วันที่ 2 กันยายน 2568

TamperedChef มัลแวร์ปลอมตัวเป็นโปรแกรมแก้ไข PDF ขโมยรหัสผ่านและคุกกี้

นักวิจัยด้านความปลอดภัยได้ค้นพบการโจมตีทางไซเบอร์รูปแบบใหม่ที่ใช้กลยุทธ์โฆษณาอันตราย (malvertising) เพื่อหลอกล่อให้ผู้ใช้งานดาวน์โหลดมัลแวร์ตัวใหม่ชื่อ TamperedChef ซึ่งออกแบบมาเพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่านและคุกกี้จากเว็บเบราว์เซอร์

“เป้าหมายคือการล่อให้เหยื่อดาวน์โหลดและติดตั้งโปรแกรมแก้ไข PDF เวอร์ชันปลอม ที่แฝงมากับมัลแวร์ชื่อ TamperedChef” นักวิจัยจาก Truesec กล่าวในรายงาน “มัลแวร์นี้ถูกสร้างมาเพื่อเก็บข้อมูลสำคัญ รวมถึงรหัสผ่านและคุกกี้”

หัวใจหลักของการโจมตีคือการใช้เว็บไซต์ปลอมหลายแห่งโปรโมตตัวติดตั้งของโปรแกรมที่อ้างว่าเป็น AppSuite PDF Editor ฟรี ซึ่งเมื่อผู้ใช้ติดตั้งและเปิดใช้งาน จะมีหน้าต่างเด้งขึ้นมาให้กดยอมรับข้อตกลงการใช้งานและนโยบายความเป็นส่วนตัว แต่ในเบื้องหลัง โปรแกรมติดตั้งจะเชื่อมต่อกับเซิร์ฟเวอร์ภายนอกเพื่อดาวน์โหลดตัวโปรแกรม PDF editor จริง พร้อมทั้งตั้งค่าให้รันอัตโนมัติหลังเปิดเครื่องใหม่ ผ่านการแก้ไขค่าใน Windows Registry โดยจะใส่พารามิเตอร์ --cm เพื่อส่งคำสั่งให้ตัวโปรแกรมทำงานตามที่กำหนด

กลไกการทำงานของมัลแวร์

บริษัทด้านความปลอดภัยไซเบอร์ของเยอรมัน G DATA ซึ่งได้วิเคราะห์การโจมตีนี้เช่นกัน ระบุว่า เว็บไซต์เหล่านี้ที่แจกโปรแกรม PDF จะดาวน์โหลดไฟล์ติดตั้งตัวเดียวกันทั้งหมด และเมื่อผู้ใช้กดยอมรับข้อตกลง โปรแกรมติดตั้งจะไปดึงโปรแกรม PDF editor มาจากเซิร์ฟเวอร์

“จากนั้นจะรันแอปพลิเคชันหลักโดยไม่ใส่คำสั่งเพิ่มเติม ซึ่งเท่ากับการเริ่มการทำงานในโหมด --install” นักวิจัยกล่าว “มันยังสร้าง task ให้รันอัตโนมัติ โดยใส่คำสั่ง --cm=--fullupdate สำหรับการทำงานครั้งถัดไปของมัลแวร์”

คาดว่าการโจมตีนี้เริ่มต้นขึ้นเมื่อวันที่ 26 มิถุนายน 2025 ซึ่งเป็นช่วงที่เว็บไซต์ปลอมหลายแห่งถูกสร้างขึ้นหรือเริ่มโฆษณาผ่าน Google อย่างน้อย 5 แคมเปญ

“ในช่วงแรก โปรแกรม PDF ดูเหมือนจะไม่เป็นอันตรายมากนัก แต่ในโค้ดมีการเขียนไว้ให้ตรวจสอบไฟล์ .js ที่ใช้คำสั่ง --cm เป็นระยะ เพื่อรอรับการอัปเดต” นักวิจัยอธิบาย “ตั้งแต่วันที่ 21 สิงหาคม 2025 เป็นต้นมา เครื่องที่เชื่อมต่อกลับไปยังเซิร์ฟเวอร์จะได้รับคำสั่งให้เปิดการทำงานของมัลแวร์ที่ชื่อ TamperedChef”

