แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

กลุ่ม APT ขยายเป้าหมายการโจมตี และ อัปเดตเครื่องมือที่เป็นอันตราย

วันที่แจ้งเตือน 20 พฤษภาคม 2569

ThaiCERT สกมช. ได้ติดตามข่าวสาร พบรายงานของ Bitdefender ตรวจพบกลุ่ม APT ได้ขยายขอบเขตการโจมตีไปยังหน่วยงานในภาคพลังงาน โทรคมนาคม การเงิน และหน่วยงานของรัฐ พร้อมทั้งมีการปรับปรุงเครื่องมือ Backdoor และ Remote Access Trojan (RAT) เพื่อเพิ่มความสามารถในการหลบเลี่ยงการตรวจจับและรักษาการเข้าถึงระบบ โดยมีรายละเอียด ดังนี้

กลุ่มผู้ไม่หวังดี	รายละเอียด	ผลกระทบ
Salt Typhoon (Earth Estries, FamousSparrow, GhostEmperor และ UNC2286)	ผู้ไม่หวังดีอาศัยช่องโหว่ของ Microsoft Exchange Server ติดตั้ง Web Shell เพื่อสร้างช่องทางเข้าระบบ และใช้เทคนิค DLL Sideloading เพื่อติดตั้งมัลแวร์ Deed RAT รวมถึง Backdoor ชนิด TernDoor เพื่อคงสิทธิการเข้าถึงระบบ นอกจากนี้ยังพบการใช้เครื่องมือ Impacket, Remote DesktopProtocol (RDP) และการปลอมชื่อ Service ให้คล้ายกับซอฟต์แวร์เชิงพาณิชย์ เช่น LogMeln Hamachi เป็นต้น เพื่อหลบเลี่ยงการตรวจสอบจากผู้ดูแลระบบ	พบการโจมตีไปยังบริษัทด้านน้ำมันและก๊าซ ในประเทศอาเซอร์ไบจาน จากเป้าหมายเดิมที่มุ่งโจมตีหน่วยงานของรัฐ โทรคมนาคม และเทคโนโลยีในสหรัฐฯ เอเชีย ตะวันออกกลาง และแอฟริกา
Twill Typhoon (Mustang Panda)	ผู้ไม่หวังดีพัฒนา RAT Framework แบบ Modular ที่พัฒนาด้วย .NET Framework ที่ชื่อ FDMTP และใช้เทคนิค DLL Sideloading ร่วมกับ Binary ที่ถูกต้องตามกฎหมาย รวมถึงปลอมโดเมนให้คล้ายบริการ Content Delivery Network (CDN) และบริการของบริษัทชื่อดัง เช่น Yahoo และ Apple เป็นต้น เพื่อหลอกให้ระบบรักษาความปลอดภัยเชื่อถือทราฟฟิกที่เกิดขึ้น มัลแวร์ดังกล่าวสามารถโหลด Plugin เพิ่มเติมได้ ทำให้ผู้ไม่หวังดีสามารถควบคุมระบบ รันคำสั่งบนเครื่อง ขโมยข้อมูล ดาวน์โหลด Payload และสร้าง Persistence ภายในระบบ และยังอาศัย Windows ClickOnce และ Visual Studio Hosting เพื่อช่วยให้มัลแวร์หลบเลี่ยงการตรวจจับจากระบบ	มุ่งเป้าโจมตีหน่วยงานในภูมิภาคเอเชียแปซิฟิก และ ญี่ปุ่น

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 19 พ.ค. 2569
2. https://businessinsights.bitdefender.com/famoussparrow-apt-targets-azerbaijani-oil-gas-industry?
3. https://www.securityweek.com/chinese-apts-expand-targets-update-backdoors-in-recent-campaigns/?

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