แคสเปอร์สกี้ แลป เผย โจรไซเบอร์ล่อผู้ใช้ติดตั้งซอฟต์แวร์ผิดกฎหมาย เพื่อใช้เป็นแหล่งขุดเงินคริปโต

นักวิจัยของแคสเปอร์สกี้ แลป ได้เปิดเผยกลโกงโดยการแพร่กระจายไมน์นิ่งซอฟต์แวร์และติดตั้งในเครื่องพีซีของผู้ใช้ผ่านซอฟต์แวร์ผิดกฎหมายที่ใช้กันทั่วไปในการทำงานและเพื่อความบันเทิง เช่น ซอฟต์แวร์ตกแต่งภาพและข้อความ เป็นต้น เครื่องพีซีจะถูกใช้เป็นตัวสร้างเงินดิจิทัล หรือ คริปโตเคอเรนซี่ (cryptocurrency) เพื่อสร้างกำไรให้กับโจรไซเบอร์

ปัจจุบัน ตลาดเงินดิจิทัลได้ขยายตัวอย่างรวดเร็วทั้งจำนวนและมูลค่าการลงทุน โจรไซเบอร์ก็ได้จับตามองการเติบโตนี้อย่างใกล้ชิด ความตื่นตัวต่อเงินดิจิทัลทำให้ผู้ใช้จำนวนมากเริ่มเล่นรวมถึงผู้ใช้ที่ขาดความรู้ความชำนาญด้านไอทีจึงกลายเป็นเหยื่อกลโกงได้ง่าย ยกตัวอย่างเช่น เทรนด์นักขุดเงินดิจิทัล (cryptocurrency miner) ซึ่งเป็นหนึ่งในเทรนด์สำคัญของปี 2017 จากข้อมูลในรายงาน Kaspersky Security Bulletin นักวิจัยของแคสเปอร์สกี้ แลป ได้ทำนายเทรนด์นี้ไว้เมื่อปี 2016 ตอนที่พบการกลับมาของไมน์นิ่งซอฟต์แวร์ขณะที่เงินดิจิทัล Zcash กำลังเป็นที่นิยม หนึ่งปีหลังจากนั้น ก็พบไมเนอร์หรือนักขุดเงินเกิดขึ้นจำนวนมาก โจรไซเบอร์เองก็ใช้เครื่องมือและเทคนิคต่างๆ เช่น แคมเปญโซเชียลเอ็นจิเนียริ่ง และการแพร่กระจายซอฟต์แวร์ที่แคร็กไว้เพื่อเพิ่มจำนวนเครื่องพีซีติดเชื้อให้มากที่สุด

เร็วๆ นี้ผู้เชี่ยวชาญของแคสเปอร์สกี้ แลป ได้ค้นพบเว็บไซต์จำนวนหนึ่งที่มีความคล้ายคลึงกัน คือ เสนอช่องทางให้ผู้ใช้อินเทอร์เน็ตสามารถดาวน์โหลดซอฟต์แวร์ผิดกฎหมายมาใช้โดยไม่เสียค่าใช้จ่าย โจรไซเบอร์ได้เลือกใช้โดเมนเนมที่คล้ายกับเว็บไซต์ของจริง หลังจากที่ผู้ใช้ดาวน์โหลดซอฟต์แวร์แล้ว ก็จะได้รับ archive ที่บรรจุโปรแกรมขุดมาด้วย

ตัว archive การติดตั้งจะประกอบด้วยไฟล์ข้อความที่มีข้อมูลการติดตั้ง คือแอดเดรสของวอลเล็ต (wallet) และไมนิ่งพูล (mining pool) ไมนิ่งพูลคือเซิร์ฟเวอร์ที่รวมผู้เข้าร่วม (participant) ทั้งหลายไว้ที่เดียวกันและแบ่งงานขุดในคอมพิวเตอร์หลายเครื่อง ผู้เข้าร่วมจะได้รับส่วนแบ่งเป็นเงินดิจิทัลซึ่งจะไวกว่าการขุดผ่านคอมพิวเตอร์ของตัวเองเพียงเครื่องเดียว การขุดเงินบิตคอยน์และเงินดิจิทัลอื่นๆ เป็นกระบวนการที่ใช้เวลาและทรัพยากรมาก ดังนั้น การขุดผ่านพูลจึงเพิ่มผลผลิตและความรวดเร็วการในผลิตเงินดิจิทัล

