัยของห้องปฏิบัติการ Citizen Lab

๓.๒.๕ ในปี ๒๕๖๔ กระทรวงพาณิชย์ของสหรัฐอเมริกา ยังได้เพิ่มรายชื่อ[redacted] เข้าในบัญชีรายชื่อบริษัทที่มีส่วนร่วมในกิจกรรมที่ขัดต่อความมั่นคงของชาติและผลประโยชน์ด้านนโยบายต่างประเทศของสหรัฐอเมริกา เนื่องจากมีหลักฐานว่ามีการพัฒนาและจัดหาสปายแวร์ให้แก่รัฐบาลหลายประเทศ เพื่อใช้โจมตีไปยังเป้าหมายที่เป็นเจ้าหน้าที่ของรัฐ ผู้สื่อข่าว นักธุรกิจ นักกิจกรรม และนักวิชาการ ซึ่งส่งผลให้เกิดการปราบปรามผู้เห็นต่างโดยไม่จำกัดพรมแดน อันเป็นการกระทำที่ขัดต่อพันธกรณีระหว่างประเทศ

๓.๓ เมื่อพิจารณาข้อเท็จจริงข้างต้นประกอบกันแล้ว คณะกรรมการสิทธิมนุษยชนแห่งชาติเห็นว่า

/๓.๓.๑ ข้อเท็จจริง...

๓.๓.๑ ข้อเท็จจริงตามคำร้องมีเหตุผลที่ทำให้เชื่อได้ว่า มีการใช้งานสปายแวร์เพกาซัสโจมตีระบบโทรศัพท์เคลื่อนที่เพื่อสอดแนมข้อมูลของผู้ร้อง รวมถึงนักกิจกรรม นักวิชาการ และผู้ที่ทำงานในองค์กรภาคประชาสังคมในประเทศไทย ซึ่งผู้ร้องและบุคคลที่ถูกโจมตีด้วยสปายแวร์เพกาซัสข้างต้น ไม่มีประวัติเข้าไปเกี่ยวข้องกับการก่อการร้ายหรือการก่ออาชญากรรมที่มีความร้ายแรง เช่น การค้าอาวุธ การค้ามนุษย์ หรือการค้ายาเสพติด มีเพียงการถูกดำเนินคดีที่เนื่องมาจากการใช้เสรีภาพในการแสดงความคิดเห็นและเสรีภาพในการชุมนุมเพื่อคัดค้านหรือวิพากษ์วิจารณ์การดำเนินงานของรัฐบาลในช่วงที่ผ่านมา

๓.๓.๒ การเจาะระบบโทรศัพท์เคลื่อนที่เพื่อสอดแนมข้อมูลด้วยสปายแวร์เพกาซัส ซึ่งเป็นเครื่องมือสอดแนมศักยภาพสูงที่สามารถเข้าถึงข้อมูลในโทรศัพท์เคลื่อนที่ของผู้ที่ตกเป็นหมายได้ทุกคนโดยไม่มีขีดจำกัดและโดยที่ไม่รู้ตัวดังเช่นที่เกิดขึ้นกับผู้ร้องและเหยื่ออีกหลายคนในประเทศไทยนี้ จึงเข้าข่ายเป็นการใช้งานโดยมิชอบและผิดวัตถุประสงค์ของการผลิตหรือพัฒนาสปายแวร์เพกาซัส ตามที่ [redacted] ได้กล่าวอ้างไว้ **ถือเป็นการกระทำที่ละเมิดสิทธิมนุษยชน โดยเฉพาะต่อสิทธิในความเป็นอยู่ส่วนตัวของผู้ร้อง รวมถึงนักกิจกรรม นักวิชาการ และผู้ที่ทำงานในองค์กรภาคประชาสังคมดังกล่าว นอกจากนี้ ยังส่งผลให้เกิดความหวาดกลัวและความกังวลต่อการวิพากษ์วิจารณ์โดยสุจริตหรือการตรวจสอบการทำงานของรัฐบาลและหน่วยงานของรัฐ อันเป็นสิ่งที่พึงกระทำได้ตามปกติของการปกครองในระบอบประชาธิปไตย ซึ่งการกระทำเช่นนี้จะนำไปสู่การจำกัดเสรีภาพในการแสดงความคิดเห็น รวมทั้งสิทธิและเสรีภาพอื่น ๆ ของประชาชนที่จะเข้าไปมีส่วนร่วมทางการเมืองโดยตรงด้วย**

