ประจำวันพุธที่ 28 กันยายน 2565

Erbium มัลแวร์ตัวใหม่ สามารถขโมยรหัสผ่าน ที่แพร่กระจายไปกับโปรแกรมแคร็กเกม

มัลแวร์ใหม่ที่ขโมยข้อมูล 'Erbium' กำลังถูกแพร่กระจายไปกับโปรแกรมการโกงสำหรับวิดีโอเกมยอดนิยม เพื่อใช้ขโมยข้อมูลประจำตัวของเหยื่อและ cryptocurrency wallets

โดยที่ Erbium เป็น Malware-as-a-Service (MaaS) ที่ให้บริการสมาชิกรูปแบบใหม่ เพื่อใช้ขโมยข้อมูลที่กำลังได้รับความนิยมในชุมชนอาชญากรรมทางอินเทอร์เน็ต ด้วยฟังก์ชันการทำงานที่มากขึ้น และราคาที่ไม่สูงมาก โดยนักวิจัยจาก ทีมของ Cluster25 เป็นคนแรกที่รายงานเกี่ยวกับ Erbium เมื่อต้นเดือน

Erbium เริ่มแรกมีค่าบริการราคา 9 ดอลลาร์ต่อสัปดาห์ แต่เนื่องจากความนิยมเพิ่มขึ้นในช่วงปลายเดือนสิงหาคม ราคาจึงเพิ่มขึ้นถึง 100 ดอลลาร์ต่อเดือน หรือ 1,000 ดอลลาร์สำหรับใบอนุญาตเต็มปี เมื่อเทียบกับตัวเลือก "defacto" ค่าใช้จ่ายของ Erbium อยู่ที่ประมาณหนึ่งในสาม ดังนั้น จึงตั้งเป้าที่จะขัดขวางตลาดสำหรับมัลแวร์ที่มักใช้โดยผู้คุกคาม เช่นเดียวกับมัลแวร์ขโมยข้อมูลอื่นๆ Erbium จะขโมยข้อมูลที่จัดเก็บไว้ในเว็บเบราว์เซอร์ (ที่ใช้ Chromium หรือ Gecko) เช่น รหัสผ่าน คุกกี้ บัตรเครดิต และข้อมูลป้อนอัตโนมัติ มัลแวร์ยังพยายามกรองข้อมูลจากกระเป๋าเงินดิจิตอลขนาดใหญ่ที่ติดตั้งบนเว็บเบราว์เซอร์เป็นส่วนขยาย เช่น Exodus, Atomic, Armory, Bitecoin-Core, Bytecoin, Dash-Core, Electrum, Electron, Coinomi, Ethereum, Litecoin-Core, Monero-Core, Zcash และ Jaxx ก็ถูกขโมยเช่นกัน

Erbium ยังขโมยรหัสการตรวจสอบสิทธิ์แบบสองปัจจัยจาก Trezor Password Manager, EOS Authenticator, Authy 2FA และ Authenticator 2FA และสามารถจับภาพหน้าจอจากจอภาพทั้งหมด ขโมยโทเค็น Steam และ Discord ขโมยไฟล์ตรวจสอบสิทธิ์ของ Telegram และกำหนดโปรไฟล์โฮสต์ตามระบบปฏิบัติการและฮาร์ดแวร์

โดย Cluster25 รายงานการโจมตีของ Erbium ทั่วโลก รวมทั้งในสหรัฐอเมริกา ฝรั่งเศส โคลอมเบีย สเปน อิตาลี อินเดีย เวียดนาม และมาเลเซีย โดยแคมเปญ Erbium ใช้การ Crack game เป็นตัวล่อ ซึ่งเป็นช่องทางที่สามารถกระจายได้อย่างมาก ดังนั้น เพื่อป้องกันไม่ให้ภัยคุกคาม ควรหลีกเลี่ยงการดาวน์โหลดซอฟต์แวร์ละเมิดลิขสิทธิ์ สแกนไฟล์ที่ดาวน์โหลดทั้งหมดบนเครื่องมือ และทำการอัปเดทซอฟต์แวร์ให้ทันสมัยอยู่เสมอ และทำการติดตั้งแพตช์ความปลอดภัยล่าสุดที่มี

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/new-erbium-password-stealing-malware-spreads-as-game-cracks-cheats/