

[test](#)

- [sikayet var](#) [sikayet.com](#) [sikayet](#) [sikayet sitesi](#) [alo sikayet](#)

เรียน ผู้ใช้งาน internet ทุกท่าน
เรื่อง แจ้งเตือน มัลแวร์เรียกค่าไถ่ Petya สายพันธุ์ใหม่ แพร่กระจายแบบเดียวกับ WannaCry เขารหัสลับข้อมูลทั้งดิสก์

ข่าวประชาสัมพันธ์ : [29 มิถุนายน 2560]

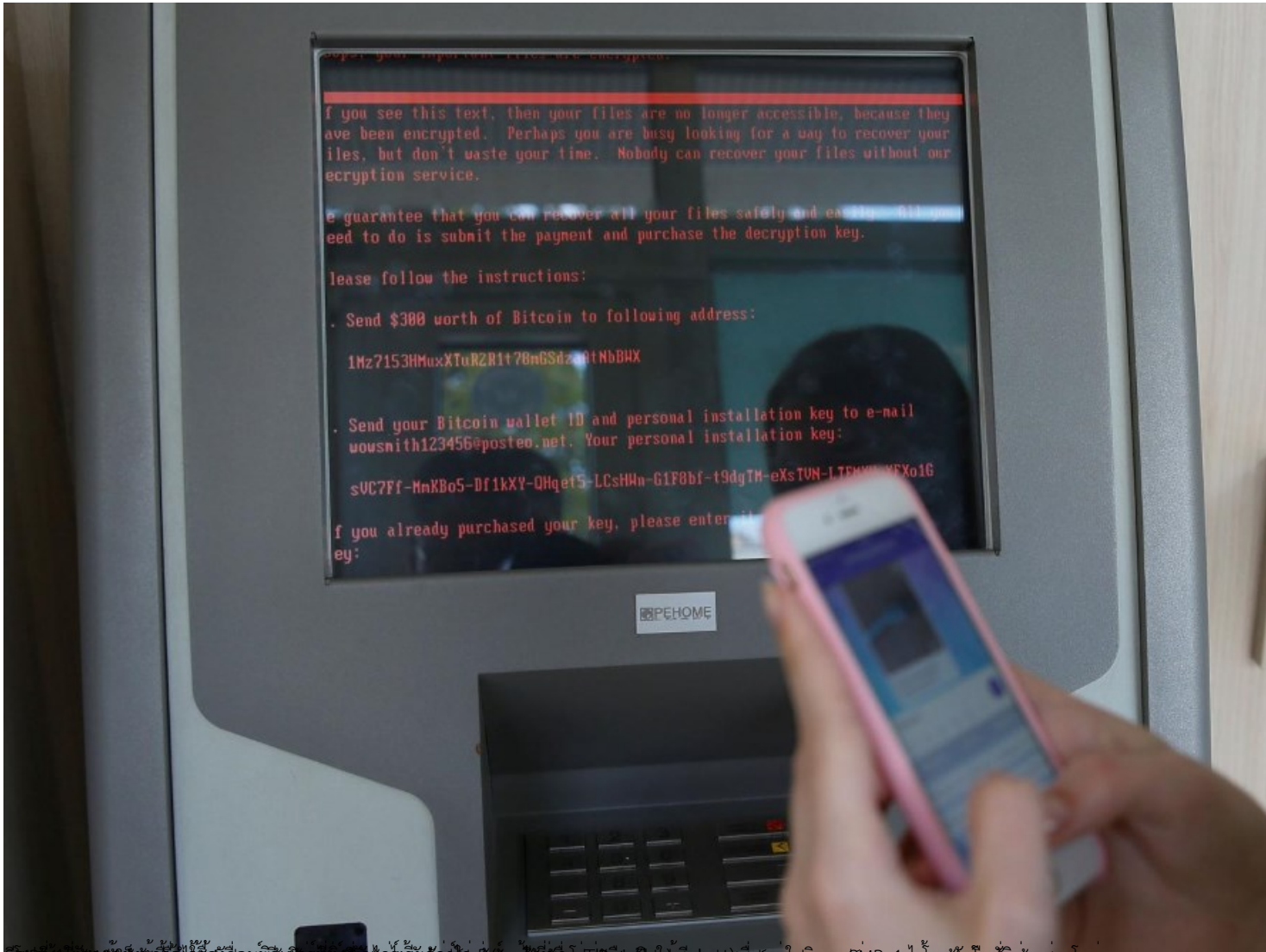
เรียน ท่านผู้ใช้งานอินเทอร์เน็ตทุกท่าน

เรื่อง แจ้งเตือน มัลแวร์เรียกค่าไถ่ Petya สายพันธุ์ใหม่ แพร่กระจายแบบเดียวกับ WannaCry เขารหัสลับข้อมูลทั้งดิสก์

