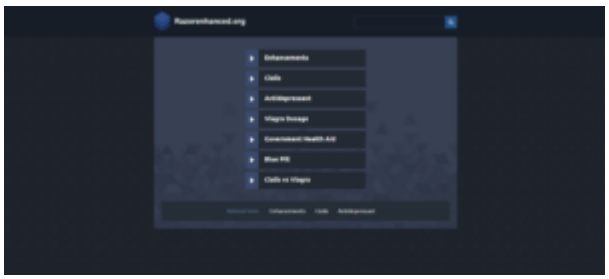
แคสเปอร์สกี้เตือนการเข้าโดเมนอันตรายที่โจรไซเบอร์ใช้ดักหาเงิน



นักวิจัยแคสเปอร์สกี้ค้นพบว่า ในจำนวนโดเมนที่ inactive แล้วนั้น มีโดเมนจำนวนมากกว่าพันรายการที่หากคุณคลิกเข้าไปจะโยงคุณยัง URL ไม่พึงประสงค์ ซึ่งล้วนเป็นเพจอันตรายทั้งสิ้น และนี่คือกลวิธีหาเงินของพวกผู้ร้ายไซเบอร์

เมื่อบริษัทยุติการเช่าโดเมนหนึ่งๆ ก็อาจจะถูกซื้อเพื่อไปขายต่อในไซต์แหล่งประมูลราคาไซต์เก่า ซึ่งเมื่อคลิกเข้าไปที่เว็บไซต์เก่าเหล่านี้ จะแอบโยงไปยัง auction stub ซึ่งผู้ร้ายจะดูได้ว่าโดเมนใดกำลังประกาศขายทอดในตลาดบ้าง หรืออย่างน้อยๆ ก็น่าจะถูกประกาศขาย ดังนั้น เมื่อหาทางแทนที่ stub ด้วยอย่างอื่น เช่น ลิ้งก์ที่เป็นอันตราย (malicious link) เป็นต้น พวกคนโกงเหล่านี้ก็มีหนทางที่ล่อให้ยูสเซอร์เข้าไปติดกับ หรือใส่เล่ห์กลเพื่อหาทางกินเงินคนอื่นไปฟรีๆ จนได้
ขณะที่ทีมนักวิจัยของแคสเปอร์สกี้สำรวจวิเคราะห์ตัวเครื่องมือช่วยเหลือของเกมส์ออนไลน์ยอดฮิตอยู่นั้น ได้พบว่ามีความพยายามของแอปพลิชันที่จะย้าย(transfer)พวกเขาไปยัง URL ไม่พึงประสงค์ ซึ่งปรากฏว่าเป็น URL ที่ขึ้นรายการสำหรับจำหน่ายไว้ที่ไซต์ประมูลโดเมนไม่ใช้แล้วนั่นเอง อย่างไรก็ตาม แทนที่จะโยงกลับไปที่ไซต์ stub ที่ถูกต้อง กลับส่งต่อยูสเซอร์ไปอีกเพจที่ติดแบล็กลิสต์

การวิเคราะห์เจาะลึกเพิ่มเติมพบว่าประมาณ 1,000 เว็บไซต์ที่ถูกเสนอขายตามแพลตฟอร์มประมูลหลายแห่ง หลังจากที่ถูกโยงมายังเพจที่สอง พวก 1,000 เพจเหล่านี้จะทำการส่งต่อยูสเซอร์ไปยัง URL ไม่พึงประสงค์ 2,500 รายการ มีการดาวน์โหลดโทรจัน Shlayer ซึ่งเป็นภัยคุกคามของ macOS ที่ทำการติดตั้งแอดแวร์ลงบนอุปกรณ์ของเหยื่อ และแพร่กระจายต่อไปด้วยเว็บเพจที่มีคอนเท้นท์ที่เป็นอันตรายเหล่านี้

ระหว่างเดือนมีนาคม 2019 ถึง กุมภาพันธ์ 2020 เพจรองรับการส่งต่อ (second-stage) นับได้ 89 เปอร์เซ็นต์ จะโยงต่อไปที่เพจที่เน้นแอด ขณะที่ 11 เปอร์เซ็นต์เป็นเพจอันตราย ยูสเซอร์จะได้ข้อความกระตุ้นให้ลงโปรแกรม (ที่แท้เป็น) มัลแวร์หรือดาวน์โหลด MS Office หรือไฟล์ PDF ที่ติดเชื้อ หรือตัวเพจเองก็เต็มไปด้วยโค้ดอันตราย

