กองวิทยาการ สำนักแผนและอำนวยการสื่อสาร กรมการสื่อสารทหาร

Signal Today Post

บทความวิทยาการ เทคโนโลยี สาระน่ารู้ รายปักษ์ ประจำวันที่ ๑๖ – ๓๐ มิ.ย.๖๓

Microsoft เปิดข้อมูลการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับ COVID-19 ให้ใช้งานได้ฟรี รับผ่าน MISP ได้

หนึ่งในกระบวนการที่จะช่วยให้องค์กรสามารถรับมือ ตรวจจับ และป้องกันการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ คือ การติดตามข้อมูลข่าวสารอย่างสม่ำเสมอ ซึ่งโดยหลัก ๆ แล้วสามารถทำได้ 2 วิธี คือ การติดตามสถานการณ์ทางไซเบอร์จากสื่อสาธารณะ (เป็นการใช้คนอ่านข้อมูล) และการรับข้อมูลที่เกี่ยวข้องกับการโจมตีจาก feed แบบอัตโนมัติ (เป็นการใช้ระบบอ่านข้อมูล) ซึ่งในช่วงสถานการณ์การระบาดของโรค COVID-19 นี้ก็มีหลายภาคส่วนได้พัฒนาแหล่งข้อมูลในลักษณะที่เป็น threat intelligence สำหรับแลกเปลี่ยนข้อมูลภัยคุกคามและการโจมตี เช่น ข้อมูลของมัลแวร์ หรือรูปแบบพฤติกรรมการโจมตีที่ควรตรวจสอบ

เมื่อวันที่ 14 พฤษภาคม 2563 บริษัท Microsoft ได้ประกาศเปิดแหล่งข้อมูลการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับ COVID-19 ให้องค์กรหรือผู้ที่สนใจดาวน์โหลดไปใช้งานได้ฟรี โดยตัวข้อมูลจะเป็นในลักษณะ indicator ค่าแฮชของมัลแวร์ จุดประสงค์เพื่อให้ผู้ดูแลระบบนำข้อมูลดังกล่าวไปปรับปรุงระบบตรวจจับหรือป้องกันการโจมตี (เช่น ตั้งค่าการบล็อคอีเมลใน Office 365 หรือเพิ่มในฐานข้อมูลของโปรแกรมแอนติไวรัส) การรับข้อมูลดังกล่าวสามารถทำได้ทั้งผ่าน Azure Sentinel และ MISP โดยตัวอย่างการตั้งค่าสามารถศึกษาเพิ่มเติมได้จากที่มา

ที่มา : https://www.thaicert.or.th/newsbite/2020-05-18-02.html