หลังจากติดตั้งโปรแกรมแล้ว นักขุดเงินก็เริ่มงานผลิตเงินดิจิทัลให้โจรไซเบอร์ที่เครื่องของเหยื่ออย่างเงียบๆ จาก

รายงานของแคสเปอร์สกี้ แลป เคสที่พบทุกเคสใช้ซอฟต์แวร์โปรเจ็ก NiceHash ซึ่งเพิ่งถูกเจาะความปลอดภัยครั้งใหญ่เมื่อเร็วๆ นี้ เป็นการโจรกรรมเงินดิจิทัลมูลค่าหลายล้านดอลล่าร์ เหยื่อบางรายก็เกี่ยวข้องกับไมนิ่งพูลเดียวกันด้วย

นอกจากนี้ ผู้เชี่ยวชาญยังพบว่านักขุดบางรายมีฟีเจอร์พิเศษที่ให้ผู้ใช้เปลี่ยนเลขวอลเล็ตหรือเปลี่ยนพูลได้จากระยะไกล ซึ่งหมายความว่า โจรไซเบอร์จะสามารถตั้งจุดหมายการขุดเงินดิจิทัลใหม่ได้ตามต้องการ และสามารถบริหารจัดการรายได้ด้วยการกระจายการขุดระหว่างวอลเล็ต หรือตั้งค่าให้เครื่องคอมพิวเตอร์ของเหยื่อเป็นพูลอีกแห่งก็ยังได้

อเล็กซานเดอร์ โคเลสนิคอฟ นักวิเคราะห์มัลแวร์ของแคสเปอร์สกี้ แลป กล่าวว่า “ถึงจะไม่นับเป็นโปรแกรมมุ่งร้าย แต่ไมนิ่งซอฟต์แวร์ก็ลดประสิทธิภาพการทำงานของระบบคอมพิวเตอร์ ซึ่งส่งผลกระทบต่อผู้ใช้แน่นอน รวมถึงค่าไฟฟ้าที่สูงขึ้นด้วย ซึ่งถึงแม้จะไม่ใช่ประเด็นหลักของการตกเป็นเหยื่อ แต่ก็ยังเป็นเรื่องที่ไม่น่าพิสมัย ผู้ใช้บางรายอาจจะรู้สึกดีที่เห็นคนอื่นรวยขึ้น แต่เราขอแนะนำให้ผู้ใช้ต่อต้านกลโกงนี้ เพราะถึงแม้จะไม่ได้เกิดจากมัลแวร์ แต่ก็นับเป็นการโกงอยู่ดี”

แคสเปอร์สกี้ แลป ขอแนะนำวิธีป้องกันเครื่องคอมพิวเตอร์ไม่ให้ตกอยู่ในเครือข่ายการขุดเงินดิจิทัล ดังนี้
- ดาวน์โหลดซอฟต์แวร์ถูกกฎหมายจากแหล่งที่เชื่อถือได้เท่านั้น
- ติดตั้งโซลูชั่นเพื่อความปลอดภัย เช่น Kaspersky Internet Security หรือ Kaspersky Free ที่จะช่วยปกป้องจากภัยคุกคามต่างๆ รวมถึงไมนิ่งซอฟต์แวร์ด้วย

ข้อมูลเพิ่มเติม
- ข้อมูลโครงการนักขุดที่เพิ่งค้นพบ

    Nhash: petty pranks with big finances

- ข้อมูลการพัฒนาเงินดิจิทัลในแง่ความปลอดภัยไซเบอร์

    Threat Predictions for Cryptocurrencies in 2018

https://www.brighttalk.com/webcast/15591/289993