ที่ นภ ๐๐๑๓/๓๖๒๕

ศาลากลางจังหวัดหนองบัวลำภู
ถนนหนองบัวลำภู-เลย ๓๙๐๐๐

๓๐ มิถุนายน ๒๕๖๐

เรื่อง แจ้งเตือนไวรัสคอมพิวเตอร์ Ransomware:Petya

เรียน หัวหน้าส่วนราชการทุกส่วนราชการ หัวหน้าหน่วยงานรัฐวิสาหกิจ นายอำเภอทุกอำเภอ
ผู้บริหารองค์กรปกครองส่วนท้องถิ่น และผู้บริหารองค์กรภาคเอกชน

สิ่งที่ส่งมาด้วย แผ่นประชาสัมพันธ์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เตือนภัยฯ จำนวน ๑ ชุด

ด้วย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ได้แจ้งเตือนไวรัสคอมพิวเตอร์ประเภทมัลแวร์ Ransomware ชื่อ Petya หากถูกโจมตีจาก Petya ข้อมูลจะถูกเข้ารหัสและไม่สามารถแก้ไขได้ หากต้องการถอดรหัสผู้ใช้งานจะต้องทำการจ่ายเงิน เพื่อให้ได้มาซึ่งรหัสปลดล็อค

ในการนี้ จังหวัดหนองบัวลำภู จึงขอแจ้งแนวทางป้องกัน ดังนี้

<u>แนวทางการป้องกันการติดมัลแวร์เรียกค่าไถ่ ชื่อ</u> Petya

๑. ไม่เปิดเอกสารแนบอีเมล์โดยไม่จำเป็น และตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมล์ฉบับนั้นจริงหรือไม่

๒. ควรหลีกเลี่ยงการ Dowload Fite จาก Web Site ที่ไม่น่าเชื่อ

๓. ทำการสำรองข้อมูลที่สำคัญโดยสม่ำเสมอ

๔. ปรับปรุงระบบปฏิบัติการ Microsoft Windows (Patch Update) ให้เป็นปัจจุบันอยู่เสมอ

หากพบการติดไวรัสดังกล่าวให้ปิดเครื่องและแจ้งเจ้าหน้าที่ไทยเซิร์ต (ETDA) ที่หมายเลขโทรศัพท์ ๐๒-๑๒๓๑-๒๑๒ ได้โดยตรง

จึงเรียนมาเพื่อทราบและพิจารณาดำเนินการ

ขอแสดงความนับถือ

(นายโชติ เชื้อไชย)
รองผู้ว่าราชการจังหวัด ปฏิบัติราชการแทน
ผู้ว่าราชการจังหวัดหนองบัวลำภู

สำนักงานสถิติจังหวัด
โทร ๐-๔๒๓๑-๖๗๓๗
E-mail : nblamphu@nso.go.th

1058

สำนักงานสถิติจังหวัดหนองบัวลำภู
รับที่ 1058
วันที่ 28 มิ.ย. 60
เวลา 09.10 น.

ด่วนที่สุด บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มพัฒนาระบบเครื่องคอมพิวเตอร์ฯ โทร. ๑๗๓๔๖

ที่ ๐๔.๓/ ๒๒ **วันที่** ๒๗ มิถุนายน ๒๕๖๐

เรื่อง แจ้งเตือนไวรัสคอมพิวเตอร์ Ransomware: Petya

เรียน ผสช./ รสช./ ผตก./ ผอ.ศูนย์/ สำนัก/ กลุ่มขึ้นตรงต่อผู้บริหาร/ สถิติจังหวัด และ ผอ.กลุ่มใน ศทก.