ตามความเห็นของผู้เชี่ยวชาญ เหตุที่ซ่อนอยู่เบื้องหลังแผนการโยงใยส่งต่อหลายซับหลายซ้อนแบบนี้คือเรื่องการเงิน คนร้ายได้เงินจากการหาทราฟฟิกเข้ามาที่เพจเยอะๆ ทั้งที่เป็นเพจแบบโฆษณาถูกต้อง และที่เป็นเพจแฝงอันตราย วิธีการล่อลวงแบบนี้เรียกว่า Malvertising ยกตัวอย่างเพจหนึ่งที่เราเจอ พบว่าได้รับการส่งต่อเหยื่อที่โยงมาเข้าเพจนี้ด้วยไม่รู้เรื่องเลยถึง 600 รายภายใน 10วัน ที่น่าจะเป็นได้มากที่สุดคือผู้ร้ายได้รับเงินค่าตอบแทนตามจำนวนที่มีคนคลิกเข้ามา ในกรณีของ Shlayer คนที่ช่วยแพร่กระจายมัลแวร์ได้รับเงินต่อทุกครั้งที่มีการลงมัลแวร์บนดีไวซ์ เป็นได้ว่าสแกม (scam) เป็นผลของความบกพร่องการกรองแอดในโมดูลที่แสดงคอนเท้นท์ในเครือข่ายโฆษณาของบรรดาเธิร์ดปาร์ตี้

“โชคไม่ดีนักที่ยูสเซอร์เองก็ไม่สามารถที่จะทำอะไรได้มากนักเพื่อเลี่ยงการถูกลากโยงไปเพจที่เป็นอันตราย โดเมนที่ที่การทำแบบนี้ก็มักจะเป็นโดเมนที่ครั้งหนึ่งก็ใช้งานถูกต้องไม่มีปัญหาอะไร บางทีอาจจะเป็นโดเมนที่ยูสเซอร์เองก็เคยคลิกเข้าไปอยู่บ่อยๆ ก็ได้ และก็ไม่มีทางจะรู้ได้ว่าเป็นเพจที่ตอนกลายร่างเป็นศูนย์ส่งต่อไปหาเพจที่ดาวน์โหลดมัลแวร์มาใส่เราหรือไม่ ที่เพิ่มความท้าทายเข้าอีกก็คือการที่เผอิญคลิกเข้าไปยังรูปแบบต่างๆ ที่เป็นแขนขาของไซต์อันตราย เช่น วันหนึ่งคุณคลิกเข้าไซต์ที่ไม่ได้ประสบปัญหาแต่อย่างใด แต่ถ้าคุณลองพยายามจะเข้าผ่าน VPN คุณอาจจะถูกโยงส่งต่อไปเพจที่ดาวน์โหลด Shlayer มาให้ โดยทั่วไปแล้วกลเม็ดแบบ malvertising เช่นนี้จะมีความซับซ้อนอยู่พอตัว ยากต่อการเปิดโปงล่วงรู้รายละเอียดทั้งหมด ดังนั้น การป้องกันตัวเองที่ดีที่สุดของเราที่ทำได้คือการมีโซลูชั่นซีเคียวริตี้ที่แกร่งป้องกันครบทุกด้านลงบนอุปกรณ์ของเราเท่านั้นเอง” ดิมิทรี คอนดราตเยฟ นักวิเคราะห์มัลแวร์

อ่านเพิ่มเติมเกี่ยวกับลิ้งก์อันตรายเหล่านี้ได้ที่ https://securelist.com/redirect-auction/96944/

เพื่อเป็นการลดความเสี่ยงของการตกเป็นเหยื่อโทรจันผ่านทางไซต์อันตรายเช่นนี้ ต่อไปนี้คือคำแนะนำจากผู้เชี่ยวชาญของแคสเปอร์สกี้:

- ติดตั้งโปรแกรมและอัพเดทจากแหล่งที่เชื่อถือไว้ใจได้เท่านั้น
- ใช้โซลูชั่นเพื่อความปลอดภัยที่ไว้ใจได้ เช่น Kaspersky Security Cloud ที่มีฟีเจอร์แอนตี้ฟิชชิ่ง ป้องกันการโยงไปเพจที่น่าสงสัยได้