ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ ศสป. **โทร.** ๐-๒๒๘๒-๑๐๔๗-๔๘

ที่ มท ๐๓๑๗/ว ๒๕๔ **วันที่** ๑๕ พฤษภาคม ๒๕๖๐

เรื่อง การแจ้งเตือนและป้องกันการแพร่กระจายของไวรัสเรียกค่าไถ่ Ransomware Wanacrypt

เรียน อธ.วปค. ผอ.สน. หน.ผตปค. ผตปค. ผชช. ผช.ลธ.ศอ.บต.(ปค.) ผอ.กอง ลปค. หน.กพร. และ หน.กตภ.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้แจ้งเตือนการแพร่กระจายของ Ransomware (ไวรัสเรียกค่าไถ่) ชื่อ Wanacrypt ไปยังเครื่องคอมพิวเตอร์ทั่วโลกผ่านทางสื่อออนไลน์และประสานงานผ่านทางจดหมายอิเล็กทรอนิกส์มายัง ศสป. โดยในวันที่ ๑๒ พ.ค. ๒๕๖๐ กลุ่ม Hacker ได้ทำการแพร่กระจายไวรัสประเภท Ransomware ชื่อ Wanacrypt ผ่านทางช่องโหว่ของระบบปฏิบัติการ Windows ชื่อ SMBv๑ Protocal ซึ่งสามารถแพร่กระจายผ่านทางเครื่องคอมพิวเตอร์ในสำนักงานที่เชื่อมต่อเครือข่ายเดียวกันได้อย่างรวดเร็ว จนสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ทั่วโลก รวมทั้งประเทศไทย โดยช่องโหว่ดังกล่าวเป็นช่องโหว่ที่สำนักงานความมั่นคงแห่งชาติ (NSA) ของสหรัฐอเมริกาใช้ในการหาข่าวกรองด้านความมั่นคง และถูกนำออกมาเผยแพร่โดยกลุ่ม Hacker

จากการตรวจสอบพบว่า Ransomware ดังกล่าวจะทำการเข้ารหัสไฟล์งานบนเครื่องคอมพิวเตอร์ทำให้ไม่สามารถใช้งานไฟล์ได้ และเรียกร้องเงินค่าไถ่ เพื่อแลกกับรหัสปลดล๊อกไฟล์ โดยการโจมตีครั้งนี้ถือเป็นการโจมตีที่ใหญ่ที่สุดและสร้างความเสียหายเป็นวงกว้าง ในต่างประเทศพบการโจมตีบริษัทเอกชนและหน่วยงานราชการในหลายประเทศจนสร้างความเสียหายให้กับธุรกิจและการปฏิบัติงาน สำหรับในประเทศไทยพบการแพร่กระจายดังกล่าวแล้วในหลายหน่วยงานทั้งภาครัฐและเอกชน

เพื่อป้องกันการแพร่กระจายของ Ransomware ดังกล่าว ศสป. ขอความร่วมมือท่านได้กรุณาแจ้ง จนท. ผู้ปฏิบัติงานกับเครื่องคอมพิวเตอร์ในหน่วยงานของท่านให้ดำเนินการ Update ระบบปฏิบัติการ Windows บนเครื่องคอมพิวเตอร์ทุกเครื่องทันที โดยเฉพาะเครื่องคอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการ Windows XP เพื่อปิดช่องโหว่ดังกล่าว โดยสามารถดูขั้นตอนการ Update ระบบปฏิบัติการได้ที่เว็บไซต์ https://multi.dopa.go.th/icad (*คลิกเลือกหัวข้อข่าวประชาสัมพันธ์ เลือกการป้องกันการแพร่กระจายของ Ransomware Wanacrypt*) และให้ดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ในหน่วยงานของท่านหากพบเครื่องคอมพิวเตอร์ใดติด Ransomware ดังกล่าวให้ดำเนินการตัดการเชื่อมต่อผ่านเครือข่าย Lan หรือปิด Wifi โดยทันทีและแจ้งให้ ศสป. ทราบทางหมายเลขโทรศัพท์ ๐๒-๒๘๒-๑๐๔๗-๔๘ และ ๐๒-๒๘๓-๑๒๒๒ ทั้งนี้ ศสป.จะดำเนินการตัดการเชื่อมต่อผ่านเครือข่ายของหน่วยงานนั้นเพื่อระงับการแพร่กระจายไปยังหน่วยงานอื่นของ ปค. หลังจากแก้ไขปัญหาของหน่วยงานดังกล่าวเรียบร้อยแล้ว จึงจะเปิดให้ใช้งานตามปกติต่อไป

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นายศุภลักษณ์ ปรีติเขมรัตน์)
ผอ.ศสป.