ด้วย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ได้แจ้งเตือนไวรัสคอมพิวเตอร์ประเภทมัลแวร์ Ransomware ชื่อ Petya หากถูกโจมตีจาก Petya ข้อมูลจะถูกเข้ารหัสและไม่สามารถแก้ไขได้ หากต้องการถอดรหัสผู้ใช้งานจะต้องทำการจ่ายเงิน เพื่อให้ได้มาซึ่งรหัสในการปลดล็อค

ดังนั้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ขอแจ้งเตือนผู้ใช้งานโปรดระมัดระวังในการใช้งานระบบสารสนเทศ สสช. โดยมีแนวทางป้องกัน ดังนี้

๑. ไม่เปิดเอกสารแบบอีเมล์โดยไม่จำเป็น และตรวจสอบกับผู้ส่งก่อนว่าได้ส่งอีเมล์ฉบับนั้นจริงหรือไม่

๒. ควรหลีกเลี่ยงการ Download File จาก Web Site ที่ไม่น่าเชื่อถือ

๓. ทำการสำรองข้อมูลที่สำคัญโดยสม่ำเสมอ

๔. ปรับปรุงระบบปฏิบัติการ Microsoft Windows (Patch Update) ให้เป็นปัจจุบันอยู่เสมอ

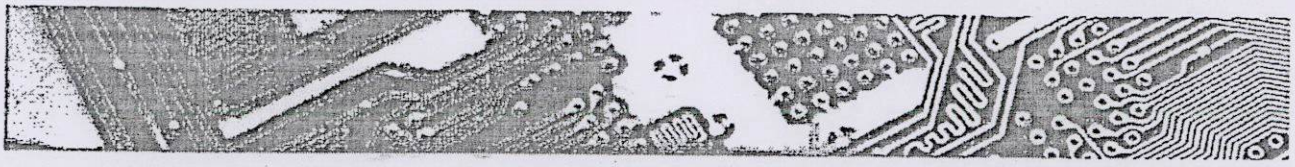
ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้แนบข้อแนะนำในการป้องกันจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) มาพร้อมนี้ หากพบการติดไวรัสดังกล่าวให้ปิดเครื่องและแจ้งเจ้าหน้าที่ไทยเซิร์ต (ETDA) ที่หมายเลขโทรศัพท์ ๐๒-๑๒๓๑-๒๑๒ ได้โดยตรง หรือกลุ่มพัฒนาระบบเครื่องคอมพิวเตอร์และเครือข่าย หมายเลขโทรศัพท์ ๑๗๓๔๕, ๑๗๓๔๙

จึงเรียนมาเพื่อโปรดทราบ

(นายธเนส โกมลวิภาต)
ผู้อำนวยการกลุ่มพัฒนาระบบเครื่องคอมพิวเตอร์และเครือข่าย
รักษาราชการแทน
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

28 มิ.ย. 60 เวลา 9.10 น.

