แคสเปอร์สกี้ แลป เผย ZooPark มัลแวร์แอนดรอยด์อาละวาดผ่านเว็บไซต์ตัวล่าสุด

นักวิจัยของแคสเปอร์สกี้ แลป พบ “ZooPark” แคมเปญจารกรรมทางไซเบอร์อันซับซ้อน มีเป้าหมายที่ผู้ใช้แอนดรอยด์ในกลุ่มประเทศตะวันออกกลาง ใช้เว็บไซต์เป็นแหล่งแพร่กระจายเชื้อ ดูจากรูปการณ์น่าจะเป็นแคมเปญที่มีรัฐบาลอยู่เบื้องหลัง เน้นการโจมตีหน่วยงานการเมือง กลุ่มเคลื่อนไหว และเป้าหมายอื่นๆ ในภูมิภาค

เร็วๆ นี้ นักวิจัยของแคสเปอร์สกี้ แลป ได้พบตัวอย่างของแอนดรอยด์มัลแวร์ ในทีแรกมัลแวร์นี้ดูจะเป็นทูลจารกรรมไซเบอร์ที่เรียบง่าย ไม่น่าซับซ้อนนัก แต่นักวิจัยตัดสินใจที่จะตรวจสอบลงลึกต่อไป จึงค้นพบเวอร์ชั่นที่มีความซับซ้อนและใหม่กว่าของแอพนี้ และตั้งชื่อว่า ZooPark

แอพร้ายกาจพวกนี้บางตัวถูกแพร่กระจายออกมาจากเว็บไซต์ข่าวหรือเว็บไซต์การเมืองที่เป็นที่นิยมกันในภูมิภาคตะวันออกกลาง โดยแฝงตัวมาในรูปของแอพที่ถูกต้อง เช่น ‘TelegramGroups’ และ ‘Alnaharegypt news’ เป็นต้น ซึ่งเป็นชื่อที่คนในท้องที่นั้นๆ จะจำได้และรู้จักกันดี หลังจากกระจายเชื้อมัลแวร์สำเร็จแล้ว ผู้ร้ายไซเบอร์จะได้ข้อมูลต่างๆ ดังนี้:

- ชื่อที่ติดต่อ
- ข้อมูลของแอ็คเค้าท์
- บันทึกการโทรศัพท์รวมทั้งเสียงบันทึกการโทร
- รูปภาพใน SD Card ของอุปกรณ์นั้น
- พิกัด GPS
- ข้อความ SMS
- รายละเอียดแอพพลิเคชั่น ข้อมูลเบราเซอร์
- ข้อมูลการพิมพ์คีย์ล็อกและคลิปบอร์ด
- อื่นๆ

ฟังก์ชั่นแบ็คดอร์:

- แอบส่ง SMS
- แอบโทรศัพท์
- ดำเนินการคำสั่งเชลล์คอมมานด์

นอกจากนี้ ยังมีฟังก์ชั่นอื่นๆ ที่ใช้แอพพลิเคชั่นสื่อสาร อาทิ Telegram, WhatsApp, IMO, Chrome และแอพพลิเคชั่นอื่นๆ อีก มัลแวร์จะคอยขโมยฐานข้อมูลภายในของแอพที่ถูกควบคุม ตัวอย่างเช่น จารกรรมข้อมูลสำคัญส่วนตัวที่เก็บไว้ตามเว็บไซต์ต่างๆ

ข้อมูลจากการตรวจสอบพบว่า ผู้อยู่เบื้องหลังการโจมตีนี้มีเป้าหมายโจมตีผู้ใช้ในประเทศอียิปต์ จอร์แดน โมร็อกโก เลบานอน และอิหร่าน และเมื่อวิเคราะห์จากหัวข้อข่าวที่ผู้ร้ายใช้ล่อเหยื่อให้หลงกลลงมัลแวร์แล้ว คาดว่าสมาชิกกลุ่มผู้บรรเทาทุกข์แห่งสหประชาชาติ และหน่วยงานต่างๆ น่าจะกำลังเป็นเหยื่อของมัลแวร์ ZooPark ด้วย

“ปัจจุบันผู้คนมากมายใช้อุปกรณ์สื่อสารโมบาย และส่วนมากถึงกับใช้เป็นช่องทางสื่อสารหลักทางเดียว ซึ่งเป็นแนวโน้มที่ถูกจับตามองของผู้โจมตีที่ได้รับการหนุนหลังจากประเทศที่กำลังสร้างทูลเซ็ตให้มีประสิทธิภาพมากพอ เพื่อใช้ติดตามข้อมูลของผู้ใช้โมบาย มัลแวร์ ZooPark APT เป็นสปายสอดส่องเป้าหมายในประเทศในตะวันออกกลาง และนี่ก็เป็นตัวอย่างหนึ่งเท่านั้น” อเล็กซี่ เฟิร์ซ ผู้เชี่ยวชาญด้านความปลอดภัย แคสเปอร์สกี้ แลป กล่าว

นักวิจัยของแคสเปอร์สกี้ แลป สามารถระบุมัลแวร์เพื่อการจารกรรมที่เกี่ยวโยงกับครอบครัวมัลแวร์ ZooPark ได้อย่างน้อยถึง 4 เจเนเรชั่น ซึ่งออกอาละวาดมาอย่างน้อยที่สุดน่าจะตั้งแต่ปี 2015 ผลิตภัณฑ์ของแคสเปอร์สกี้ แลป สามารถตรวจจับและบล็อกภัยไซเบอร์ตัวนี้ได้เป็นผลสำเร็จ

อ่านเพิ่มเติมเกี่ยวกับมัลแวร์ ZooPark ภัยไซเบอร์แบบ APT ได้ที่
https://securelist.com/whos-who-in-the-zoo/85394/