แฮ็กเกอร์ใช้เทคนิคเอาเมาส์วางในพาวเวอร์พอยต์เพื่อฝังมัลแวร์

กลุ่มอาชญากรไซเบอร์ชื่อดังที่เชื่อว่าทางการรัสเซียสนับสนุนอย่าง APT28 กำลังใช้เทคนิคใหม่สำหรับรันโค้ดอันตราย ด้วยการใช้การเคลื่อนเมาส์บนพาวเวอร์พอยต์เพื่อติดตั้งมัลแวร์ เมื่อผู้ใช้กดพรีเซนต์แล้วเริ่มขยับเมาส์

บริษัทด้านความปลอดภัยทางไซเบอร์ Cluster25 ออกรายงานทางเทคนิค ระบุว่า “แค่ขยับเมาส์ก็รันสคริปต์พาวเวอร์เชลล์อันตรายที่ดาวน์โหลดและรันดรอปเปอร์ใน OneDrive ต่อได้แล้ว แม้ตัวดรอปเปอร์ดูไม่มีพิษมีภัย

แต่ก็เป็นสะพานนำไปสู่การโหลดมัลแวร์ตัวจริงอย่าง Graphite ที่ใช้ Microsoft Graph API และ OneDrive สื่อสารกับเซิร์ฟเวอร์ศูนย์บัญชาการ (C&C) เพื่อโหลดข้อมูลอันตรายเพิ่มเติม เทคนิคนี้เป็นการล่อหลอกให้ผู้ใช้ใช้เท็มเพลตตัวหนึ่ง

ที่พบความเชื่อมโยงกับหน่วยงานระดับนานาชาติที่อยู่กรุงปารีสอย่าง Organisation for Economic Co-operation and Development (OECD) และพบว่าการโจมตีแบบนี้ยังคงระบาดต่อเนื่องตั้งแต่ช่วงสิงหาคมจนถึงปัจจุบัน แม้จะพบร่องรอยของการใช้เทคนิคนี้ตั้งแต่มกราคมก็ตาม

ที่มา : THN