วันที่ 17 กันยายน 2568

## Mustang Panda ใช้ Worm บน USB ชื่อ SnakeDisk เพื่อฝังแบ็กดอร์ Yokai ลงบนไอพีในประเทศไทย

นักวิจัยด้านความปลอดภัยจาก IBM X-Force ได้เปิดเผยว่า กลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐบาลจีนในชื่อ Mustang Panda (หรือที่รู้จักในชื่อ Hive0154, Earth Preta, Twill Typhoon) กำลังปฏิบัติการโจมตีอย่างต่อเนื่อง โดยใช้เครื่องมือที่ได้รับการอัปเดตใหม่ล่าสุด ซึ่งมีเป้าหมายที่ประเทศไทยโดยเฉพาะ

**การโจมตี Operation BarrelFire และมัลแวร์ใหม่**

รายงานระบุว่า Mustang Panda ได้พัฒนาเครื่องมือโจมตีสองตัวหลัก:

TONESHELL: แบ็กดอร์ตัวใหม่ที่ปรับปรุงความสามารถให้สามารถสื่อสารกับเซิร์ฟเวอร์ควบคุม (C2) ผ่านพร็อกซีเซิร์ฟเวอร์ เพื่อให้ดูเหมือนเป็นทราฟฟิกปกติภายในองค์กร นอกจากนี้ยังสามารถเปิดช่องทางลับ (reverse shell) ได้พร้อมกันถึงสองช่องทาง TONESHELL เวอร์ชันล่าสุด (TONESHELL8 และ TONESHELL9) ยังมีการฝังโค้ดที่คัดลอกมาจากหน้าเว็บ OpenAI ChatGPT เพื่อหลีกเลี่ยงการตรวจจับจากโปรแกรมสแกนแบบทั่วไป

SnakeDisk: เวิร์มบน USB ที่ไม่เคยถูกรายงานมาก่อน ซึ่งมีความสามารถในการแพร่กระจายตัวเองผ่านอุปกรณ์พกพา และจะทำงานก็ต่อเมื่อตรวจพบว่า IP สาธารณะของเครื่องเป้าหมายนั้นอยู่ในประเทศไทยเท่านั้น หลังจากนั้นจะปล่อยแบ็กดอร์ชื่อ Yokai ลงสู่เครื่องของเหยื่อ

**ลำดับการโจมตีและกลไกการทำงาน**

การโจมตีมักเริ่มต้นด้วยอีเมลหลอกล่อแบบ spear-phishing เพื่อให้เหยื่อเปิดมัลแวร์อย่าง PUBLOAD หรือ TONESHELL หลังจากนั้น มัลแวร์จะใช้เทคนิค DLL side-loading เพื่อรันตัวเองและดาวน์โหลดเพลย์โหลดเพิ่มเติม

เมื่อ SnakeDisk แพร่กระจายผ่าน USB มันจะย้ายไฟล์เดิมบน USB ไปไว้ในโฟลเดอร์ย่อย แล้วสร้างไฟล์ปฏิบัติการปลอมชื่อ “USB.exe” หรือชื่อที่คล้ายกับโวลุ่มเดิมของ USB เพื่อหลอกให้เหยื่อคลิกเปิด เมื่อมัลแวร์ทำงาน จะทำการคัดลอกไฟล์เดิมกลับมาและติดตั้ง Yokai ซึ่งเป็นแบ็กดอร์ที่ช่วยให้ผู้โจมตีสามารถสั่งรันคำสั่งใดๆ บนเครื่องได้จากระยะไกล

**ข้อสรุปและแนวโน้มการโจมตี**

การใช้ SnakeDisk ร่วมกับ Yokai แสดงให้เห็นว่ามีกลุ่มย่อยภายใน Mustang Panda ที่มุ่งเน้นเป้าหมายที่ประเทศไทยโดยเฉพาะ และสะท้อนให้เห็นถึงการพัฒนาชุดเครื่องมืออย่างต่อเนื่อง

นักวิจัยจาก IBM X-Force สรุปว่า Mustang Panda ยังคงเป็นกลุ่มที่มีความสามารถสูงและมีการพัฒนาอย่างรวดเร็ว โดยดูแลระบบนิเวศของมัลแวร์ขนาดใหญ่ ซึ่งมีความเชื่อมโยงกันทั้งในด้านโค้ด, เทคนิคการโจมตี, และเป้าหมายที่เลือก

**ข้อมูลอ้างอิง**

**Sep 15, 2025, By Ravie Lakshmanan**

- https://thehackernews.com/2025/09/mustang-panda-deploys-snakedisk-usb.html
- https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor