แจ้งเตือน : การโจมตี Ransomware จากกลุ่ม BlackCat

ผลกระทบทางธุรกิจ
- ☒ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☒ Privacy violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : WHITE

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ข่าวการแจ้งเตือนการโจมตีของกลุ่ม Ransomware BlackCat/ALPHV

วันที่แจ้งเตือน 27 เมษายน 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับพฤติกรรมการโจมตีของกลุ่มผู้ไม่หวังดี BlackCat/ALPHV ที่มีการโจมตีแบบ Ransomware-as-a-Service (RaaS) และเรียกค่าไถ่แบบสองชั้น (Double Extortion)[1] โดยมีลักษณะการโจมตีด้วยเทคนิคและวิธีการต่างๆ เช่น

1. การโจมตีช่องโหว่ระบบโครงสร้างด้านเทคโนโลยีสารสนเทศเช่น เครื่องแม่ข่ายที่ใช้การส่งจดหมายอิเล็กทรอนิกส์ (Microsoft Exchange Server) และอุปกรณ์รักษาความปลอดภัย (Firewall)
2. การใช้โปรแกรมที่ไม่หวังดี (Malware) และโปรแกรมประเภท Backdoor
3. การโจมตีผู้ใช้งานโดยตรงเพื่อเข้าถึงเครือข่ายภายใน จากนั้นยกระดับสิทธิเพื่อติดตั้ง Ransomware ตลอดจนเครื่องมือควบคุมสั่งการระบบเป้าหมายและเครื่องมือโจรกรรมและถ่ายโอนข้อมูลออก

ทั้งนี้ มีรายงานจากสำนักงานสอบสวนกลางของสหรัฐ (Federal Bureau of Investigation: FBI) พบว่ากลุ่ม Blackcat ได้โจมตีบริษัทกว่า 60 แห่งทั่วโลก ตั้งแต่เดือนพฤศจิกายน 2564 จนถึงเดือนมีนาคม 2565 รวมถึงมีรายงานจาก Threat Intelligence ถึงความเชื่อมโยงระหว่างกลุ่ม BlackCat/ALPHV และกลุ่ม BlackMatter

<u>เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้</u>

1. จัดให้มีกระบวนการตรวจสอบบัญชีผู้ใช้งานในระบบที่ถูกสร้างขึ้นใหม่และบัญชีที่ไม่ทราบที่มา (Unrecognized Account) บนเครื่อง Domain Controller เครื่อง Active Directory เครื่องแม่ข่าย และเครื่องลูกข่ายอย่างต่อเนื่อง
2. สำรองข้อมูลให้มีความพร้อมใช้อย่างสม่ำเสมอเพื่อให้มั่นใจว่าข้อมูลสำรองของระบบสำคัญจะสามารถใช้งานได้เมื่อเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ
3. สอบทานโปรแกรม Windows Task Scheduler อย่างสม่ำเสมอ เพื่อค้นหาตารางงานและ Application ที่น่าสงสัยที่ถูกติดตั้งและประมวลผลโดยอัตโนมัติอยู่บนเครื่องภายในองค์กร
4. สอบทานบัญชีสิทธิสูงอย่างสม่ำเสมอ รวมถึงตั้งค่าการเข้าถึงระบบงานและเครือข่ายภายในองค์กรตามหลักการ Least Privilege
5. แบ่งแยกเครือข่ายด้านเทคโนโลยีสารสนเทศ (Network Segmentation) ภายในองค์กรอย่างปลอดภัยเพียงพอเพื่อป้องกันการโจมตีจากภายนอก

[1] วิธีการนำข้อมูลออกจากระบบและเข้ารหัสข้อมูลเพื่อสร้างเงื่อนไขในการเรียกค่าไถ่เพื่อกู้คืนข้อมูลในครั้งแรก หลังจากนั้นจะนำข้อมูลดังกล่าวมาสร้างเงื่อนไขข่มขู่ครั้งที่สองในการเผยแพร่ข้อมูลสู่สาธารณะ

ข่าวการแจ้งเตือนการโจมตีของกลุ่ม Ransomware BlackCat/ALPHV

วันที่แจ้งเตือน 27 เมษายน 2565

6. กำหนดและควบคุมสิทธิการติดตั้งโปรแกรมบนเครื่องแม่ข่าย และเครื่องลูกข่ายให้แก่ผู้ที่มีสิทธิที่ได้รับอนุญาตเท่านั้น
7. ตรวจสอบและดำเนินการอัปเดต Security Patch ของระบบงานต่าง ๆ และโปรแกรม Antivirus /Antimalware อย่างสม่ำเสมอ
8. ปิดการใช้งานโปรโตคอลหรือบริการสำหรับการเชื่อมต่อจากระยะไกลหากไม่มีความจำเป็นต้องใช้งาน ในกรณีที่มีความจำเป็นต้องใช้ควรใช้ช่องทางที่มีความมั่นคงปลอดภัยเพียงพอในการเข้าถึงเช่น เครือข่าย Virtual Private Network (VPN)
9. ตั้งค่าการตรวจจับและป้องกันการโจมตีในช่องทางต่างๆที่มีการรายงานในรายการ Indicator of Compromise (IOC) ได้แก่ IP Address และเครื่องมือโจมตีระบบที่เกี่ยวข้อง จากข้อมูล Threat Intelligence ใน link ที่อ้างอิง
10. ผู้ดูแลระบบควรประเมินความเสี่ยงจากการดำเนินการดังกล่าวก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

ข้อมูลอ้างอิง *External Link*

1. https://www.ic3.gov/Media/News/2022/220420.pdf (IOC File)
2. https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
3. https://www.kaspersky.com/blog/black-cat-ransomware/44120/
4. https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html
5. https://thehackernews.com/2022/04/fbi-warns-of-blackcat-ransomware-that.html
6. https://securityaffairs.co/wordpress/130582/reports/fbi-blackcat-ransomware.html