แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

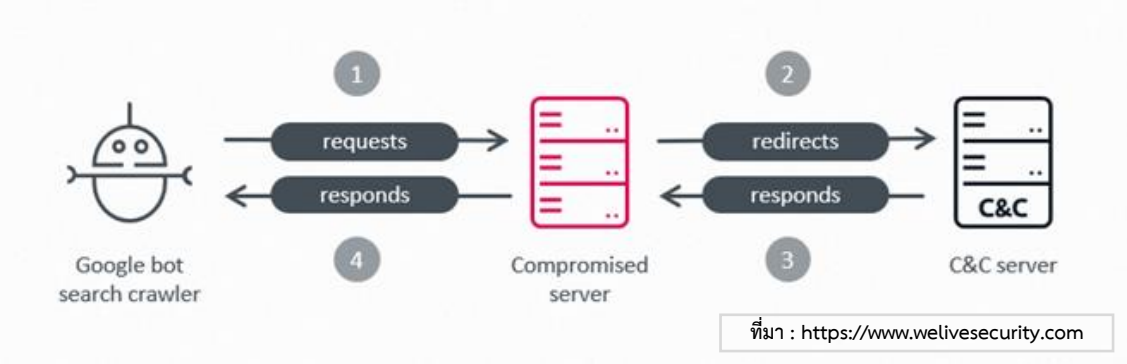
# แจ้งเตือน การโจมตีจากกลุ่ม GhostRedirector

วันที่แจ้งเตือน 11 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีกลุ่มผู้โจมตี GhostRedirector มีพฤติกรรมมุ่งเป้าโจมตีระบบปฏิบัติการ Microsoft Windows Server ที่เปิดให้บริการเว็บ (IIS) โดยปัจจุบันตรวจพบการถูกโจมตีในหลายประเทศ เช่น บราซิล เวียดนาม และไทย เป็นต้น มีวัตถุประสงค์หลักในการให้บริการที่เรียกว่า SEO fraud-as-a-service ซึ่งเป็นบริการการเพิ่มอันดับการค้นหาบน Google โดยมิชอบผ่านวิธีการที่เรียกว่า SEO Poisoning ก่อให้เกิดความเสี่ยงโดยตรงต่อความน่าเชื่อถือและชื่อเสียงขององค์กร อีกทั้งยังทำให้เว็บไซต์ที่ถูกโจมตีถูกมองว่าเป็นแหล่งเผยแพร่มัลแวร์อีกด้วย โดยมีรายละเอียดดังนี้

กลุ่ม GhostRedirector อาศัยการฝังมัลแวร์เข้าสู่ระบบ โดยมัลแวร์จะปรับแต่งการตอบสนองของเซิร์ฟเวอร์ของเหยื่อ โดยเมื่อ Google Bot เข้ามาอ่านข้อมูลเว็บไซต์แล้ว จะส่งข้อมูลที่ดึงมาจากเครื่องของผู้ไม่หวังดี (C&C server) เพื่อให้เว็บไซต์ที่ตนต้องการโปรโมตมีอันดับการค้นหาสูงขึ้น ซึ่งอาจทำให้เกิดการเข้าใจที่คลาดเคลื่อน




ที่มา : https://www.welivesecurity.com

**แนวทางการป้องกันและลดผลกระทบ**

- อัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุด
- ตรวจสอบการตั้งค่า IIS ระบบฐานข้อมูลเพื่อป้องกันการโจมตี SQL Injection
- เฝ้าระวังการใช้งานที่มีพฤติกรรมที่ผิดปกติ รวมถึงสแกนหาสคริปต์หรือโมดูลแปลกปลอม (สามารถค้นหา IoCs ที่เกี่ยวข้องได้ตาม **อ้างอิง 2**)
- เสริมมาตรการควบคุมสิทธิ์การใช้งานระบบ และใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)
- สนับสนุนให้มีการประเมินและทดสอบความมั่นคงปลอดภัยของระบบอย่างต่อเนื่อง

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

**ข้อมูลอ้างอิง**


1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 10 ก.ย. 2568
2) https://www.welivesecurity.com/en/eset-research/ghostredirector-poisons-windows-servers-backdoors-side-potatoes/?ref=metacurity.com
3) https://thehackernews.com/2025/09/ghostredirector-hacks-65-windows.html