วันที่ 8 ตุลาคม 2568

กลุ่ม BatShadow ใช้มัลแวร์ใหม่ที่พัฒนาด้วยภาษา Go ชื่อว่า “Vampire Bot” เพื่อหลอกล่อนักหางาน

กลุ่มผู้ไม่หวังดีจากเวียดนามที่ถูกระบุชื่อว่า BatShadow กำลังถูกเชื่อมโยงกับแคมเปญโจมตีใหม่ที่ใช้กลยุทธ์ทางสังคม (Social Engineering) สุดซับซ้อน เพื่อหลอกล่อนักหางานและผู้เชี่ยวชาญด้านการตลาดดิจิทัลให้ดาวน์โหลดมัลแวร์ชนิดใหม่ที่ไม่เคยถูกบันทึกมาก่อนชื่อว่า Vampire Bot

กลลวงสมัครงาน: หลอกด้วยเอกสารปลอม

นักวิจัยจาก Aryaka Threat Research Labs คือ Aditya K Sood และ Varadharajan K เปิดเผยว่า “ผู้โจมตีแสร้งทำตัวเป็นฝ่ายสรรหาพนักงาน โดยส่งไฟล์ที่ดูเหมือนเป็นเอกสารรายละเอียดงานหรือเอกสารของบริษัทมาให้” และเน้นย้ำว่า “เมื่อเหยื่อเปิดไฟล์เหล่านั้นกระบวนการติดมัลแวร์ที่เขียนด้วยภาษา Go จะเริ่มต้นขึ้น”

เส้นทางการโจมตี (Attack Chain) มีหลายขั้นตอนที่ซับซ้อน:

1. จุดเริ่มต้น: การโจมตีจะเริ่มจากไฟล์ ZIP ที่ภายในมีเอกสาร PDF หลอกตา พร้อมไฟล์ลัด (LNK) หรือไฟล์ปฏิบัติการ (EXE) ที่ถูกทำให้ดูเหมือนเป็น PDF เพื่อหลอกให้เหยื่อเปิด
2. การดาวน์โหลดมัลแวร์: เมื่อเหยื่อเปิดไฟล์ LNK จะมีสคริปต์ PowerShell ฝังอยู่ ซึ่งจะเชื่อมต่อไปยังเซิร์ฟเวอร์ภายนอกเพื่อดาวน์โหลด:
    - เอกสารหลอก: ไฟล์ PDF เกี่ยวกับตำแหน่งงานด้านการตลาดที่โรงแรม Marriott เพื่อให้เหยื่อตายใจ
    - เครื่องมือควบคุม: ไฟล์ ZIP อีกชุด ซึ่งภายในมีไฟล์ที่เกี่ยวข้องกับซอฟต์แวร์ XtraViewer ซึ่งเป็นโปรแกรมเชื่อมต่อเดสก์ท็อประยะไกล และมีแนวโน้มว่าจะถูกใช้เพื่อสร้างช่องทางเข้าถึงเครื่องของเหยื่ออย่างต่อเนื่อง

กลอุบาย "บังคับ" ใช้ Microsoft Edge

ขั้นตอนที่ซับซ้อนที่สุดคือการพยายามหลีกเลี่ยงการบล็อกของเบราว์เซอร์ Chrome และบังคับให้เหยื่อไปใช้ Microsoft Edge:

- หากเหยื่อคลิกลิงก์ในไฟล์ PDF ที่หลอกให้ “ดูรายละเอียดงานเพิ่มเติม” จะถูกพาไปยังหน้าเว็บอีกหน้าหนึ่ง
- หน้านั้นจะแสดง ข้อความผิดพลาดปลอมๆ ว่าเบราว์เซอร์ที่ใช้อยู่ไม่รองรับ และ “หน้านี้สามารถดาวน์โหลดได้เฉพาะบน Microsoft Edge เท่านั้น”

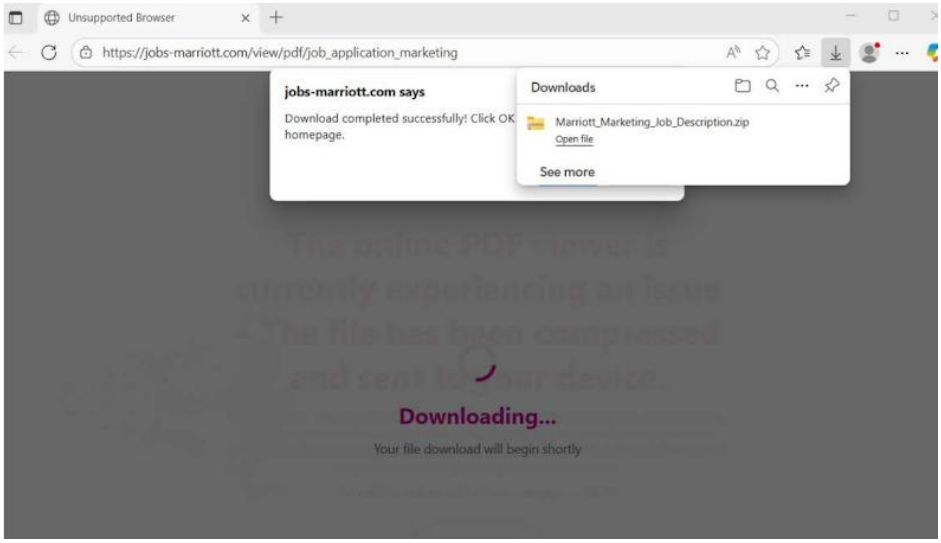
Aryaka อธิบายกลไกนี้ว่า: “เมื่อผู้ใช้คลิกปุ่ม OK เบราว์เซอร์ Chrome จะบล็อกการเปลี่ยนหน้าโดยอัตโนมัติ” จากนั้น หน้าดังกล่าวจะแสดงข้อความอีกอันหนึ่งที่บอกให้ผู้ใช้ คัดลอก URL แล้วเปิดในเบราว์เซอร์ Edge ด้วยตนเองเพื่อดาวน์โหลดไฟล์