1936



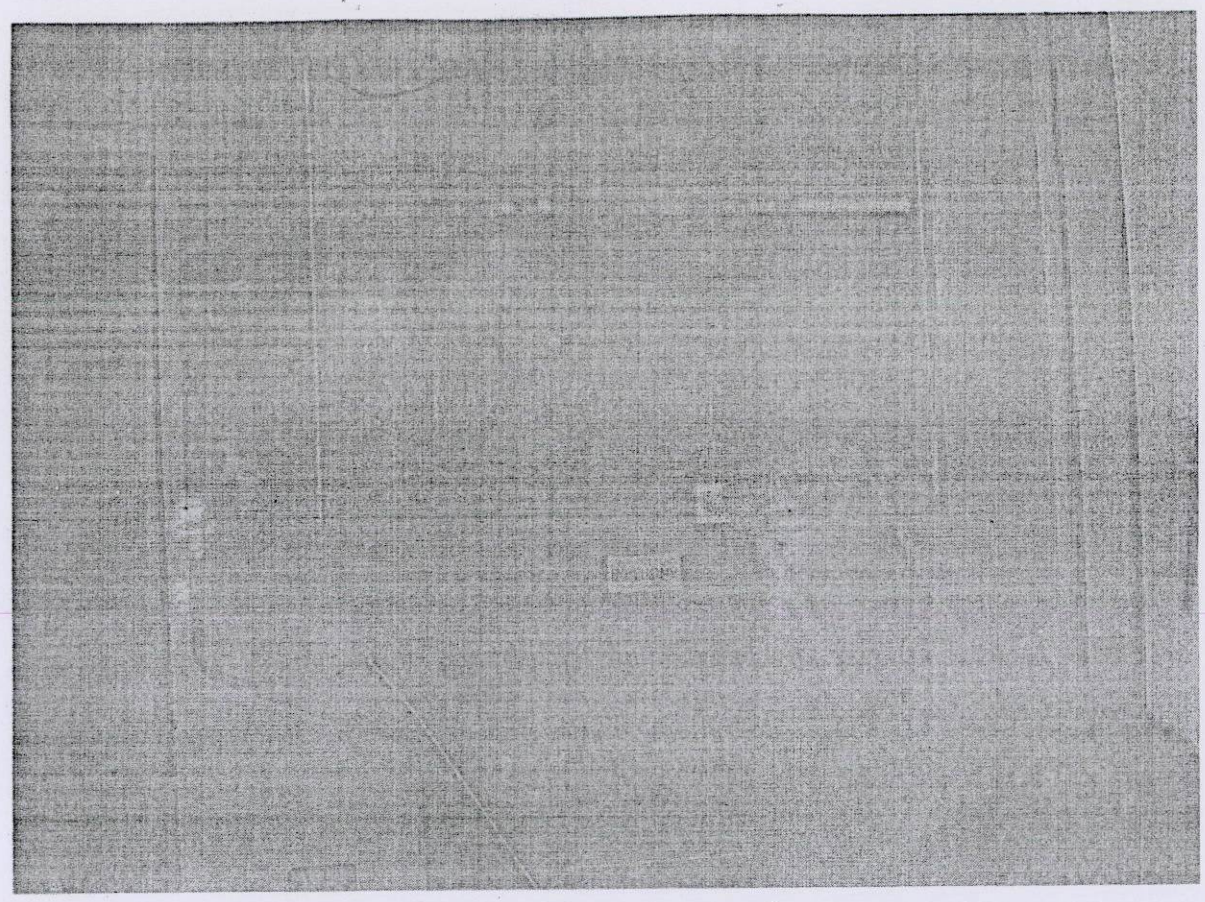
แจ้งเตือน มัลแวร์เรียกค่าไถ่ Petya สายพันธุ์ใหม่ แพร่กระจายแบบเดียวกับ WannaCry เข้ารหัสลับข้อมูลทั้งดิสก์

วันที่ประกาศ: 27 มิถุนายน 2560
ปรับปรุงล่าสุด: 27 มิถุนายน 2560
เรื่อง: แจ้งเตือน มัลแวร์เรียกค่าไถ่ Petya สายพันธุ์ใหม่ แพร่กระจายแบบเดียวกับ WannaCry เข้ารหัสลับข้อมูลทั้งดิสก์
ประเภทภัยคุกคาม: Intrusion

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 [1] [2]

มัลแวร์เรียกค่าไถ่ Petya เคยมีการแพร่ระบาดมาแล้วก่อนหน้านี้เมื่อกลางปี 2559 [3] ลักษณะการทำงานจะไม่ใช่การเข้ารหัสลับไฟล์ข้อมูลเหมือนมัลแวร์เรียกค่าไถ่ทั่วไป แต่จะเข้ารหัสลับ Master File Table (MFT) ของฮาร์ดดิสก์ ซึ่งเป็นตารางที่ใช้ระบุตำแหน่งชื่อไฟล์และเนื้อหาของไฟล์ในฮาร์ดดิสก์ ทำให้ผู้ใช้ไม่สามารถเข้าถึงข้อมูลในฮาร์ดดิสก์ได้ [4]

