แคสเปอร์สกี้ เผยครึ่งปีแรก 2019 อุตสาหกรรมพลังงานเป็นเป้าหมายโจมตีไซเบอร์มากที่สุด

จากรายงาน Kaspersky ICS CERT Report ในช่วงหกเดือนแรกของปี 2019 โซลูชั่นของแคสเปอร์สกี้ตรวจพบภัยคุกคามในเครื่องคอมพิวเตอร์จำนวนเกือบครึ่ง (41.6%) ในระบบการควบคุมอุตสาหกรรม (Industrial Control System หรือ ICS) ขององค์กรด้านพลังงาน ภัยคุกคาม 3 อันดับแรกที่โจมตีคอมพิวเตอร์คิดรวมกันเป็น 14% คือเวิร์ม สปายแวร์ และการขุดเงินคริปโต

เหตุการณ์โจมตีไซเบอร์ในภาคอุตสาหกรรมเป็นหนึ่งในเหตุอันตรายที่สุดด้วยจะทำให้การผลิตหยุดชะงักและความสูญเสียทางการเงินก็เป็นเรื่องเอาชนะได้ยาก โดยเฉพาะเมื่อเกิดเหตุขึ้นกับอุตสาหกรรมที่เกี่ยวข้องกับชีวิตความเป็นความตายอย่างพลังงาน สถิติครึ่งปีแรกของ 2019 ผลิตภัณฑ์ของแคสเปอร์สกี้ตรวจพบว่าเครื่องคอมพิวเตอร์ ICS จำนวน 41.6% ในภาคพลังงานโดนคุกคามทางไซเบอร์ มัลแวร์ที่ถูกตรวจจับและบล็อกจำนวนมากไม่ได้ถูกออกแบบเพื่อโจมตี ICS โดยเฉพาะ ในจำนวนโปรแกรมมุ่งร้ายทั้งหมดที่ถูกบล็อกพบภัยร้ายแรงคือ ตัวขุดคริปโต (2.9%) เวิร์ม (7.1%) และสปายแวร์ (3.7%) การติดมัลแวร์จะทำให้เกิดผลกระทบต่อการใช้งานและความน่าเชื่อถือของระบบ ICS และระบบอื่นๆ ในเน็ตเวิร์กอุตสาหกรรมได้

ในกลุ่มมัลแวร์ที่ตรวจพบนี้มีมัลแวร์บางตัวที่น่าสนใจ ตัวแรกคือ AgentTesla ซึ่งเป็นมัลแวร์พวกโทรจันสปายที่ออกแบบมาเพื่อขโมยข้อมูลยืนยันตัวตน ภาพบันทึกหน้าจอ ข้อมูลที่บันทึกจากเว็บแคมและคีย์บอร์ด ซึ่งผู้โจมตีจะส่งข้อมูลเหล่านี้ผ่านเมลบ็อกที่แฮกไว้ นอกจากมัลแวร์ก็ยังพบ Meterpreter แบ็กดอร์ที่ใช้ควบคุมคอมพิวเตอร์ใน

เน็ตเวิร์กจากระยะไกล ผู้โจมตีจะสามารถควบคุมเครื่องคอมพิวเตอร์ ICS ได้อย่างลับๆ และสร้างความเสียหายได้อย่างหนักแก่ระบบอุตสาหกรรม มัลแวร์อีกตัวคือ Syswin เวิร์มไวเปอร์ตัวใหม่ที่เขียนด้วย Python และอยู่ในรูปแบบไฟล์ปฏิบัติการของวินโดวส์ ซึ่งจะส่งผลกระทบต่อคอมพิวเตอร์ ICS โดยการแพร่กระจายด้วยตนเองและทำลายข้อมูล

อุตสาหกรรมพลังงานไม่ใช่ภาคส่วนเดียวที่ประสบกับเหตุร้ายไซเบอร์ ผู้เชี่ยวชาญของแคสเปอร์สกี้พบว่าอุตสาหกรรมผลิตรถยนต์ (39.3%) และอุตสาหกรรมควบคุมอาคารอัตโนมัติ (37.8%) มีจำนวนคอมพิวเตอร์ ICS ที่ถูกโจมตีมากเป็นอันดับที่สองและสาม

นายคิริล ครูกลอฟ นักวิจัยด้านความปลอดภัย แคสเปอร์สกี้ กล่าวว่า “จากสถิติและการวิเคราะห์ภัยไซเบอร์ที่โจมตีภาคอุตสาหกรรมทำให้เราประเมินแนวโน้มปัจจุบันและคาดประเภทของอันตรายที่เราต้องเตรียมตัวรับมือได้ รายงานฉบับนี้ได้ระบุว่าผู้เชี่ยวชาญด้านความปลอดภัยจะต้องระวังซอฟต์แวร์มุ่งร้ายที่จ้องขโมยข้อมูล สอดส่องข้อมูลสำคัญ รุกล้ำเข้า พื้นที่และทำลายข้อมูล ซึ่งเหตุการณ์เหล่านี้จะสร้างความเสียหายอย่างมากแก่ภาคอุตสาหกรรม”

คำแนะนำมาตรการทางเทคนิคจาก Kaspersky ICS CERT

- อัพเดทระบบที่เชื่อมต่อเป็นส่วนหนึ่งของเน็ตเวิร์กอุตสาหกรรมอย่างสม่ำเสมอ ทั้งระบบปฏิบัติการ ซอฟต์แวร์แอปพลิเคชั่น และโซลูชั่นเพื่อความปลอดภัย
- จำกัดทราฟฟิกเน็ตเวิร์กของพอร์ตและโปรโตคอลที่ใช้กับเอดจ์เร้าเตอร์และในเน็ตเวิร์กเทคโนโลยีส่วนปฏิบัติการ (operational technology หรือ OT)
- ตรวจสอบการควบคุมการเข้าถึงและขอบเขตสำหรับส่วนประกอบของ ICS ในเน็ตเวิร์กอุตสาหกรรมของเอ็นเทอร์ไพรซ์
- จัดฝึกอบรมเรื่องการเข้าถึงเน็ตเวิร์ก OT/ICS เป็นประจำ ทั้งแก่พนักงาน พาร์ตเนอร์และซัพพลายเออร์
- ใช้โซลูชั่นเพื่อความปลอดภัยสำหรับเอ็นพอยต์โดยเฉพาะ สำหรับเซิร์ฟเวอร์ เวิร์กสเตชั่น และ HMI เพื่อปกป้อง OT และโครงสร้างระบบอุตสาหกรรมจากการโจมตีไซเบอร์ รวมถึงการตรวจสอบทราฟฟิกของเน็ตเวิร์ก โซลูชั่นอย่างเช่น Kaspersky Industrial CyberSecurity สามารถวิเคราะห์ ตรวจจับ และป้องกันระบบจากการโจมตีแบบเลือกเป้าหมายได้

รายงานฉบับเต็ม
https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/