Rocket Kitten ส่งมัลแวร์ Woolen-GoldFish และ GHOLE ออกโจมตี

Rocket Kitten ส่งมัลแวร์ Woolen-GoldFish และ GHOLE ออกโจมตี
ร็อคเก็ท คิทเท่น (Rocket Kitten) คือกลุ่มภัยคุกคามไซเบอร์ที่ยกขบวนโจมตีองค์กรภาครัฐและเอกชนของอิสราเอลและฝั่งยุโรป ซึ่งขณะนี้ Rocket Kitten ได้มีการโจมตีทางไซเบอร์สองรูปแบบ ได้แก่ การโจมตีผ่านมัลแวร์ในตระกูล GHOLE และ ปฏิบัติการ Woolen-GoldFish โดยการโจมตีทั้งสองรูปแบบมีเป้าหมายเดียวกันและอาจเป็นไปได้ว่ามีหน่วยงานระดับประเทศอยู่เบื้องหลัง
GHOLE เป็นตระกูลของมัลแวร์ที่ได้รับการกล่าวถึงในงาน Chaos Communication Congress ครั้งที่ 31หรือ 31C3 ของกลุ่มสมาพันธ์แฮกเกอร์ที่รู้จักกันในนาม Chaos Computer Club (CCC) ในระหว่างการบรรยายว่า ได้เข้าไปมีส่วนร่วมในการโจมตีแบบเจาะจงกลุ่มเป้าหมาย (targeted attack) และจากการรวบรวมตัวอย่างมัลแวร์ตัวตั้งแต่อดีตพบว่า มัลแวร์ตระกูลนี้ถือกำเนิดในปี 2011 โดย Rocket Kitten เพื่อปฏิบัติหน้าที่โจมตีเป้าหมายแบบเจาะจงของพวกเขา
ในขณะที่ ปฏิบัติการ Woolen-GoldFish เป็นการโจมตีทางไซเบอร์ที่มีผู้ตั้งข้อสงสัยว่ามีหน่วยงานระดับประเทศเป็นผู้สนับสนุน หรือมีสาเหตุทางการเมืองเป็นปัจจัยกระตุ้น โดยการโจมตีดังกล่าวมีเป้าหมายดังต่อไปนี้:

- องค์กรพลเรือนในอิสราเอล
- สถาบันการศึกษาในอิสราเอล
- องค์กรภาครัฐที่พูดภาษาเยอรมัน
- องค์กรภาครัฐของยุโรป
- องค์กรเอกชนของยุโรป

เบื้องหลัง, การวิเคราะห์, การค้นพบ

โจมตีของมัลแวร์ GHOLE:

- ในเดือนกุมภาพันธ์ ปี 2015 เราได้รับการแจ้งเตือนเกี่ยวกับ ไฟล์ Excel ที่ติดมัลแวร์ โดยการวิเคราะห์และพิสูจน์พบว่า เป็นส่วนหนึ่งของ GHOLE ซึ่งเป็นหนึ่งในมัลแวร์ที่ถูกสร้างโดยกลุ่ม Rocket Kitten

- มัลแวร์ GHOLE แพร่กระจายโดยการส่งอีเมล์ถึงเหยื่อพร้อมกับการแนบไฟล์ไปด้วย ซึ่งไฟล์ที่แนบไปจะอยู่ในรูปของไฟล์ Excel ที่มักจะมีมัลแวร์ประเภทมาโครฝังอยู่

• เมื่อคุณคลิ๊กที่อีเมล์ ไฟล์ Excel จะปล่อยไฟล์ .DLL ที่จะถูกเรียกใช้โดยมัลแวร์ประเภทมาโครที่ฝังอยู่ในไฟล์ Excel

• ไฟล์ Excel ถูกสร้างขึ้นมาเพื่อลวงให้ผู้ใช้เรียกใช้มาโคร หากผู้ใช้ไม่ได้เปิดใช้งานมาโคร ไฟล์ DLL ก็จะไม่ถูกเรียกขึ้นมาทำงาน

• มัลแวร์ตระกูล Ghole ได้รับการดัดแปลงมาจากผลิตภัณฑ์ Core Impact ซึ่งเป็นซอฟต์แวร์ประเภท penetration testing ของบริษัท Core Security ซึ่งเป็นบริษัทที่ถูกต้องตามกฎหมาย

• การวิเคราะห์เพิ่มเติมพบว่ามัลแวร์ตระกูล GHOLE มีการทำงานผ่านการเชื่อมต่อเซิร์ฟเวอร์ C&C ที่มีโฮสต์หลักอยู่ในประเทศเยอรมัน โดยเซิร์ฟเวอร์ได้รับการจดทะเบียนภายใต้ลูกค้าชื่อ Medhi Mavadi แต่เราไม่แน่ใจถึงชื่อบุคคลคนนี้เนื่องจากเป็นชื่อที่พบโดยทั่วไปในประเทศเยอรมัน และเซิร์ฟเวอร์ของลูกค้าอาจจะบุกรุกและถูกใช้เป็นทางผ่านมากกว่าที่จะเป็นของกลุ่ม Rocket Kitten จริงๆ