๓.๓.๓ แม้ [redacted] ได้อ้างว่า บริษัทไม่ได้เป็นผู้ใช้งานสปายแวร์เพกาซัสด้วยตนเอง แต่จะขายสิทธิการใช้งานให้แก่หน่วยงานของรัฐนำไปใช้ในการป้องกันและปราบปรามอาชญากรรมเท่านั้น แต่จากข้อเท็จจริงที่ปรากฏข้างต้น แสดงให้เห็นว่ากระบวนการกลั่นกรองประเมินความเสี่ยงและความเหมาะสมของผู้ซื้อ เพื่อป้องกันการใช้ผลิตภัณฑ์ของบริษัทไปในทางที่ไม่ชอบนั้น ยังมีข้อบกพร่องอยู่ [redacted] จึงไม่อาจปฏิเสธความรับผิดชอบต่อการละเมิดสิทธิมนุษยชนดังกล่าวได้ และเป็นหน้าที่โดยตรงของรัฐบาลไทย ตามหลักการชี้แนะของสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน ข้อที่ ๑ และข้อที่ ๒๗ ที่จะต้องคุ้มครองไม่ให้เกิดการละเมิดสิทธิมนุษยชนจากการดำเนินกิจกรรมขององค์กรธุรกิจขึ้นภายในดินแดนหรือเขตอำนาจของประเทศไทย รวมทั้งจะต้องแสวงหามาตรการเยียวยาผลจากการละเมิดสิทธิมนุษยชนดังกล่าวอย่างครอบคลุม

๓.๓.๔ แม้ข้อเท็จจริงตามคำร้องจะยังไม่มีพยานหลักฐานที่ระบุได้อย่างชัดเจนว่าหน่วยงานใดของรัฐในประเทศไทยเป็นผู้ใช้งานสปายแวร์เพกาซัสเจาะระบบโทรศัพท์เคลื่อนที่เพื่อสอดแนม

/ข้อมูลของ...

ข้อมูลของผู้ร้อง รวมถึงนักกิจกรรม นักวิชาการ และผู้ที่ทำงานในองค์กรภาคประชาสังคมในประเทศไทย แต่หากพิจารณาถึงข้อมูลบ่งชี้ในบริบทแวดล้อม และความน่าจะเป็นต่าง ๆ ประกอบกัน ได้แก่

๑) การยอมรับโดย [redacted] เองว่า จะขายสิทธิการใช้งานผลิตภัณฑ์ของบริษัทซึ่งรวมถึงสปายแวร์เพกาซัสให้แก่เฉพาะหน่วยงานของรัฐในประเทศต่าง ๆ เท่านั้น ไม่ขายให้แก่บุคคลหรือบริษัทเอกชนทั่วไป

๒) การพิจารณาถึงความคุ้มค่า แรงจูงใจ และผลประโยชน์ที่หน่วยงานของรัฐในประเทศไทยจะได้รับจากการใช้งานสปายแวร์เพกาซัส ซึ่งเป็นเทคโนโลยีที่มีราคาสูงมาใช้งาน โดยเฉพาะอย่างยิ่งจากช่วงเวลาที่มีการโจมตีพบว่า มักจะเกิดขึ้นไม่นานก่อนที่จะมีการจัดกิจกรรมหรือการชุมนุมเรียกร้องซึ่งส่วนใหญ่มักจะเป็นการวิพากษ์วิจารณ์การทำงานของรัฐบาลในด้านลบ

๓) การที่ผู้แทนของสำนักข่าวกรองแห่งชาติได้ให้ข้อเท็จจริงว่า [redacted] เคยนำผลิตภัณฑ์ประเภทสปายแวร์มาเสนอขายให้แก่หน่วยงานของรัฐด้านความมั่นคง

๔) เอกสารประกอบการของบประมาณในการจัดซื้อจัดจ้าง “โครงการจัดหาระบบรวบรวมและประมวลผลข่าวกรองชั้นสูง” ของกองบัญชาการตำรวจปราบปรามยาเสพติด พบข้อมูลว่าระบบเข้าถึงข้อมูลข่าวสารอิเล็กทรอนิกส์ที่เคยได้จัดซื้อไว้แล้ว และที่จะจัดหามาใช้งานใหม่นั้น มีคุณสมบัติในการส่ง Application Agent ไปติดตั้งบนโทรศัพท์เคลื่อนที่โดยที่เป้าหมายไม่รู้ตัว ซึ่งคุณสมบัติดังกล่าวมีลักษณะคล้ายกับระบบการโจมตีหรือรูปแบบการเจาะระบบปฏิบัติการของโทรศัพท์เคลื่อนที่เป้าหมายแบบไม่ต้องคลิก ที่เป็นคุณสมบัติเด่นของสปายแวร์เพกาซัส

