วันที่ 25 มิถุนายน 2568

## มัลแวร์ XDigo ใช้ประโยชน์จากจุดบกพร่อง LNK ของ Windows ในการโจมตีของรัฐบาลยุโรปตะวันออก


นักวิจัยด้านความปลอดภัยทางไซเบอร์ได้ค้นพบมัลแวร์ที่เขียนด้วยภาษา Go ชื่อว่า XDigo ซึ่งถูกนำมาใช้ในปฏิบัติการโจมตีหน่วยงานรัฐบาลในยุโรปตะวันออกเมื่อเดือนมีนาคม 2025 ห่วงโซ่การโจมตีนี้มีการใช้ไฟล์ทางลัดของ Windows (ไฟล์ .LNK) หลายไฟล์เป็นส่วนหนึ่งของขั้นตอนหลายชั้น เพื่อกระจายมัลแวร์ ตามรายงานของบริษัทด้านความปลอดภัยไซเบอร์จากฝรั่งเศส HarfangLab

### XDSpy และ Silent Werewolf: กลุ่มผู้โจมตีที่น่ากังวล

XDSpy คือชื่อของปฏิบัติการจารกรรมไซเบอร์ที่รู้จักกันดีว่ามุ่งเป้าไปที่หน่วยงานรัฐบาลในยุโรปตะวันออกและแถบบอลข่านตั้งแต่ปี 2011 โดยถูกเปิดเผยครั้งแรกโดย CERT ของเบลารุสเมื่อต้นปี 2020 ในช่วงไม่กี่ปีที่ผ่านมา บริษัทในรัสเซียและมอลโดวาถูกโจมตีด้วยแคมเปญหลายรูปแบบ เพื่อติดตั้งมัลแวร์ตระกูลต่างๆ เช่น UTask, XDDown และ DSDownloader ซึ่งสามารถดาวน์โหลดไฟล์อันตรายและขโมยข้อมูลสำคัญจากเครื่องที่ถูกเจาะ

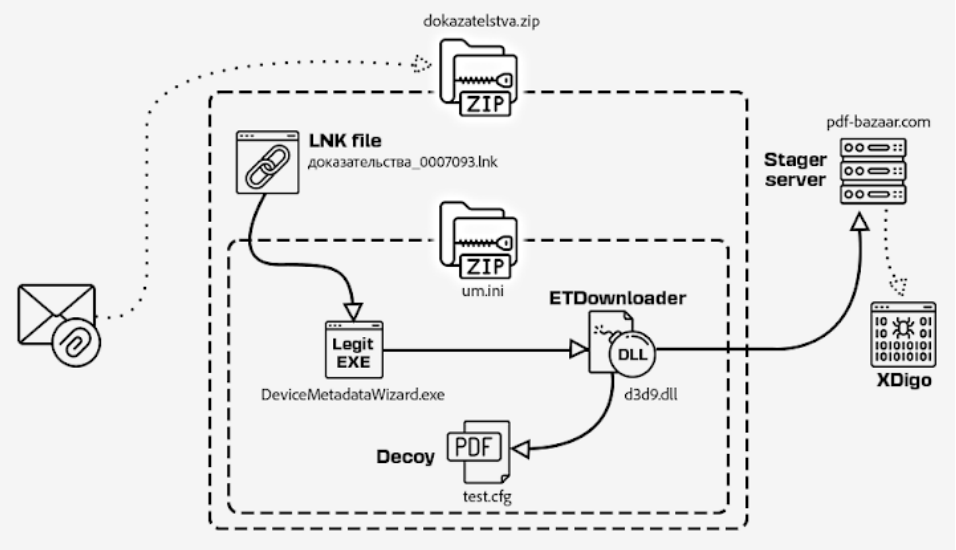
HarfangLab กล่าวว่า กลุ่มผู้โจมตีใช้ประโยชน์จากช่องโหว่ Remote Code Execution ใน Microsoft Windows ที่เกิดขึ้นเมื่อประมวลผลไฟล์ LNK ที่ถูกสร้างขึ้นอย่างพิเศษ ช่องโหว่นี้ (รหัส ZDI-CAN-25373) ถูก Trend Micro เปิดเผยต่อสาธารณะเมื่อเดือนมีนาคมที่ผ่านมา