เครื่องที่ตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่ จะไม่สามารถเปิดระบบปฏิบัติการขึ้นมาใช้งานได้ตามปกติ โดยจะปรากฏหน้าจอเป็นข้อความดังตามรูปที่ 1 ผู้พัฒนามัลแวร์เรียกร้องให้เหยื่อจ่ายเงินเป็นจำนวน 300 ดอลลาร์สหรัฐ โดยให้จ่ายเป็น Bitcoin เพื่อปลดล็อกถอดรหัสลับข้อมูล



รูปที่ 1 ตัวอย่างหน้าจอเครื่องคอมพิวเตอร์ที่ติดมัลแวร์เรียกค่าไถ่ Petya (ที่มา - The Independent [5])

จากข้อมูลเบื้องต้น มัลแวร์เรียกค่าไถ่ Petya สายพันธุ์ใหม่ (ถูกเรียกชื่อว่า Petwrap) มีความสามารถในการแพร่กระจายโดยอัตโนมัติผ่านช่องโหว่ของระบบ SMBv1 ใน Windows ทำให้เครื่องคอมพิวเตอร์ที่ยังไม่ได้อัปเดตแพตช์แก้ไขช่องโหว่หรือเปิดให้สามารถเชื่อมต่อบริการ SMBv1 ได้จากเครือข่ายภายนอก มีโอกาสที่จะตกเป็นเหยื่อได้

ข้อแนะนำในการป้องกัน

1. สำหรับครั้งแรกก่อนมีการเปิดใช้งานเครื่องคอมพิวเตอร์ ให้ตัดการเชื่อมต่อทางเครือข่ายก่อน (LAN และ WiFi) จากนั้นเปิดเครื่องคอมพิวเตอร์เพื่อติดตั้งแพตช์ (ข้อ 3) หรือตั้งค่าปิดการใช้งาน SMBv1 (ข้อ 4) และทำการ Restart เครื่องคอมพิวเตอร์อีกครั้ง
2. ในขณะใช้งานหากเครื่องคอมพิวเตอร์หยุดทำงานและแสดงหน้าจอสีน้ำเงิน ห้าม Restart เครื่อง เนื่องจากมัลแวร์ Petya จะเข้ารหัสลับข้อมูลหลัง Restart เครื่อง ฉะนั้นให้รีบปิดเครื่องคอมพิวเตอร์และติดต่อผู้ดูแลระบบเพื่อสำรองข้อมูลออกจากเครื่องคอมพิวเตอร์โดยด่วน
3. ติดตั้งแพตช์แก้ไขช่องโหว่ SMBv1 จาก Microsoft โดย Windows Vista, Windows Server 2008 ถึง Windows 10 และ Windows Server 2016 ดาวน์โหลดอัปเดตได้จาก https://technet.microsoft.com/en-us/library/security/ms17-010.aspx ส่วน Windows XP และ Windows Server 2003 ดาวน์โหลดอัปเดตได้จาก https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
4. หากไม่สามารถติดตั้งอัปเดตได้ เนื่องจากมัลแวร์เรียกค่าไถ่ Petya แพร่กระจายผ่านช่องโหว่ SMBv1 ซึ่งถูกใช้ใน Windows เวอร์ชันเก่า เช่น Windows XP, Windows Server 2003 หรืออุปกรณ์เครือข่ายบางรุ่น หากใช้งาน Windows เวอร์ชันใหม่และไม่มีความจำเป็นต้องใช้ SMBv1 ผู้ดูแลระบบอาจพิจารณาปิดการใช้งาน SMBv1 โดยดูวิธีการปิดได้จาก https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
5. หากไม่สามารถติดตั้งอัปเดตได้ ผู้ดูแลระบบควรติดตามและป้องกันการเชื่อมต่อพอร์ต SMB (TCP 137, 139 และ 445 UDP 137 และ 138) จากเครือข่ายภายนอก อย่างไรก็ตาม การบล็อกพอร์ต SMB อาจมีผลกระทบกับบางระบบที่จำเป็นต้องใช้งานพอร์ตเหล่านี้ เช่น file sharing, domain, printer ผู้ดูแลระบบควรตรวจสอบก่อนบล็อกพอร์ตเพื่อป้องกันไม่ให้เกิดปัญหา
6. อัปเดตระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุดอยู่เสมอ หากเป็นได้ได้ควรหยุดใช้งานระบบปฏิบัติการ Windows XP, Windows Server 2003 และ Windows Vista เนื่องจากสิ้นสุดระยะเวลาสนับสนุนด้านความมั่นคงปลอดภัยแล้ว หากยังจำเป็นต้องใช้งานไม่ควรใช้กับระบบที่มีข้อมูลสำคัญ
7. ติดตั้งแอนตี้ไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ ปัจจุบันแอนตี้ไวรัสจำนวนหนึ่งสามารถตรวจจับมัลแวร์ Petya สายพันธุ์ที่กำลังมีการแพร่ระบาดได้แล้ว

