แคสเปอร์สกี้ แลป พบภัยคุกคามคืนชีพ “สปริง ดราก้อน”

รายงานเตือนภัยจากแคสเปอร์สกี้ แลป พบภัยคุกคามคืนชีพ “สปริง ดราก้อน” กลับมาด้อมๆ มองๆ ประเทศแถบทะเลจีนใต้
ครอบคลุม ไต้หวัน อินโดนีเซีย เวียดนาม ฟิลิปปินส์ มาเก๊า มาเลเซีย ฮ่องกง และไทย!

ต้นปี พ.ศ. 2560 นักวิจัยของแคสเปอร์สกี้ แลป ได้สังเกตพบกิจกรรมของ APT ที่เรียกว่า สปริง ดราก้อน “Spring Dragon” (หรือรู้จักกันในชื่อ LotusBlossom) มีจำนวนเพิ่มขึ้น โดยเป็นการจู่โจมที่เกี่ยวข้องกับเครื่องมือทั้งแบบใหม่และที่ได้ปรับเปลี่ยน รวมทั้งเทคนิคใหม่ และพบประเทศเป้าหมายอยู่แถบทะเลจีนใต้ ผู้เชี่ยวชาญของแคสเปอร์สกี้ แลป ได้ตีพิมพ์ผลการวิเคราะห์ชุดเครื่องมือที่ผู้ทำการบุกรุกจู่โจมดังกล่าวนำมาใช้งาน เพื่อช่วยให้องค์กรมีความเข้าใจลักษณะของภัยคุกคาม และทำการปกป้องตนเองได้ดียิ่งขึ้น

Spring Dragon เป็นตัวกระตุ้นภัยคุกคามที่อยู่มาเป็นเวลานาน มีเป้าหมายที่องค์กรการเมือง หน่วยงานรัฐบาล และองค์กรการศึกษาระดับสูงในเอเชียมาตั้งแต่ปี พ.ศ. 2555 และทางแคสเปอร์สกี้ แลปได้ทำการติดตามแกะรอย APT ในช่วงหลายปีที่ผ่านมา

ต้นปี พ.ศ. 2560 แคสเปอร์สกี้ แลปได้ระบุชี้การโจมตีที่ถูกปลุกฟื้นคืนชีพขึ้นใหม่ ที่พบในตัวกระตุ้นภัยคุกคามที่มาอาละวาดในแถบทะเลจีนใต้ จากผลการตรวจวัดระยะไกลโดยแคสเปอร์สกี้ แลปพบว่า ไต้หวันตกเป็นเป้าหมายการโจมตีสูงที่สุด ตามด้วยอินโดนีเซีย เวียดนาม ฟิลิปปินส์ มาเก๊า มาเลเซีย ฮ่องกง และไทย นักวิจัยของแคสเปอร์สกี้ แลปได้ทำการตรวจสอบรายละเอียดของตัวอย่างมัลแวร์ Spring Dragon จำนวน 600 ตัวอย่างเพื่อเป็นการช่วยเหลือให้องค์กรได้มีความเข้าใจที่ชัดเจน และทำการปกป้องตนเองได้ดียิ่งขึ้น

ภาพรวมจากการตรวจสอบเครื่องมือของ Spring Dragon โดยแคสเปอร์สกี้ แลป มีดังนี้

• ชุดเครื่องมือประกอบด้วยเซ็ตของลิ้งก์ที่ปรับแต่งขึ้นมาโดยเฉพาะและเชื่อมโยงไปยังคอมมานด์และคอนโทรลเซิร์ฟเวอร์ของแต่ละมัลแวร์ ตัวอย่างมัลแวร์มีไอพีแอดเดรสเฉพาะตัวจำนวนมากกว่า 200 แอดเดรส

• ชุดเครื่องมือนี้มาพร้อมกับข้อมูลสำหรับการติดตั้งที่ปรับแต่งมาโดยเฉพาะสำหรับการโจมตีแต่ละครั้งเพื่อทำให้การตรวจจับดำเนินไปได้ยาก

• คลังสรรพาวุธ (arsenal) ประกอบด้วยแบ็คดอร์โมดูลที่มีความหลากหลายแตกต่างกันด้านลักษณะและหน้าที่ ทั้งหมดนี้มีความสามารถในการดาวน์โหลดไฟล์เพิ่มเข้ามายังเครื่องของเหยื่อ อัพโหลดไฟล์ไปยังเซิร์ฟเวอร์ และทำให้ไฟล์หรือคอมมานด์ทำงานบนเครื่องของเหยื่อ ซึ่งจะทำให้ผู้บุกรุกเข้ามาสามารถกระทำการไม่พึงประสงค์ต่างๆ ได้ตามต้องการบนเครื่องเหยื่อ โดยเฉพาะอย่างยิ่งปฏิบัติการจารกรรมทางไซเบอร์