เมื่อวันที่ 27 มิถุนายน 2560 มีรายงานการแพร่ระบาดของมัลแวร์เรียกค่าไถ่ Petya สายพันธุ์ใหม่ที่แพร่กระจายผ่านช่องโหว่ของระบบ SMBv1 แบบเดียวกับที่มัลแวร์ WannaCry ใช้ (มัลแวร์เรียกค่าไถ่ WannaCry <https://www.thaicert.or.th/alerts/user/2017/al2017us001.html>) สถิติความเสียหายพบคอมพิวเตอร์ทั่วโลกติดมัลแวร์นี้แล้วกว่า 300,000 เครื่องภายใน 72 ชั่วโมง ประเทศที่ได้รับแจ้งว่าถูกโจมตี ได้แก่ รัสเซีย ยูเครน อินเดีย และประเทศในแถบยุโรป หน่วยงานที่ได้รับผลกระทบ เช่น ธนาคารกลาง บริษัทพลังงานไฟฟ้า สนามบิน เป็นต้น

มัลแวร์เรียกค่าไถ่ Petya เคยมีการแพร่ระบาดมาแล้วก่อนหน้านี้เมื่อกลางปี 2559 ลักษณะการทำงานจะไม่ใช้การเข้ารหัสลับไฟล์ข้อมูลเหมือนมัลแวร์เรียกค่าไถ่ทั่วไป แต่จะเข้ารหัสลับ Master File Table (MFT) ของพาร์ทิชัน ซึ่งเป็นตารางที่ใช้ระบุตำแหน่งชื่อไฟล์และเนื้อหาของไฟล์ในฮาร์ดดิสก์ ทำให้ผู้ใช้ไม่สามารถเข้าถึงข้อมูลในฮาร์ดดิสก์ได้

เครื่องที่ตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่ จะไม่สามารถเปิดระบบปฏิบัติการขึ้นมาใช้งานได้ตามปกติ โดยจะปรากฏหน้าจอเป็นข้อความสีดำตามรูป ผู้พัฒนามัลแวร์เรียกร้องให้เหยื่อจ่ายเงินเป็นจำนวน 300 ดอลลาร์สหรัฐ โดยให้จ่ายเป็น Bitcoin เพื่อปลดล็อกถอดรหัสลับข้อมูล



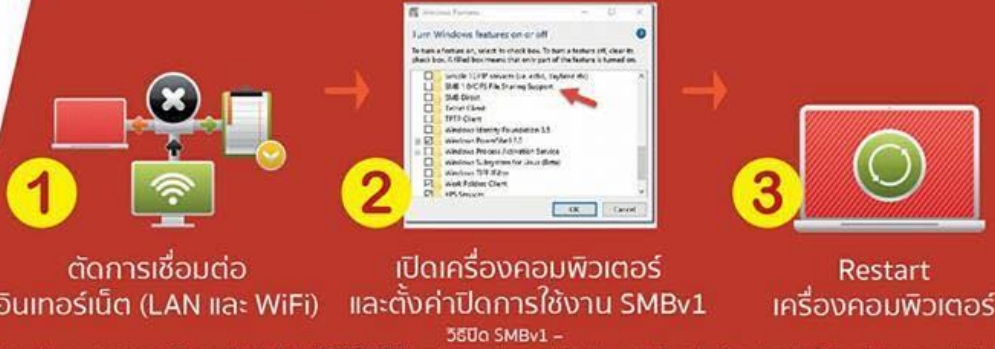
2. แสดงข้อมูลที่อยู่ของเครื่องคอมพิวเตอร์ที่โดนโจมตีและข้อมูลที่เกี่ยวข้อง (เช่น ชื่อเครื่อง, ที่อยู่ IP, ชื่อผู้ใช้, ชื่อระบบปฏิบัติการ, ชื่อเครือข่าย LAN, ชื่อ WiFi) และชื่อเครื่องที่

ป้องกัน รับมือ RANSOMWARE PETYA สำหรับผู้ใช้งานทั่วไป



ก่อนเปิดเครื่องคอมพิวเตอร์

28 มิ.ย. 60 9.30 น.



<https://support.microsoft.com/th-th/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows>

ปรับปรุงระบบปฏิบัติการของคอมพิวเตอร์ให้เป็นปัจจุบันทันที



ขณะใช้เครื่องคอมพิวเตอร์ หากเครื่องคอมพิวเตอร์หยุดทำงาน Reboot ตัวเอง และหน้าจอแสดง CHKDSK

- 1 ปิดเครื่องทันที เนื่องจาก Petya จะเข้ารหัสลับข้อมูลหลัง Restart
- 2 ติดต่อผู้ดูแลระบบ เพื่อสำเนาข้อมูลโดยบูทเครื่องจากสื่อบันทึกข้อมูลภายนอก

*อย่าลืมสำรองข้อมูลอย่างสม่ำเสมอ และปรับปรุงระบบปฏิบัติการให้เป็นปัจจุบัน

ข้อมูลสนับสนุน ภัยคุกคาม
www.thaicert.or.th | www.etrda.or.th

ศูนย์ประสานการรณรงค์ความปลอดภัยไซเบอร์ (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