ด้วยเหตุที่กล่าวมานี้ จึงไม่อาจปฏิเสธได้ว่าหน่วยงานของรัฐในประเทศไทยไม่ได้จัดซื้อ จัดหา หรือไม่ได้มีส่วนเกี่ยวข้องกับการใช้งานสปายแวร์เพกาซัสโจมตีระบบของอุปกรณ์การสื่อสารเพื่อสอดแนมข้อมูลของนักกิจกรรม นักวิชาการ ผู้ที่ทำงานในองค์กรภาคประชาสังคม และผู้ร้อง

๓.๓.๕ นอกจากนี้คณะกรรมการสิทธิมนุษยชนแห่งชาติยังมีข้อสังเกตด้วยว่า กฎหมายที่ให้อำนาจเจ้าหน้าที่ของรัฐสามารถใช้งานสปายแวร์หรือเทคโนโลยีสอดแนมเพื่อเข้าถึงข้อมูลในอุปกรณ์สื่อสารซึ่งถูกต้องสงสัยว่ามีการกระทำความผิดตามกฎหมาย ซึ่งมีอยู่หลายฉบับดังที่ได้กล่าวถึงไว้แล้วข้างต้นนั้น อาจมีกลไกการกำกับ ควบคุม และตรวจสอบการใช้งานที่ยังไม่รัดกุมหรือครอบคลุมเพียงพอ โดยเฉพาะการพิจารณาถึงความสุ่มเสี่ยงต่อการละเมิดสิทธิมนุษยชน

๓.๓.๖ ดังนั้น เพื่อให้เรื่องนี้มีความชัดเจนมากยิ่งขึ้น รวมถึงเพื่อเป็นการป้องกันไม่ให้เกิดการละเมิดสิทธิมนุษยชนในลักษณะนี้ขึ้นอีก คณะกรรมการสิทธิมนุษยชนแห่งชาติเห็นควรเสนอแนะมาตรการหรือแนวทางในการส่งเสริมและคุ้มครองสิทธิมนุษยชนในเรื่องนี้ต่อคณะรัฐมนตรีต่อไป

/๔. มติคณะกรรมการ...

๔. มติคณะกรรมการสิทธิมนุษยชนแห่งชาติ

อาศัยเหตุผลดังกล่าวข้างต้น คณะกรรมการสิทธิมนุษยชนแห่งชาติ ในคราวประชุมด้านการคุ้มครองและส่งเสริมสิทธิมนุษยชน ครั้งที่ ๑๓/๒๕๖๗ เมื่อวันที่ ๒ เมษายน ๒๕๖๗ จึงมีมติว่า

๔.๑ กรณีตามคำร้องมีเหตุผลทำให้เชื่อได้ว่ามีการใช้งานสปายแวร์เพกาซัสโจมตีระบบโทรศัพท์เคลื่อนที่เพื่อสอดแนมข้อมูลของผู้ร้อง รวมถึงนักกิจกรรม นักวิชาการ และผู้ที่ทำงานในองค์กรภาคประชาสังคมในประเทศไทย กรณีจึงเป็นการกระทำอันเป็นการละเมิดสิทธิมนุษยชน แต่เนื่องจากข้อเท็จจริงไม่สามารถระบุได้ว่าหน่วยงานของรัฐด้านความมั่นคง (ผู้ถูกร้อง) หน่วยงานใดกระทำการดังกล่าว จึงไม่อาจเสนอแนะมาตรการหรือแนวทางที่เหมาะสมในการป้องกันหรือแก้ไขการละเมิดสิทธิมนุษยชน รวมทั้งการเยียวยาผู้ได้รับความเสียหายจากการละเมิดสิทธิมนุษยชนต่อหน่วยงานของรัฐดังกล่าวได้โดยตรง

