วันที่ 9 กันยายน 2568

แคมเปญ “Noisy Bear” ที่เล็งเป้าภาคพลังงานคาซัคสถาน ถูกเปิดเผยว่าเป็นการทดสอบฟิชชิง

มีการเปิดเผยจากนักวิจัยว่า ผู้ไม่หวังดีซึ่งอาจมีต้นกำเนิดจากรัสเซีย ได้ถูกเชื่อมโยงกับชุดการโจมตีใหม่ที่มุ่งเป้าไปยังภาคพลังงานในคาซัคสถาน

กิจกรรมนี้มีรหัสว่า Operation BarrelFire และเกี่ยวข้องกับกลุ่มผู้ไม่หวังดีใหม่ที่ Seqrite Labs ติดตามในชื่อ Noisy Bear ซึ่งกลุ่มนี้เริ่มเคลื่อนไหวอย่างน้อยตั้งแต่เดือนเมษายน 2025 โดยการโจมตีในครั้งนี้มุ่งเป้าไปที่พนักงานของ KazMunaiGas (KMG) ซึ่งเป็นบริษัทน้ำมันและก๊าซแห่งชาติของคาซัคสถาน โดยผู้ไม่หวังดีส่งเอกสารปลอมที่เกี่ยวข้องกับฝ่าย IT ของ KMG เลียนแบบการสื่อสารภายในบริษัทจริงๆ และใช้หัวข้อเกี่ยวกับอัปเดตนโยบาย, กระบวนการรับรองภายใน และการปรับเงินเดือน

ลำดับการโจมตี

ลำดับการติดเชื้อเริ่มจากอีเมลฟิชชิง ที่มีไฟล์ ZIP แนบมาด้วย ซึ่งภายในประกอบด้วย:

- ตัวดาวน์โหลด Windows shortcut (LNK)
- เอกสารล่อหลอกที่เกี่ยวกับ KazMunaiGas
- ไฟล์ README.txt ที่มีคำแนะนำเป็นภาษารัสเซียและคาซัค ให้เรียกใช้โปรแกรมชื่อ “KazMunayGaz_Viewer”

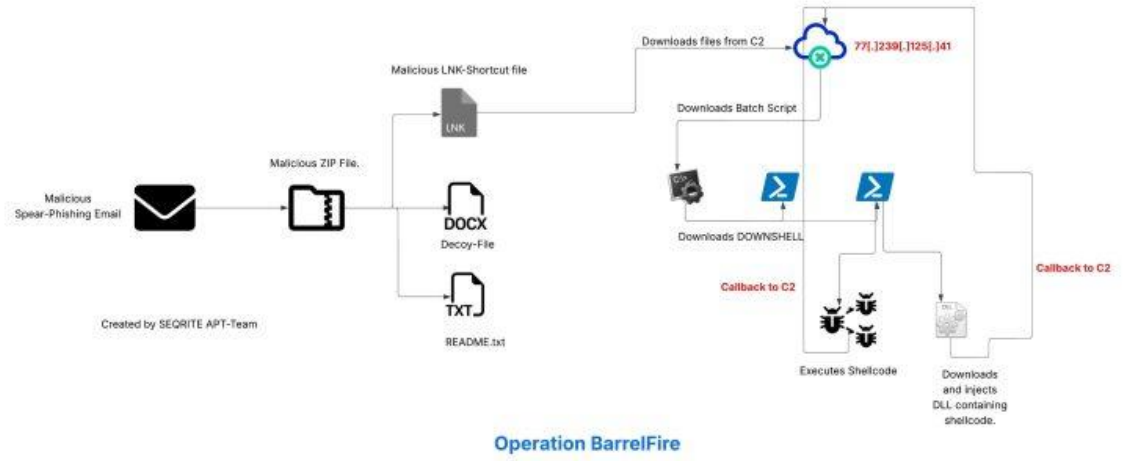
อีเมลดังกล่าวถูกส่งจากอีเมลที่ถูกเจาะของพนักงานฝ่ายการเงินของ KazMunaiGas และมุ่งเป้าไปยังพนักงานคนอื่นในเดือนพฤษภาคม 2025

ไฟล์ LNK นี้ถูกออกแบบมาเพื่อติดตั้ง payload เพิ่มเติม รวมถึง สคริปต์ batch ที่เป็นอันตราย ซึ่งจะทำหน้าที่โหลด PowerShell loader ชื่อ DOWNSHELL การโจมตีจะสิ้นสุดด้วยการติดตั้ง DLL-based implant ซึ่งเป็นไฟล์ 64-bit ที่สามารถรัน shellcode เพื่อสร้าง reverse shell

นอกจากนี้ การวิเคราะห์โครงสร้างพื้นฐานของผู้ไม่หวังดียังพบว่าถูกโฮสต์บนบริการโฮสติ้ง BPH ของรัสเซียชื่อ Aeza Group ซึ่งถูกสหรัฐอเมริกาคว่ำบาตรในเดือนกรกฎาคม 2025 เนื่องจากสนับสนุนกิจกรรมที่เป็นอันตราย