เมื่อเริ่มทำงาน มัลแวร์นี้จะตรวจสอบว่าเครื่องมีโปรแกรมป้องกันใดติดตั้งอยู่บ้าง และพยายามปิดเว็บเบราว์เซอร์ เพื่อเข้าถึงข้อมูลสำคัญอย่างรหัสผ่านและคุกกี้

Backdoor และชุดคำสั่งที่ใช้

การวิเคราะห์เพิ่มเติมโดย G DATA พบว่า โปรแกรมนี้ทำงานเหมือนเป็น backdoor ที่รองรับหลายคำสั่ง ได้แก่:

- --install: สร้าง scheduled task ชื่อ PDFEditorScheduledTask และ PDFEditorUScheduledTask ให้รันโปรแกรมพร้อมคำสั่ง --cm=--partialupdate และ --cm=--backupupdate ตามลำดับ เพื่อกระตุ้นให้ทำงานฟังก์ชัน --check และ --ping
- --cleanup: ใช้ตอนถอนการติดตั้ง เพื่อลบไฟล์ backdoor ออกจากเครื่อง ยกเลิกการลงทะเบียนกับเซิร์ฟเวอร์ และลบ scheduled task ทั้งหมด
- --ping: ใช้ติดต่อกับเซิร์ฟเวอร์สั่งการ (C2) เพื่อรับคำสั่งต่างๆ เช่น ดาวน์โหลดมัลแวร์เพิ่ม, ขโมยข้อมูล หรือแก้ไขค่า Registry
- --check: ใช้ติดต่อ C2 เพื่อดึงการตั้งค่า, อ่านข้อมูลจากเบราว์เซอร์, แก้ไขการตั้งค่าเบราว์เซอร์, และสั่งรันคำสั่งเพื่อขโมยหรือแก้ไขข้อมูลของเบราว์เซอร์ตระกูล Chromium, OneLaunch และ Wave รวมถึงรหัสผ่าน, ประวัติการใช้งาน, คุกกี้ หรือเปลี่ยนค่า search engine
- --reboot: ทำงานเหมือน --check แต่มีเพิ่มความสามารถในการปิดโปรเซสที่ระบุ

“ช่วงเวลาจากเริ่มโฆษณาจนถึงปล่อยอัปเดตอันตรายคือ 56 วัน ซึ่งใกล้เคียงกับอายุแคมเปญโฆษณา Google ปกติที่ประมาณ 60 วัน แสดงให้เห็นว่าผู้โจมตีตั้งใจปล่อยให้แคมเปญโฆษณารันจนสุด เพื่อให้มีจำนวนดาวน์โหลดมากที่สุด ก่อนเปิดการทำงานที่เป็นอันตราย” Truesec กล่าว

การเปิดเผยนี้เกิดขึ้นพร้อมกับรายงานของ Expel ที่พบแคมเปญโฆษณาขนาดใหญ่โปรโมตโปรแกรมแก้ไข PDF โดยโฆษณาพาผู้ใช้ไปยังเว็บไซต์ที่แจกเครื่องมืออย่าง AppSuite, PDF OneStart และ PDF Editor ซึ่งในบางกรณี โปรแกรมเหล่านี้จะดาวน์โหลดแอปที่ฝังมัลแวร์ตัวอื่นเพิ่ม หรือเปลี่ยนเครื่องของเหยื่อให้กลายเป็นพร็อกซี

“AppSuite PDF Editor เป็นโปรแกรมอันตราย” G DATA ระบุ “มันคือโทรจันที่แฝง backdoor และกำลังถูกดาวน์โหลดอย่างมหาศาลในตอนนี้”

ข้อมูลอ้างอิง

Aug 29, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/tamperedchef-malware-disguised-as-fake.html