• การลงเวลาของการคอมไพล์มัลแวร์นั้นจะเป็นที่ GMT +8 แต่ผู้เชี่ยวชาญก็จะขอเตือนว่านั่นอาจไม่ใช้ตัวระบุเวลาที่เชื่อถือได้

อนาสตาเซีย พารา เร ผู้จัดการทั่วไป แคสเปอร์สกี้ แลป ประจำออสเตรเลียและนิวซีแลนด์ กล่าวว่า “องค์กรและธุรกิจต่างๆ จำเป็นที่จะต้องลุกขึ้นมาให้ความสนใจกับการบริหารจัดการความเสี่ยงด้านบริการและชื่อเสียง ความสูญเสียโดยเฉลี่ยที่เกิดจากการโจมตีเจาะจงเป้าหมายนั้นมีมูลค่าใกล้เคียง 1,000,000 เหรียญสหรัฐ ไม่นับรวมผลกระทบที่เกิดต่อชื่อเสียง กรณีที่ถูกโจมตีทางไซเบอร์นั้น จะเกิดการลงทุนปริมาณหนึ่งเพื่อนำมาใช้รับมือเหตุการณ์ที่เกิดขึ้นเป็นกรณีเร่งด่วน และเพื่อพัฒนาปรับปรุงซอฟต์แวร์ รวมไปถึงโครงสร้างระบบพื้นฐาน แต่จริงๆ แล้วควรที่จะเป็นในทางกลับกันต่างหาก คือ เราต้องไม่รีรอจนเกิดการโจมตีเสียก่อน แล้วถึงจะหันมาระวังตัว”

นูชิน ชาบับ นักวิจัยด้านความปลอดภัยอาวุโส ทีม GReAT ของแคสเปอร์สกี้ แลป เสริมว่า“เราเชื่อว่า Spring Dragon จะโผล่กลับขึ้นมาอยู่เรื่อยๆ อย่างต่อเนื่องในเอเชีย เป็นเรื่องสำคัญที่จะต้องทำความคุ้นเคยกับเครื่องมือและเทคนิคของมัน เราสนับสนุนให้ทุกฝ่ายไม่ว่าจะเป็นรายบุคคลทั่วไปหรือองค์กรธุรกิจให้ปฏิบัติตามกฎ Yara และกลไกการตรวจสอบอื่นๆ ที่มีใช้งานอยู่ และขอแนะนำอย่างยิ่งให้ใช้ และตรวจสอบกระบวนการทำงานของระบบความปลอดภัยแบบมัลติเลเยอร์หลายลำดับชั้นอย่างสม่ำเสมอ”

เพื่อเป็นการป้องกันข้อมูลส่วนตัวและธุรกิจให้รอดพ้นจากการโจมตีทางไซเบอร์ แคสเปอร์สกี้ แลป ขอแนะนำดังต่อไปนี้

 ติดตั้งโซลูชั่นเพื่อความปลอดภัยแบบมัลติเลเยอร์ที่มีความทันสมัยก้าวหน้า ที่มีศักยภาพครอบคลุมดูแลระบบเครือข่าย ระบบและเอ็นด์พอยต์ได้ทั้งหมด

 ให้การศึกษาและฝึกอบรมพนักงานของคุณเกี่ยวกับวิศวกรรมเชิงสังคม เนื่องจากวิธีการนี้มักจะถูกใช้เพื่อเข้าหาเหยื่อ ล่อให้เหยื่อเปิดเอกสารติดเชื้อหรือคลิ้กบนลิ้งก์ที่ติดเชื้อ

 ดำเนิจการประเมินประสิทธิภาพของระบบความปลอดภัยของโครงสร้างระบบไอทีขององค์กรเป็นประจำ

 ใช้ Kaspersky’s Threat Intelligence ของแคสเปอร์สกี้ แลป ที่ติดตามร่องรอยการจู่โจมทางไซเบอร์ เหตุการณ์หรือภัยคุกคาม และนำเสนอข้อมูลที่เกี่ยวข้องที่ทันเหตุการณ์แก่ลูกค้าเพื่อให้ตามทันเหตุการณ์ ขอข้อมูลเพิ่มเติมได้จาก intelreports@kaspersky.com