การโจมตีอื่นๆ ในยุโรปตะวันออก

HarfangLab ระบุว่า กลุ่มผู้ไม่หวังดีที่มีความเกี่ยวข้องกับเบลารุสชื่อ Ghostwriter ที่รู้จักในชื่อ FrostyNeighbor หรือ UNC1151 มีแคมเปญโจมตียูเครนและโปแลนด์ตั้งแต่เดือนเมษายน 2025 โดยใช้ไฟล์ ZIP และ RAR ที่มีเป้าหมายเพื่อรวบรวมข้อมูลและติดตั้ง implant



- ไฟล์เหล่านี้มักมี สเปรดชีต XLS ที่ฝัง VBA macro เพื่อโหลด DLL
- DLL จะเก็บข้อมูลระบบที่ถูกเจาะและดาวน์โหลดมัลแวร์ขั้นต่อไปจาก C2 server

บางครั้ง DLL จะถูกบรรจุในไฟล์ CAB พร้อมกับ LNK shortcut เพื่อสกัดและรัน DLL ซึ่งหลังจากนั้นจะเริ่มทำ reconnaissance และดาวน์โหลดมัลแวร์ขั้นต่อไป สำหรับโปแลนด์ แคมเปญปรับการโจมตีเล็กน้อย โดยใช้ Slack เป็นช่องทางสื่อสารและขโมยข้อมูล พร้อมดาวน์โหลด payload ขั้นสองที่ติดต่อโดเมน pesthacks[.]icu ในบางกรณี DLL ที่ถูกโหลดจาก Excel macro ถูกใช้เพื่อรัน Cobalt Strike Beacon เพื่อให้สามารถทำ post-exploitation ต่อได้

HarfangLab ระบุว่า “การเปลี่ยนแปลงเล็กน้อยเหล่านี้แสดงให้เห็นว่า UAC-0057 อาจกำลังสำรวจวิธีอื่นเพื่อหลีกเลี่ยงการตรวจจับ แต่ยังให้ความสำคัญกับการดำเนินงานต่อเนื่องมากกว่าการซ่อนตัวหรือความซับซ้อน”

รายงานการโจมตีต่อรัสเซีย

ในช่วงครึ่งแรกของปี 2025 กลุ่ม OldGremlin ได้โจมตีบริษัทรัสเซียหลายแห่ง โดยใช้ฟิชชิงและเทคนิค BYOVD (Bring Your Own Vulnerable Driver) เพื่อปิดระบบความปลอดภัยบนเครื่องเหยื่อ

การโจมตีแบบฟิชชิงที่มุ่งเป้ารัสเซียยังพบมัลแวร์ใหม่ชื่อ Phantom Stealer ซึ่งพัฒนาจาก Stealerium ใช้รวบรวมข้อมูลหลากหลายผ่านอีเมลล่อด้วยเนื้อหาผู้ใหญ่หรือการชำระเงิน

- Phantom Stealer มีโมดูล PornDetector ที่ถ่ายภาพจากกล้องเว็บแคมเมื่อผู้ใช้เข้าชมเว็บไซต์ลามก
- ข้อมูลนี้มักใช้สำหรับ sextortion

นอกจากนี้ยังมีการโจมตีโดยกลุ่ม Cloud Atlas, PhantomCore, และ Scaly Wolf เพื่อขโมยข้อมูลและส่ง payload เพิ่มเติม เช่น VBShower, PhantomRAT, PhantomRShell

กลุ่มผู้ไม่หวังดีบางกลุ่มพัฒนา มัลแวร์ Android ปลอมเป็นแอป FSB เพื่อโจมตีผู้แทนธุรกิจรัสเซีย เช่น แอปชื่อ SECURITY_FSB, **ФСБ**, GuardCB

- มัลแวร์สามารถขโมยข้อมูลจากแอปแชทและเบราว์เซอร์, สตรีมกล้อง, และบันทึกคีย์สโตร์
- ต้องการสิทธิ์ SMS, พิกัด, เสียง, กล้อง, และสิทธิ์ผู้ดูแลระบบ
- มีฟีเจอร์ป้องกันการลบโดยใช้ Accessibility Services

Doctor Web ระบุว่า “อินเทอร์เฟซของแอปมีแค่ภาษารัสเซีย ทำให้มุ่งเป้าเฉพาะผู้ใช้รัสเซียเท่านั้น”

อัปเดตสำคัญ

บริษัทน้ำมันและก๊าซรัฐของคาซัคสถาน KazMunayGas ได้ ปฏิเสธ รายงานของ Seqrite ว่ามีกลุ่มสอดแนมไซเบอร์ใหม่โจมตีพนักงานของบริษัท โดยระบุว่า ภาพหน้าจอที่กล่าวถึงในรายงานเป็นส่วนหนึ่งของการ ทดสอบฟิชชิงภายใน ที่บริษัทดำเนินการในเดือนพฤษภาคม 2025 (เนื้อหาถูกปรับปรุงหลังการเผยแพร่เพื่อตามรายงานสื่อท้องถิ่นของคาซัคสถาน และหัวข้อข่าวจึงถูกแก้ไขให้สะท้อนว่ามันเป็นการทดสอบฟิชชิง)

ข้อมูลอ้างอิง

Sep 6, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/noisy-bear-targets-kazakhstan-energy.html