### เบื้องหลังช่องโหว่ LNK: ความคลาดเคลื่อนใน Windows

“ข้อมูลที่ถูกสร้างขึ้นในไฟล์ LNK สามารถซ่อนเนื้อหาที่เป็นอันตรายไม่ให้ผู้ใช้เห็นได้เมื่อดูไฟล์ผ่านอินเทอร์เฟซของ Windows” โครงการ Zero Day Initiative (ZDI) ของ Trend Micro กล่าวในตอนนั้น “ผู้โจมตีสามารถใช้ช่องโหว่นี้เพื่อรันโค้ดในสิทธิ์ของผู้ใช้ปัจจุบันได้”

การวิเคราะห์ไฟล์ LNK ที่ใช้โจมตีด้วยการอาศัย ZDI-CAN-25373 พบไฟล์ตัวอย่างย่อยอีก 9 ไฟล์ ซึ่งใช้ประโยชน์จากความสับสนในการประมวลผลไฟล์ LNK อันเกิดจากการที่ Microsoft ไม่ได้ทำตามสเปก MS-SHLLINK (เวอร์ชัน 8.0) ของตนเอง

ตามสเปกกำหนดว่า ความยาวสูงสุดทางทฤษฎีของข้อความในไฟล์ LNK คือค่าจำนวนเต็มมากที่สุดที่เก็บได้ในสองไบต์ (คือ 65,535 ตัวอักษร) แต่การทำงานจริงใน Windows 11 จำกัดเนื้อหาที่เก็บได้สูงสุด 259 ตัวอักษร ยกเว้นในส่วนของอาร์กิวเมนต์คำสั่ง (command-line arguments)




“สิ่งนี้ทำให้เกิดความสับสน เช่น ไฟล์ LNK บางไฟล์อาจถูกประมวลผลแตกต่างกันระหว่างตามสเปกกับวิธีที่ Windows ใช้งานจริง หรือแม้แต่ไฟล์ LNK ที่ควรจะถือว่าไม่ถูกต้องตามสเปก ก็ยังสามารถใช้งานได้จริงใน Microsoft Windows”

“ด้วยความคลาดเคลื่อนนี้ ผู้โจมตีจึงสามารถสร้างไฟล์ LNK ให้ดูเหมือนว่าจะรันคำสั่งหนึ่ง แต่ในความจริงกลับรันอีกคำสั่งหนึ่งเมื่อทำงานบน Windows หรือไฟล์เดียวกันอาจถูกมองว่าไม่ถูกต้องโดยโปรแกรมวิเคราะห์ของบุคคลที่สามได้เช่นกัน”

ผลกระทบจากการนำปัญหา whitespace padding มารวมกับความสับสนในการประมวลผล LNK คือ ผู้โจมตีสามารถซ่อนคำสั่งที่จะถูกสั่งรัน ไม่ให้มองเห็นได้ทั้งในอินเทอร์เฟซของ Windows และเครื่องมือวิเคราะห์จากบุคคลที่สาม

**วิธีการแพร่กระจายและเป้าหมายของ XDigo**

ไฟล์ LNK ทั้ง 9 ไฟล์นี้ถูกแจกจ่ายภายในไฟล์ ZIP ซึ่งแต่ละไฟล์ ZIP จะมี ZIP อีกชั้นหนึ่ง ที่ด้านในบรรจุไฟล์ PDF, ไฟล์ปฏิบัติการจริงแต่ถูกเปลี่ยนชื่อ และไฟล์ DLL อันตรายที่จะถูก sideload ผ่านไฟล์ปฏิบัติการนั้น

