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 Botnet ขนาดใหญ่โจมตี Microsoft 365 โดยวิธี Password Spraying ผ่านช่องโหว่ Basic Authentication

วันที่แจ้งเตือน 26 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามเกี่ยวกับการโจมตีทางไซเบอร์ พบการรายงานกรณีนักวิจัยด้านความมั่นคงปลอดภัยจาก SecurityScorecard พบ Botnet กว่า 130,000 เครื่องโจมตี Microsoft 365 ด้วยเทคนิค Password Spraying ผ่านช่องโหว่ Basic Authentication ซึ่งเป็นการยืนยันตัวตนแบบเก่าที่ให้เข้าใช้งานระบบโดยพิมพ์รหัสผ่านเข้าสู่ระบบโดยตรง (Non-Interactive) และอาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต แพร่กระจายมัลแวร์ และอาจทำให้ระบบหยุดชะงัก

เพื่อป้องกันความเสี่ยงเหล่านี้ องค์กรควรพิจารณาดำเนินการโดยประยุกต์ใช้การยืนยันตัวตนแบบ Modern Authentication (OAuth 2.0) เช่น Multi-Factor Authentication เป็นต้น และหมั่นตรวจสอบการลงชื่อเข้าใช้งานระบบเพื่อตรวจจับ Password Spraying และตรวจสอบการทำงานของระบบ Conditional Access Policies เพื่อให้มีประสิทธิภาพอยู่เสมอ ซึ่งจะช่วยเสริมสร้างความปลอดภัยให้กับระบบขององค์กรได้อย่างมีประสิทธิภาพ รวมทั้งติดตามข่าวสารจากเจ้าของผลิตภัณฑ์กรณีที่อาจมีการประกาศยกเลิกการใช้งานบาง Feature และเพิ่มมาตรการควบคุมที่เหมาะสม เพื่อลดโอกาสที่ผู้ไม่หวังดีอาจใช้เป็นช่องโหว่เพื่อการโจมตีได้

ข้อมูล Command and Control (C2) Servers IP Address และ Ports ที่ตรวจพบในรายงาน ได้แก่

70.39.115.74
70.39.120.10
204.188.218.178
204.188.218.179
204.188.210.226
204.188.210.227

Port	Service	Potential Usage
1002	Unassigned (Often RPC related)	Unknown
2181	Zookeeper	Likely managing a Kafka distributed botnet setup
3306	MySQL	Could store stolen data or botnet configuration
6379	Redis	Potential key-value store for botnet related tasking
7779	Unknown	Unknown
8081	Jetty web service	Zookeeper query service
10050	Zabbix Agent	Potential botnet monitoring
33060	MySQL X Protocol	Likely used with MySQL service

Port	Possible Use
12341	Likely Botnet C2 channel (Client Registration)
12342	Possibly used for tasking infected hosts
12347	Possible data exfil or backup C2
12348	High probability of main C2 command execution

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/botnet-targets-basic-auth-in-microsoft-365-password-spray-attacks/
2. https://securityaffairs.com/174595/cyber-crime/large-botnet-targets-m365-password-spraying-attacks.html