ระวังมัลแวร์แพร่กระจายผ่านเว็บหลอกลวงติดตามสถานการณ์ COVID-19

TLP: WHITE

เผยแพร่วันที่ 19 มีนาคม 2563

สถานการณ์ระบาดของไวรัส Corona หรือ COVID-19 ที่ขยายตัวไปในเกือบทุกประเทศทั่วโลก ทำให้มีนักวิชาการต่างๆ สร้างเว็บไซต์ที่รวบรวมข้อมูลที่เกี่ยวกับ COVID-19 เพื่อให้ผู้สนใจสามารถติดตามสถานการณ์ รวมถึงข้อมูลที่เป็นประโยชน์ในการเตรียมตัวป้องกัน ภายใต้สถานการณ์เช่นนี้แฮกเกอร์มักจะฉวยโอกาสที่ผู้ใช้งานมุ่งความสนใจไปที่ข้อมูลที่เกี่ยวข้องกับสถานการณ์โรคระบาด จนหลายๆ ครั้งทำให้ขาดความระวังในการป้องกันตนเองในโลกไซเบอร์เมื่อเปิดอีเมลแปลกๆ ดาวน์โหลดโปรแกรมหรือเผลอให้ข้อมูลไปอย่างง่ายๆ ตัวอย่าง เช่น มีการสร้างเว็บไซต์ปลอม (www.Corona-Virus-Map[.]com) ที่แสดงแผนที่อัปเดตการแพร่กระจายของไวรัส Corona พร้อมข้อมูลต่างๆ เช่น สถิติการเสียชีวิต จำนวนผู้ที่รักษาหาย และจำนวนผู้ติดเชื้อ เป็นต้น ซึ่งใช้ข้อมูลจากเว็บของมหาวิทยาลัย John Hopkins และหลอกให้เหยื่อดาวน์โหลดและติดตั้งไฟล์มัลแวร์ลงบนเครื่องของเหยื่อ

ลักษณะของมัลแวร์

มัลแวร์นี้ถูกจัดอยู่ในตระกูล AZORult โดยเมื่อเหยื่อเยี่ยมชมเว็บไซต์ปลอมจะถูกบังคับให้ดาวน์โหลดและติดตั้งไฟล์มัลแวร์ชื่อ Corona-virus-Map.com.exe จากนั้นจะมัลแวร์นี้จะสร้างไฟล์อื่นเพิ่มเติม เช่น CoronaMap.exe, Corona.exe และ Corona.sfx.exe เป็นต้น อีกทั้งยังเชื่อมต่อไปยังเซิร์ฟเวอร์ที่แฮกเกอร์เตรียมไว้เพื่อเก็บข้อมูลด้วย

ผลกระทบ

มัลแวร์นี้จะขโมยข้อมูลสำคัญ เช่น ชื่อบัญชี รหัสผ่าน เลขที่บัตรเครดิต เงินในกระเป๋าเงินดิจิทัล ภาพหน้าจอ และข้อมูลอื่นๆ ที่ถูกเก็บอยู่ในเว็บเบราเซอร์ เป็นต้น

วิธีการแก้ไข

1. ติดตั้งโปรแกรมป้องกันมัลแวร์ที่เชื่อถือได้ และอัพเดตให้มีข้อมูลมัลแวร์ใหม่ล่าสุด
2. สแกนค้นหามัลแวร์ในเครื่อง หากพบให้ทำการลบทันที

วิธีการป้องกัน

1. ติดตามข่าวสารสถานการณ์ COVID-19 จากเว็บไซต์และช่องทางสื่อสารที่เป็นทางการจากกระทรวงสาธารณสุข เช่น
   - Web: https://ddc.moph.go.th/viralpneumonia/index.php
   - LINE : https://lin.ee/dAEiq3e
   - Twitter : https://twitter.com/thaimoph
   - Facebook : https://www.facebook.com/thaimoph
   - TikTok : https://vt.tiktok.com/jcvfwN/
2. ไม่ดาวน์โหลดและติดตั้งโปรแกรมใดๆ ที่เกี่ยวกับการติดตามสถานการณ์ไวรัส รวมถึงโปรแกรมที่ไม่ทราบหรือไม่แน่ใจว่ามาจากแหล่งที่น่าเชื่อถือ