แคสเปอร์สกี้เตือน ระวังโดน “stalkerware” สอดส่องไม่รู้ตัว!

แคสเปอร์สกี้พบยอดผู้ใช้ที่ตกเป็นเป้าหมายที่มีการพยายามติดตั้งโปรแกรม stalkerware ลงในโมบายดีไวซ์อย่างน้อยหนึ่งครั้ง เพิ่มสูงเป็น 37,532 รายในช่วงเดือนมกราคม – สิงหาคม 2019 นับเป็นสัดส่วนเพิ่มสูงถึง 35% เมื่อเทียบกับตัวเลขปีที่แล้วในช่วงเดือนเดียวกัน นอกจากนี้ขอบข่ายของ stalkerware ก็ขยายกว้างขึ้น จากรายงานเรื่อง “The State of Stalkerware in 2019” ของแคสเปอร์สกี้ พบสายพันธุ์ย่อย (variant) ของ stalkerware มากถึง 380 ตัว มากกว่าปีที่แล้วถึง 31%

โปรแกรม stalkerware เป็นสปายแวร์ (spyware) ที่มักใช้เป็นเครื่องมือในการสอดส่องรุกล้ำชีวิตส่วนตัวของผู้ใช้งาน มีความสามารถในการเข้าถึงข้อความ รูปภาพ โซเชียลมีเดีย พิกัดที่อยู่ คลิปภาพและคลิปเสียง ซึ่งในบางกรณีสามารถเข้าถึงข้อมูลเหล่านั้นได้แบบเรียลไทม์อีกด้วย โปรแกรม stalkerware ซ่อนการทำงานภายใต้แบ็คกราวน์โดยที่ผู้ใช้ไม่ยินยอมหรือไม่รู้ตัว ซึ่งแตกต่างจากแอปถูกกฎหมายที่ผู้ปกครองใช้ควบคุมดีไวซ์ของบุตรหลาน (parental control)

จากข้อมูลแปดเดือนแรกของปี 2019 มีผู้ใช้ 37,532 รายที่เป็นเป้าหมายพบความพยายามติดตั้งโปรแกรม stalkerware เมื่อเปรียบเทียบกับปี 2018 ซึ่งมี 27,798 ราย ตัวเลขนี้อาจดูไม่มากนักเมื่อเทียบกับมัลแวร์ประเภทอื่นๆ แต่ผู้ใช้ต้องพึงตระหนักว่า โปรแกรม stalkerware นั้นถูกใช้เพื่อสอดส่องเหยื่อที่เล็งไว้โดยเฉพาะ และผู้ละเมิดจำเป็นต้องติดตั้งโปรแกรมนี้ลงในโมบายดีไวซ์ของเหยื่อด้วยตัวเอง

นอกจากนี้ ในช่วงเดือนมกราคม – สิงหาคม 2018 แคสเปอร์สกี้ตรวจพบสายพันธุ์ย่อยอันตราย 290 ตัว ในปี 2019 นี้พบ 380 ตัว ซึ่งเพิ่มขึ้นเกือบหนึ่งในสามเลยทีเดียว ในประเทศไทยตรวจพบโปรแกรม stalkerware จำนวน 32 โปรแกรม ขณะที่ประเทศเพื่อนบ้านมีตัวเลขที่สูงกว่า นั่นคือ อินโดนีเซีย 392, ฟิลิปปินส์ 286, มาเลเซีย 217, เวียดนาม 107 และสิงคโปร์ 73 โปรแกรม

เอริก้า โอลเซน ผู้อำนวยการโครงการ Safety Net Project ที่เครือข่ายแห่งชาติเพื่อยุติความรุนแรงในครอบครัว (National Network to End Domestic Violence) กล่าวว่า “โปรแกรม stalkerware นี้ถูกออกแบบในทำงานในโหมดล่องหนและควบคุมให้ไม่มีการแจ้งเตือนใดๆ แก่เจ้าของดีไวซ์ จึงทำให้ผู้ล่วงละเมิดและผู้ติดตามสอดส่องมีเครื่องมือที่ใช้คุกคาม ตามเฝ้าดู สอดส่อง และล่วงละเมิดความเป็นส่วนตัวเหยื่อได้ การละเมิดนั้นน่าหวาดหวั่น สร้างความบอบช้ำ และสร้างความเสี่ยงด้านความปลอดภัย”

วลาดิเมียร์ คุสคอฟ ผู้เชี่ยวชาญด้านความปลอดภัย บริษัท แคสเปอร์สกี้ กล่าวว่า “แคสเปอร์สกี้ได้วิจัยและพัฒนาอย่างหนักเพื่อเพิ่มความสามารถด้านการตรวจจับ stalkerware ให้กับผลิตภัณฑ์ของเรา และยังได้ร่วมกับบริษัทด้านความปลอดภัยอื่นๆ เพื่อต่อต้านการคุกคามอีกด้วย หากแต่ยังมีประเด็นที่ต้องทำอีกหลายอย่าง เช่นการกำหนดคำจำกัดความของ stalkerware เพื่อสร้างความเข้าใจตรงกันของทุกฝ่าย การแยกความแตกต่างของซอฟต์แวร์จะช่วยให้ปกป้องผู้ใช้จากผู้ละเมิดความเป็นส่วนตัวได้ดียิ่งขึ้น”

คำแนะนำเพื่อหลีกเลี่ยงการตกเป็นเหยื่อ stalkerware

– ตั้งค่าปิดกั้นการติดตั้งโปรแกรมจากแหล่งที่ไม่รู้จัก
– ไม่เปิดเผยพาสเวิร์ดหรือพาสโค้ดของโมบายดีไวซ์ให้คนอื่นรู้
– ไม่เก็บไฟล์หรือแอปพลิเคชั่นที่ไม่รู้จักในดีไวซ์
– เปลี่ยนการตั้งค่าความปลอดภัยทุกอย่างเมื่อจบความสัมพันธ์กับคู่รักหรือคู่สมรส เพื่อป้องกันการนำข้อมูลส่วนตัวไปใช้ในทางที่ผิดได้
– ตรวจสอบรายการแอปพลิเคชั่นในโมบายดีไวซ์ เพื่อดูว่ามีโปรแกรมน่าสงสัยติดตั้งในดีไวซ์โดยที่เราไม่รู้ตัวหรือไม่ ใช้โซลูชั่นเพื่อความปลอดภัยที่เชื่อถือได้ เพื่อตรวจสอบและแจ้งเตือนเมื่อพบโปรแกรมสปายแวร์ที่พยายามรุกล้ำความเป็นส่วนตัวในโมบายดีไวซ์ เช่น Kaspersky Internet Security

หากสงสัยว่าตนเองตกเป็นเป้าหมายให้ติดต่อองค์กรหรือหน่วยงานผู้เชี่ยวชาญเพื่อขอความช่วยเหลือ ท่านสามารถอ่านรายงานเพิ่มเติมได้ที่ https://securelist.com/the-state-of-stalkerware-in-2019/93634/