ประจำวันอังคารที่ 23 สิงหาคม 2565

กลุ่มอาชญากรไซเบอร์ TA558 พุ่งเป้าไปยังองค์กรการบริการ โรงแรม และการท่องเที่ยว

กลุ่มแฮกเกอร์ TA558 ได้พุ่งเป้าหมายการโจมตีไปที่โรงแรมและบริษัทหลายแห่งในด้านการบริการและการท่องเที่ยว โดยผู้โจมตีได้ใช้มัลแวร์หลายตัวในการโจมตี โดยมีเป้าหมายในการติดตั้งมัลแวร์บนระบบ เพื่อเข้าถึงระบบ และทำการขโมยข้อมูลที่สำคัญและขโมยเงินออก

Proofpoint บริษัทรักษาความปลอดภัยได้ติดตามกลุ่ม TA558 มาตั้งแต่ปี 2018 ได้เรียกว่ากลุ่มนี้ว่ากลุ่มอาชญากรรมขนาดเล็ก โดยกลุ่มนี้ใช้กลยุทธ์ เทคนิค และขั้นตอนที่คล้ายเดิม คือพยายามติดตั้งมัลแวร์ต่างๆ รวมถึง Loda RAT, VjwOrm และ Revenge RAT ซึ่งมีการมุ่งเป้าหมายไปที่การใช้ภาษาโปรตุเกส สเปน และอเมริกาเป็นหลัก

แคมเปญ Phishing ของกลุ่มนี้เน้นการส่งข้อความสแปมที่เป็นอันตรายพร้อมสิ่งล่อใจในการจอง เช่น การจองโรงแรมที่มีเอกสารหรือ URL ที่ดึงดูดผู้ใช้งานเพื่อให้ติดตั้งโทรจันที่สามารถสอดแนม ขโมยข้อมูล และแจกจ่ายเพย์โหลดที่ตามมา การโจมตีได้มีการพัฒนาตลอดหลายปีที่ผ่านมา ซึ่งการโจมตีที่พบระหว่างปี 2018 และ 2021 ได้ใช้ประโยชน์จากอีเมลด้วยเอกสาร Word ที่มีมาโคร VBA หรือใช้ช่องโหว่ เช่น CVE-2017-11882 และ CVE-2017-8570 เพื่อดาวน์โหลดและติดตั้ง มัลแวร์ เช่น AsyncRAT, Loda RAT, Revenge RAT และ VjwOrm

นักวิจัยกล่าวว่ามัลแวร์ที่ใช้โดยกลุ่ม TA558 นั้นสามารถขโมยข้อมูลผู้ใช้งานของลูกค้าโรงแรมและข้อมูลบัตรเครดิตตลอดจนความสูญเสียทางการเงินที่อาจเกิดขึ้นได้

ที่มาของข่าว : https://thehackernews.com/2022/08/cybercrime-group-ta558-targeting.html