แคสเปอร์สกี้ แลป เปิดเผยภัยคุกคามหน่วยงานรัฐ “Muddy Water” โจมตีเอเชีย ยุโรป และแอฟริกา

กลุ่มผู้ร้ายคุกคามทางไซเบอร์ขั้นสูงที่ชื่อ มัดดี้วอเทอร์ (Muddy Water) ที่ตรวจพบครั้งแรกในการโจมตีอิรักและซาอุดิอาระเบียเมื่อปี 2017 แต่เมื่อต้นปี 2018 นี้ นักวิจัยของแคสเปอร์สกี้ แลป ตรวจสอบกิจกรรมของมัดดี้วอเทอร์และพบปฏิบัติการขนาดใหญ่ที่มีเป้าหมายเพิ่มเป็นหน่วยงานรัฐบาลในประเทศจอร์แดน ตุรกี อาเซอร์ไบจัน ปากีสถาน อาฟกานิสถาน มาลี ออสเตรีย รัสเซีย อิหร่าน และบาห์เรน มัลแวร์ที่ใช้แพร่กระจายผ่านการสเปียร์ฟิชชิ่งที่ไฟล์เอกสารสำนักงาน จากนั้นแจ้งให้ผู้ใช้เปิดใช้งานมาโคร ขณะนี้การโจมตียังปฏิบัติการอยู่

จากการตรวจสอบเนื้อหาของข้อความสเปียร์ฟิชชิ่ง พบว่าเป้าหมายคือหน่วยงานรัฐ หน่วยงานทางทหาร บริษัทโทรคมนาคม และสถาบันการศึกษา ในอีเมลจะแนบไฟล์ MS Office เวอร์ชั่น 97-2003 และจะเริ่มแพร่กระจายทันทีเมื่อผู้ใช้เปิดใช้งานมาโคร

ขณะนี้ ยังไม่ทราบว่า ใครอยู่เบื้องหลังปฏิบัติการมัดดี้วอเทอร์ แต่แน่ชัดว่ามีแรงจูงใจด้านภูมิศาสตร์การเมือง โค้ดที่ใช้ในการโจมตีล่าสุดออกแบบหลอกล่อให้การสืบสวนไขว้เขว เช่น การใส่ภาษาจีนในโค้ด และใช้ชื่ออย่าง ลีโอ พูพัค เว็นเด็ตต้า และเติร์ก ในมัลแวร์อีกด้วย

อามิน ฮาสบินี นักวิจัยอาวุโสด้านความปลอดภัย ทีม GReAT แคสเปอร์สกี้ แลป กล่าวว่า “ในปีที่แล้ว เราเห็นกลุ่มมัดดี้วอเทอร์ดำเนินการโจมตีจำนวนมาก และพัฒนาวิธีการและเทคนิคใหม่ๆ อย่างต่อเนื่อง กลุ่มนี้มีทีมที่คอยปรับปรุงทูลคิทเพื่อลดการถูกตรวจจับโดยผลิตภัณฑ์เพื่อความปลอดภัยต่างๆ ทำให้เชื่อว่าการโจมตีจะแข็งแกร่งยิ่งขึ้น แคสเปอร์สกี้ แลป จึงประกาศการค้นพบนี้ให้ทราบในวงกว้าง เพื่อให้องค์กรต่างๆ ได้ระมัดระวังป้องกันองค์กรของตน ปัจจุบัน เรายังทำการวิเคราะห์การดำเนินการและจับตามองปฏิบัติการเพื่อมองหาความผิดพลาดของกลุ่มนี้ ”

แคสเปอร์สกี้ แลป ขอแนะนำให้องค์กรลดความเสี่ยงจากการตกเป็นเหยื่อภัยโจมตีทางไซเบอร์ อย่างมัดดี้วอเทอร์ ดังนี้

• ดำเนินขั้นตอนความปลอดภัยเต็มรูปแบบ ได้แก่ การตรวจจับ การป้องกัน และการสืบสวนการโจมตีแบบกำหนดเป้าหมาย รวมถึงการฝึกอบรมและการใช้งานโซลูชั่นเพื่อความปลอดภัยสำหรับการโจมตีประเภทนี้

• ให้เจ้าหน้าที่ด้านความปลอดภัยเข้าถึงข้อมูล Threat Intelligence อย่างตัวบ่งชี้ช่องโหว่ (Indicators of Compromise) และ YARA rules ซึ่งจะช่วยสนับสนุนเรื่องทูลในการป้องกันการโจมตีแบบกำหนดเป้าหมายและการ

ค้นหาต่างๆ

- ติดตั้งขั้นตอนการจัดการแพทช์ระดับเอ็นเทอร์ไพรซ์
- ตรวจสอบการตั้งค่าและการทำงานต่างๆ อย่างน้อยสองครั้ง
- ให้ความรู้เจ้าหน้าที่ในการสังเกตอีเมลที่น่าสงสัยและวิธีการจัดการ

ข้อมูลเพิ่มเติมของปฏิบัติการมัดดี้วอเทอร์ https://securelist.com/muddywater/88059