การที่ผู้โจมตีพยายามให้เหยื่อใช้ Edge แทน Chrome หรือเบราว์เซอร์อื่นๆ นั้น เป็นเพราะการเปิดลิงก์แบบมีสคริปต์หรือการเปลี่ยนหน้าโดยอัตโนมัติมักถูกบล็อกโดยค่าเริ่มต้นของ Chrome แต่หากเหยื่อ คัดลอกลิงก์ไปเปิดใน Edge เอง ระบบจะมองว่าเป็นการกระทำโดยผู้ใช้ ทำให้กระบวนการติดมัลแวร์สามารถดำเนินต่อได้

การลงมือด้วย Vampire Bot

เมื่อเหยื่อเปิดหน้าใน Edge แล้ว หน้าเว็บจะเปิดโดยอัตโนมัติและแสดงข้อความผิดพลาดอีกครั้งว่า “ตัวดูไฟล์ PDF ออนไลน์มีปัญหา ขณะนี้ไฟล์ถูกบีบอัดและส่งไปยังอุปกรณ์ของคุณแล้ว”

ขั้นตอนนี้จะทำให้มีการดาวน์โหลดไฟล์ ZIP โดยอัตโนมัติ ซึ่งภายในมีไฟล์ที่อ้างว่าเป็นรายละเอียดงาน โดยใช้ชื่อว่า “Marriott_Marketing_Job_Description.pdf.exe” ซึ่งเป็นกลลวงที่พยายามทำให้เหยื่อเข้าใจผิดว่าเป็นไฟล์ PDF ด้วยการเว้นวรรคระหว่าง “.pdf” และ “.exe”



ไฟล์ปฏิบัติการดังกล่าวคือมัลแวร์ที่เขียนด้วยภาษา Go ชื่อว่า Vampire Bot ซึ่งมีความสามารถสูง:

- เก็บข้อมูลระบบของเครื่องที่ติดเชื้อ
- ขโมยข้อมูลหลากหลายประเภท
- ถ่ายภาพหน้าจอเป็นระยะๆ
- เชื่อมต่อกับเซิร์ฟเวอร์ของผู้โจมตีที่อยู่ที่ “api3.samsungcareers[.]work” เพื่อรับคำสั่งหรือดาวน์โหลดมัลแวร์เพิ่มเติม

การเชื่อมโยงกับ BatShadow และเวียดนาม

- การเชื่อมโยง BatShadow กับ เวียดนาม มาจากการใช้ที่อยู่ IP 103.124.95[.]161 ซึ่งเคยถูกตรวจพบว่าใช้โดยกลุ่มแฮ็กเกอร์จากประเทศนั้น
- กลุ่มเป้าหมายของการโจมตีคือเชี่ยวชาญด้านการตลาดดิจิทัล ซึ่งเป็นกลุ่มที่มักตกเป็นเป้าของแฮ็กเกอร์ชาวเวียดนามที่ต้องการขโมยบัญชี Facebook ธุรกิจ
- กลุ่ม BatShadow คาดว่ามีกิจกรรมมานานอย่างน้อยหนึ่งปี โดยในแคมเปญก่อนๆ เคยใช้โดเมนคล้ายกัน เช่น samsung-work.com เพื่อแพร่กระจายมัลแวร์ตระกูล Agent Tesla, Lumma Stealer, และ Venom RAT

Aryaka สรุปว่า “กลุ่ม BatShadow ยังคงใช้กลยุทธ์ทางสังคมที่ซับซ้อนเพื่อหลอกล่อนักหางานและผู้เชี่ยวชาญด้านการตลาดดิจิทัล ด้วยการปลอมเอกสารและใช้กระบวนการติดมัลแวร์หลายขั้นตอน เพื่อแพร่กระจายมัลแวร์ Vampire Bot ที่สามารถสอดแนมระบบ ขโมยข้อมูล และสั่งงานจากระยะไกลได้” ซึ่งเป็นการยืนยันความต่อเนื่องของภัยคุกคามรูปแบบนี้จากเวียดนาม ที่เคยมีการเปิดเผยการโจมตีหลายขั้นตอนที่มีลักษณะคล้ายกันโดยใช้ Quasar RAT ผ่านอีเมลฟิชชิงแนบไฟล์ รายละเอียดงานเมื่อเดือนตุลาคมปี 2024 โดยบริษัท Cyble

ข้อมูลอ้างอิง

Oct 7, 2025, By Ravie Lakshmanan
https://thehackernews.com/2025/10/batshadow-group-uses-new-go-based.html