แคสเปอร์สกี้ แลป สุดปลื้ม หลังผู้นำกลุ่มโจรไซเบอร์ด้านการเงิน “Carbanak” ถูกจับ

เร็วๆ นี้ หน่วยงานบังคับใช้กฎหมายได้ร่วมมือกันจนสามารถจับกุมหัวหน้ากลุ่ม Carbanak ซึ่งใช้มัลแวร์ถอนเงินออกจากตู้เอทีเอ็ม ทำให้เกิดความเสียหายหลายพันล้านมาแล้วทั่วโลก

“ความสำเร็จล่าสุดในการต่อสู้กับกลุ่มอาชญากรไซเบอร์ Carbanak นับเป็นข่าวที่ดีมากของวงการ และชี้ให้เห็นว่าการแลกเปลี่ยนข้อมูลระหว่างประเทศเป็นเรื่องสำคัญมากที่จะช่วยให้ต่อกรกับภัยไซเบอร์ได้” เซอร์เจย์ โกโลวานอฟ นักวิจัยด้านความปลอดภัย ทีมวิเคราะห์และวิจัย แคสเปอร์สกี้ แลป กล่าว

Carbanak เป็นภัยคุกคามที่โจมตีแบบ APT (Advanced Persistent Threat) ใช้ทูลเล็งเป้าโจมตีเหยื่อที่เป็นสถาบันการเงินทั่วโลกโดยเฉพาะ โดยมีจุดประสงค์เพื่อการขโมยเงิน

Carbanak ถูกเปิดโปงขึ้นในปี 2015 โดยแคสเปอร์สกี้ แลป ร่วมกับตำรวจสากล (INTERPOL) ตำรวจยุโรป (Europol) และหน่วยงานบังคับกฎหมายอื่นๆ ที่สืบสวนเหตุการณ์ในปี 2013 ร่วมกัน ในครั้งนั้น กลุ่มอาชญากรไซเบอร์ใช้ทูลหลายอย่าง รวมถึงโปรแกรมที่ชื่อ Carbanak ในปี 2015 หลังจากที่แคสเปอร์สกี้ แลป ประกาศเรื่องการค้นพบนี้ กลุ่มอาชญากรไซเบอร์ก็ได้ปรับเปลี่ยนทูลและใช้มัลแวร์ Cobalt-strike รวมถึงเปลี่ยนชื่อเซิร์ฟเวอร์และปรับปรุงโครงสร้างไอทีอีกด้วย

กลุ่มนี้ใช้เทคนิคโซเชียลเอ็นจิเนียริ่ง เช่น การส่งอีเมลฟิชชิ่งที่มีไฟล์แนบอันตรายไปยังพนักงานสถาบันการเงิน เมื่อคอมพิวเตอร์เหยื่อติดมัลแวร์แล้ว ผู้โจมตีจึงติดตั้งแบ็กดอร์ที่ออกแบบสำหรับการจารกรรม การขโมยข้อมูล และการจัดการระบบระยะไกล เพื่อสอดส่องดูธุรกรรมการเงิน

ในตอนที่ค้นพบกลุ่มนี้ นักวิจัยของแคสเปอร์สกี้ แลป ประเมินไว้ว่า กลุ่ม Carbanak น่าจะขโมยเงินไปแล้วมากถึง 1 พันล้านเหรียญสหรัฐ โดยกลุ่มนี้ได้โจมตีธนาคาร ระบบการจ่ายเงินออนไลน์ และสถาบันการเงินต่างๆ ไปมากกว่า 100 แห่ง ใน 30 ประเทศในทวีปยุโรป เอเชีย อเมริกาเหนือและใต้ และภูมิภาคอื่นๆ

ในปี 2016 แคสเปอร์สกี้ แลป พบว่า มีกลุ่มอาชญากรไซเบอร์อีก 2 กลุ่ม ที่ทำงานคล้ายกับ Carbanak นั่นคือ Metel และ GCMAN ซึ่งโจมตีสถาบันการเงินโดยใช้มัลแวร์และแผนการร้ายสุดล้ำเพื่อขโมยเงินออกมา นอกจากนี้ยังมีกลุ่มที่ใช้เทคนิคคล้ายกัน นั่นคือ Lazarus และ Silence