นอกจากนี้ ห่วงโซ่การโจมตีนี้ยังถูก BI.ZONE บันทึกไว้เมื่อปลายเดือนที่แล้วว่าเป็นฝีมือของกลุ่มผู้โจมตีที่เรียกว่า Silent Werewolf ซึ่งใช้วิธีเดียวกันแพร่มัลแวร์เข้าสู่บริษัทในมอลโดวาและรัสเซีย

ไฟล์ DLL จะทำหน้าที่เป็นตัวดาวน์โหลดในขั้นแรก ชื่อว่า ETDownloader โดยมีจุดประสงค์เพื่อติดตั้งโปรแกรมเก็บข้อมูลหรือ implant ที่เรียกว่า XDigo โดยดูจากโครงสร้างพื้นฐาน, กลุ่มเป้าหมาย, ช่วงเวลา, เทคนิค, และเครื่องมือที่ใช้สอดคล้อง

กัน XDigo ถูกประเมินว่าเป็นเวอร์ชันใหม่ของมัลแวร์ (“UsrRunVGA.exe”) ที่ Kaspersky เคยอธิบายไว้เมื่อเดือนตุลาคม 2023

XDigo เป็นมัลแวร์ประเภท stealer ที่สามารถดึงไฟล์, ข้อมูลจากคลิปบอร์ด, และจับภาพหน้าจอได้ อีกทั้งยังรองรับคำสั่งให้รันคำสั่งหรือไฟล์ปฏิบัติการที่ดาวน์โหลดจากเซิร์ฟเวอร์ระยะไกลผ่าน HTTP GET และจะส่งข้อมูลที่ขโมยได้ออกไปทาง HTTP POST

มีเหยื่อที่ยืนยันแล้วอย่างน้อยหนึ่งรายในเขตมินสก์ พร้อมทั้งหลักฐานอื่นๆ ที่บ่งชี้ว่ากลุ่มเป้าหมายยังรวมถึงธุรกิจค้าปลีกในรัสเซีย, สถาบันการเงิน, บริษัทประกันขนาดใหญ่, และหน่วยงานไปรษณีย์ของรัฐบาล

“โปรไฟล์เป้าหมายนี้สอดคล้องกับแนวทางของ XDSpy ที่มุ่งเล่นงานหน่วยงานรัฐบาลในยุโรปตะวันออก โดยเฉพาะในเบลารุส” HarfangLab กล่าว “ความมุ่งมั่นของ XDSpy ยังแสดงให้เห็นความสามารถในการหลบเลี่ยงการตรวจจับ เพราะมัลแวร์ของกลุ่มนี้ถูกระบุว่าเป็นมัลแวร์กลุ่มแรกที่พยายามหลบเลี่ยงการตรวจจับของ Sandbox จาก PT Security บริษัทความปลอดภัยไซเบอร์ของรัสเซียที่ให้บริการแก่หน่วยงานรัฐบาลและสถาบันการเงินในรัสเซีย”

การโจมตีด้วยมัลแวร์ XDigo นี้แสดงให้เห็นถึงความซับซ้อนของผู้โจมตีที่ใช้ประโยชน์จากช่องโหว่เล็กๆ ในระบบปฏิบัติการและความคลาดเคลื่อนระหว่างสเปกกับการทำงานจริง เพื่อซ่อนเจตนาและหลีกเลี่ยงการตรวจจับ องค์กรและผู้ใช้งานควรตระหนักถึงภัยคุกคามประเภทนี้ และอัปเดตระบบปฏิบัติการอย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่อาจถูกนำไปใช้ประโยชน์ได้

**ข้อมูลอ้างอิง**

**Jun 23, 2025 By Ravie Lakshmanan**

- https://thehackernews.com/2025/06/xdigo-malware-exploits-windows-lnk-flaw.html