วันที่ 20 มิถุนายน 2568

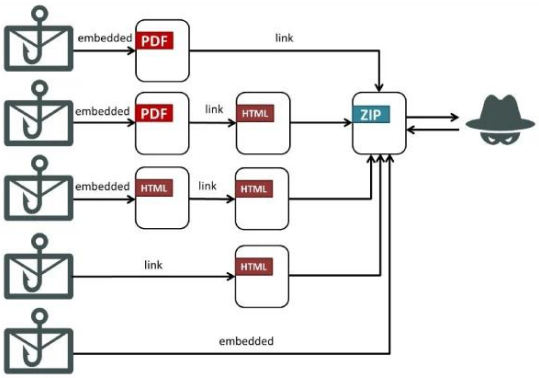
Silver Fox APT โจมตีไต้หวันด้วยมัลแวร์ Gh0stCringe และ HoldingHands RAT

นักวิจัยด้านความปลอดภัยไซเบอร์ออกมาเตือนถึงแคมเปญฟิชชิ่งรูปแบบใหม่ที่กำลังพุ่งเป้าไปยังผู้ใช้ในไต้หวัน โดยใช้มัลแวร์ HoldingHands RAT และ Gh0stCringe

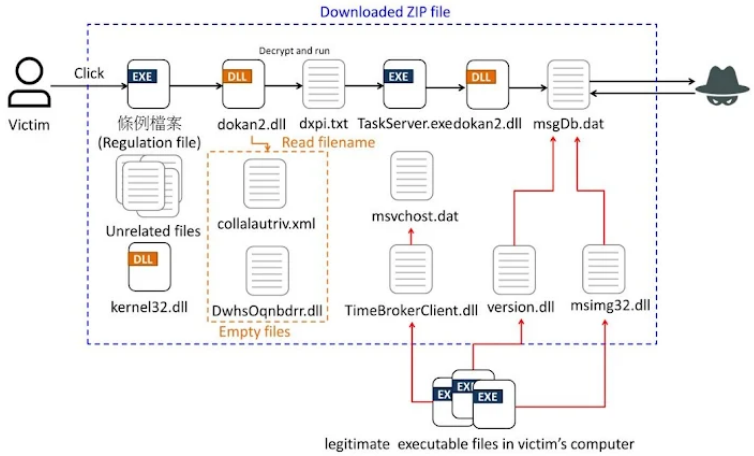
กิจกรรมนี้เป็นส่วนหนึ่งของแคมเปญขนาดใหญ่ ซึ่งก่อนหน้านี้ได้ปล่อยมัลแวร์เฟรมเวิร์ก Winos 4.0 ตั้งแต่เดือนมกราคมที่ผ่านมา โดยอาศัยการส่งอีเมลฟิชชิ่งที่ปลอมเป็นกรมสรรพากรของไต้หวัน ตามรายงานของ Fortinet FortiGuard Labs ที่เปิดเผยผ่าน The Hacker News

บริษัทด้านความปลอดภัยไซเบอร์ระบุว่า จากการติดตามอย่างต่อเนื่อง พบตัวอย่างมัลแวร์เพิ่มเติม และพบว่าเป็นฝีมือของกลุ่มผู้ก่อเหตุรายเดิมที่ใช้ชื่อว่า Silver Fox APT โดยใช้ไฟล์ PDF หรือ ZIP ที่ฝังมัลแวร์ ส่งผ่านอีเมลฟิชชิ่งเพื่อติดตั้ง Gh0stCringe และมัลแวร์ที่พัฒนาต่อยอดจาก HoldingHands RAT

นอกจากนี้ยังน่าสังเกตว่า ทั้ง HoldingHands RAT หรือที่รู้จักในชื่อ Gh0stBins และ Gh0stCringe ต่างก็เป็นเวอร์ชันดัดแปลงของมัลแวร์โทรจันควบคุมระยะไกลชื่อดัง Gh0st RAT ซึ่งเป็นเครื่องมือยอดนิยมของกลุ่มแฮ็กเกอร์จีน



จุดเริ่มต้นของการโจมตีคือ มีการส่งอีเมลฟิชชิ่งที่ปลอมตัวเป็นข้อความจากหน่วยงานรัฐบาลหรือคู่ค้าทางธุรกิจ โดยมักใช้หัวข้อเกี่ยวกับภาษี ใบแจ้งหนี้ หรือเงินบำนาญ เพื่อหลอกให้เหยื่อเปิดไฟล์แนบ หรือในบางกรณี อาจฝังภาพไว้ในเนื้อหาอีเมล เมื่อผู้รับคลิกที่ภาพหรือไฟล์แนบ มัลแวร์ก็จะถูกดาวน์โหลดทันที



ไฟล์ PDF เหล่านี้จะมีลิงก์ที่พาเหยื่อไปยังหน้าดาวน์โหลด ซึ่งจะมีไฟล์ ZIP อยู่ข้างใน โดยไฟล์ดังกล่าวมักซ่อนไฟล์ executable ปกติหลายไฟล์ ตัวโหลด shellcode และ shellcode ที่ถูกเข้ารหัสไว้

กระบวนการติดตั้งมัลแวร์จะดำเนินไปเป็นลำดับขั้น เริ่มจากตัวโหลด shellcode ที่จะถอดรหัสและรัน shellcode ซึ่งจริงๆ แล้วเป็นไฟล์ DLL ที่ถูก sideload โดยไฟล์โปรแกรมปกติ ด้วยเทคนิค DLL side-loading ในขั้นตอนต่อไปของการโจมตี จะมีการใช้ payload เพื่อหลีกเลี่ยงการตรวจจับบนเครื่อง VM และพยายามยกระดับสิทธิ์ เพื่อให้มัลแวร์ทำงานได้อย่างเต็มที่บนเครื่องที่ถูกเจาะ

ในขั้นตอนสุดท้ายจะมีการรันไฟล์ "msgDb.dat" ซึ่งทำหน้าที่เชื่อมต่อกับเซิร์ฟเวอร์สั่งการ (C2) เพื่อเก็บข้อมูลของผู้ใช้ และดาวน์โหลดโมดูลเพิ่มเติม สำหรับจัดการไฟล์และควบคุมเดสก์ท็อประยะไกล

Fortinet ยังพบว่ากลุ่มนี้เผยแพร่ Gh0stCringe ผ่านไฟล์ PDF ที่แนบมากับอีเมลฟิชชิ่ง ซึ่งจะพาผู้ใช้ไปยังหน้า HTM สำหรับดาวน์โหลดเอกสารอีกครั้ง

“ลำดับการโจมตีนี้ประกอบด้วยหลายส่วน ทั้ง shellcode และตัวโหลด ทำให้กระบวนการมีความซับซ้อนมากขึ้น” บริษัทระบุ “ตั้งแต่ Winos, HoldingHands จนถึง Gh0stCringe กลุ่มนี้ยังคงพัฒนามัลแวร์และวิธีการแพร่กระจายอย่างต่อเนื่อง”

ข้อแนะนำ (Recommendation)

- อัปเดตระบบและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด
- เฝ้าระวังพฤติกรรมต้องสงสัย เช่น การเชื่อมต่อไปยัง IP/Domain ที่ไม่รู้จัก
- จำกัดสิทธิ์ผู้ใช้งานและบัญชีแอดมิน
- สำรองข้อมูลอย่างสม่ำเสมอ และทดสอบการกู้คืน

ข้อมูลอ้างอิง

Jun 17, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/silver-fox-apt-targets-taiwan-with.html