ข้อแนะนำในการแก้ไขหากตกเป็นเหยื่อ

1. หากพบว่าเครื่องคอมพิวเตอร์ตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่ Petya ให้ตัดการเชื่อมต่อเครือข่าย (ถอดสาย LAN, ปิด Wi-Fi) และปิดเครื่องทันที
2. แจ้งเตือนผู้ดูแลระบบในหน่วยงานว่ามีเครื่องคอมพิวเตอร์ตกเป็นเหยื่อ

ข้อแนะนำอื่นๆ

- ปัจจุบันยังไม่พบช่องทางที่สามารถกู้คืนไฟล์ที่ถูกเข้ารหัสลับจากมัลแวร์เรียกค่าไถ่ Petya ได้โดยไม่จ่ายเงิน แต่การจ่ายเงินก็มีความเสี่ยงเนื่องจากไม่สามารถมั่นใจได้ว่าจะได้ข้อมูลกลับคืนมา
- ยังไม่พบรายงานว่ามัลแวร์เรียกค่าไถ่ Petya เวอร์ชันที่กำลังแพร่ระบาดอยู่ในปัจจุบันมีการแพร่กระจายผ่านอีเมลเหมือนเวอร์ชันก่อนหน้าด้วยหรือไม่ อย่างไรก็ตาม ผู้ใช้ควรตระหนักถึงความเสี่ยงของการเปิดไฟล์แนบจากอีเมลที่น่าสงสัย
- ควรสำรองข้อมูลบนเครื่องคอมพิวเตอร์ที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ โดยสามารถศึกษาข้อมูลเพิ่มเติมได้จากบทความข้อแนะนำวิธีสำรองข้อมูลเพื่อป้องกันมัลแวร์เรียกค่าไถ่หรือข้อมูลสูญหาย https://www.thaicert.or.th/papers/general/2017/pa2017ge002.html
- หากมีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิในการเข้าถึงข้อมูลแต่ละส่วน และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์อ่านหรือแก้ไขเฉพาะไฟล์ที่มีความจำเป็นต้องใช้สิทธิเหล่านั้น
- หากพบเหตุต้องสงสัยหรือต้องการคำแนะนำเพิ่มเติมในกรณีนี้ สามารถประสานกับไทยเซิร์ตได้ทางอีเมล report@thaicert.or.th หรือโทรศัพท์ 0-2123-1212

อ้างอิง

1. http://thehackernews.com/2017/06/petya-ransomware-attack.html
2. http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/
3. https://labsblog.f-secure.com/2016/04/01/petya-disk-encrypting-ransomware/
4. https://www.bleepingcomputer.com/news/security/petrwrap-ransomware-is-a-petya-offspring-used-in-targeted-attacks/
5. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)