ปฏิบัติการ Woolen-GoldFish:

• การทำงานไม่ต่างไปจาก GHOLE โดยปฏิบัติการ Woolen Goldfish คือการส่งเมล์แบบ spear-phishing โดยมีการฝังลิงค์ที่เป็นอันตรายที่เชื่อมต่อผ่าน OneDrive และนำไปสู่การดาวน์โหลดไฟล์ที่เป็นอันตราย

• มัลแวร์เพย์โหลดตัวอย่างแรกๆที่พบ พบว่าเป็นสายพันธ์หนึ่งของ GHOLE แต่ตัวอย่างที่พบในภายหลังพบว่าเป็นสายพันธ์ใหม่ซึ่งเป็นคีย์ล็อกเกอร์ส่วนใหญ่หรือที่รู้จักกันในนามของ CWoolger keylogger ซึ่งมาพร้อมกับ TSPY_WOOLERG.A

ความเป็นไปได้ในการแพร่กระจายของมัลแวร์

การวิเคราะห์ไฟล์ข้อมูลที่ติดมัลแวร์จากอีเมล์พวก spear phishing ของ Microsoft Office ผ่าน metadata เราจำกัดวงผู้ต้องสงสัยให้แคบลงเหลือแค่ “Wool3n.H4t” ซึ่งเป็นชื่อของผู้ที่แก้ไขเอกสาร Microsoft Office คนสุดท้าย โดยมี “aikido1” และ “Hoffman” เป็นผู้สมรู้ร่วมคิด
และหากศึกษาลงลึกเข้าไปอีกถึงต้นตอของ Wool3n.H4t จะพบว่า:
• เขาอาจเป็นผู้เขียนบล็อกใต้ดินภายใต้ชื่อเล่นเดียวกัน โดยในบล็อกมีเพียง 2 รายการที่ลงนามโดย “Masoud_pk”
• “Masoud_pk” อาจเป็นตัวตนที่แท้จริงของ Wool3n.H4t ทั้งนี้ “Masoud” เป็นชื่อที่พบบ่อยที่อยู่ใน 500 อันดับแรกในอิหร่าน
• debug string ที่พบในรหัส CWoolger แสดงให้เห็นว่าคอมไพลเลอร์คือ Wool3n.H4T

กล่าวโดยสรุป
จากรายงานการวิจัยเรื่องการโจมตีของ Woolen-GoldFish เจาะลึกถึงกลุ่ม Rocket Kitten โดยวิเคราะห์เครื่องมือ

ที่ใช้ในการโจมตี เราพบว่าขบวนการคุกคามในโลกไซเบอร์ยังคงอยู่ ถึงแม้ว่าจากการสืบหาต้นตอผ่านร่องรอยและรูปแบบการโจมตีด้วยมาโครอาจทำให้ดูเหมือนพวกเขายังขาดประสบการณ์อยู่บ้าง อย่างไรก็ตาม กลุ่ม Rocket Kitten กำลังพัฒนาตัวอย่างช้าๆ และได้รับความสนใจเพิ่มขึ้นเรื่อยๆ

เราสามารถยืนยันได้ว่า Wool3n.H4T ไม่เพียงแพร่กระจายไวรัสผ่านการเปิดใช้งานเอกสาร Microsoft Office ต่างๆ เท่านั้น แต่ยังมีความสามารถในการพัฒนามัลแวร์ได้อีกด้วย

จากหลักฐานทั้งหมด การโจมตีของ Rocket Kitten ชัดเจนแล้วว่ามีปัญหาทางการเมืองเป็นแรงจูงใจโดยการพุ่งเป้าการโจมตีอิหร่าน ในขณะที่แรงจูงใจที่อยู่เบื้องหลังการกำหนดเป้าหมายการโจมตีนี้ ถึงแม้เบื้องหลังของการโจมตีจะแตกต่างกัน ผลลัพธ์ในท้ายที่สุดกลับไม่แตกต่างกันคือการเปลี่ยนแปลงขั้วอำนาจ ไม่ทางเศรษฐกิจก็ทางการเมือง

สามารถอ่านรายงานการวิจัยเรื่องการโจมตีของ Woolen-GoldFish ฉบับเต็มได่ที่ : When Kittens Go Phishing for a full, detailed look into the activities and methods of Rocket Kitten. (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-woolen-goldfish.pdf)

##########################

ติดต่อข้อมูลประชาสัมพันธ์

จารุวรรณ ฤกษ์พิชญโยธิน

บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด

+662 646 1968,
jaruwan_r@trendmicro.com

วราวอง จงรักษ์

ดุษฎี เย็นสุดใจ

บริษัท เอฟเอคิว จำกัด: +662 971 3700

Trendmicrothpr@faq.co.th