๔.๒ อย่างไรก็ตาม เพื่อเป็นการแก้ไขและป้องกันไม่ให้เกิดการละเมิดสิทธิมนุษยชนในลักษณะนี้ขึ้นอีก จึงให้เสนอแนะมาตรการหรือแนวทางในการส่งเสริมและคุ้มครองสิทธิมนุษยชนและข้อเสนอแนะในการแก้ไขปรับปรุงกฎหมายเพื่อให้สอดคล้องกับหลักสิทธิมนุษยชน ต่อคณะรัฐมนตรีตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ มาตรา ๒๔๗ (๓) และพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๐ มาตรา ๒๖ (๓) ประกอบมาตรา ๔๒ เพื่อดำเนินการ ดังนี้

๔.๒.๑ ให้คณะรัฐมนตรีสั่งการให้มีมาตรการหรือกลไกที่มีความเหมาะสม เป็นอิสระและโปร่งใส ในการแสวงหาข้อเท็จจริงเกี่ยวกับการใช้งานสปายแวร์เพกาซัส สปายแวร์อื่น ๆ หรือเทคโนโลยีสอดแนมในลักษณะเดียวกันของหน่วยงานของรัฐ ในทางที่อาจไม่เป็นไปตามกรอบของกฎหมายที่ให้อำนาจหรือไม่สอดคล้องกับมาตรฐานระหว่างประเทศที่ประเทศไทยมีพันธกรณีต้องปฏิบัติตาม โดยผู้ดำเนินมาตรการหรือปฏิบัติหน้าที่ในกลไกข้างต้นต้องมีอำนาจในการเรียกเอกสาร พยานหลักฐาน หรือเข้าถึงข้อมูลที่เป็นความลับด้วย ทั้งนี้ ต้องมีการกำหนดมาตรการเยียวยาความเสียหายจากการละเมิดสิทธิมนุษยชนที่เกิดขึ้นกับผู้เสียหายอย่างมีประสิทธิภาพและครอบคลุมเพียงพอ

๔.๒.๒ ให้คณะรัฐมนตรีสั่งการให้หน่วยงานที่เกี่ยวข้องดำเนินการศึกษาข้อมูลเพื่อให้มีกฎหมาย ระเบียบ แนวปฏิบัติ หรือกลไกในการกำกับ ควบคุม และตรวจสอบการใช้งานสปายแวร์หรือเทคโนโลยีสอดแนมในลักษณะเดียวกันของหน่วยงานของรัฐ เพื่อเป็นหลักประกันในการป้องกันไม่ให้เกิดกรณีการนำสปายแวร์หรือเทคโนโลยีดังกล่าวไปใช้งานผิดวัตถุประสงค์ ไม่ชอบด้วยกฎหมายหรือไม่สอดคล้องกับมาตรฐานระหว่างประเทศด้านสิทธิมนุษยชนที่ประเทศไทยมีพันธกรณีต้องปฏิบัติตาม ทั้งนี้ ในระหว่างที่ยังไม่มีกฎหมาย ระเบียบ แนวปฏิบัติ หรือกลไกดังกล่าว ให้กำชับหน่วยงานของรัฐที่มี

/อำนาจตาม...

อำนาจตามกฎหมายซึ่งสามารถใช้งานสปายแวร์หรือเทคโนโลยีสอดแนมในลักษณะเดียวกัน ให้ใช้งานโดยถูกต้องตามกฎหมาย และสอดคล้องกับมาตรฐานระหว่างประเทศด้านสิทธิมนุษยชนที่ประเทศไทยมีพันธกรณีต้องปฏิบัติตามอย่างเคร่งครัดด้วย

คณะกรรมการสิทธิมนุษยชนแห่งชาติ

นางสาวพรประไพ กาญจนรินทร์	**ประธานกรรมการสิทธิมนุษยชนแห่งชาติ**
นางปรีดา คงแป้น	**กรรมการสิทธิมนุษยชนแห่งชาติ**
ผู้ช่วยศาสตราจารย์สุชาติ เศรษฐมาลินี	**กรรมการสิทธิมนุษยชนแห่งชาติ**
นางสาวศยามล ไกยูรวงศ์	**กรรมการสิทธิมนุษยชนแห่งชาติ**
นางสาวปิติกาญจน์ สิทธิเดช	**กรรมการสิทธิมนุษยชนแห่งชาติ**
นายวสันต์ ภัยหลีกลี้	**กรรมการสิทธิมนุษยชนแห่งชาติ**
นางสาวสุภัทรา นาคะผิว	**กรรมการสิทธิมนุษยชนแห่งชาติ**