ด่วน! WannaCry แรง ร้าย กระจายทั่วโลก
แคสเปอร์สกี้ แลป เตือนถ้าไม่อยากร้องไห้ ต้องรีบหยุดมัน!

จะป้องกันตัวเองจาก WannaCry ได้อย่างไร

โชคร้ายที่ไม่มีวิธีการถอดรหัสไฟล์ที่ถูก WannaCry เข้ารหัสไว้ วิธีการที่ดีที่สุดคือการป้องกันไม่ให้คอมพิวเตอร์ติดเชื้อได้ตั้งแต่แรก นั่นคือ

- ถ้ายูสเซอร์ใช้งานโซลูชั่นของแคสเปอร์สกี้ แลป อยู่แล้ว แนะนำให้สแกนแบบแมนวลสำหรับพื้นที่สำคัญ (critical area) และเมื่อโซลูชั่นตรวจเจอมัลแวร์ MEM:Trojan.Win64.EquationDrug.gen ให้รีบูตระบบทันที
- ให้ยูสเซอร์เปิดฟีเจอร์ System Watcher ของแคสเปอร์สกี้ แลป เพื่อช่วยตรวจสอบมัลแวร์ใหม่ๆ ที่อาจเกิดขึ้นได้ทันท่วงที
- รีบอัพเดทซอฟต์แวร์ของวินโดวส์ คือ ตัวซีเคียวริตี้อัพเดท Microsoft Security Bulletin MS17-01 โดยเฉพาะวินโดวส์รุ่นที่ไม่ซัพพอร์ตแล้วอย่าง Windows XP หรือ Windows 2003
- แบ็คอัพไฟล์อย่างสม่ำเสมอ และเก็บสำรองข้อมูลในอุปกรณ์อื่นๆ ที่ไม่เชื่อมต่อกับคอมพิวเตอร์ ถ้ายูสเซอร์มีไฟล์แบ็คอัพล่าสุดอยู่ เมื่อโดน WannaCry โจมตี ก็จะไม่ถึงขั้นหายนะ แต่ต้องเสียเวลาหลายชั่วโมงเพื่อติดตั้งระบบใหม่ ยูสเซอร์ของแคสเปอร์สกี้ แลป หากไม่ต้องการแบ็คอัพข้อมูลเอง สามารถเลือกใช้ฟีเจอร์แบ็คอัพอัตโนมัติของ Kaspersky Total Security ได้
- เลือกใช้แอนตี้ไวรัสที่น่าเชื่อถือ Kaspersky Internet Security สามารถตรวจจับ WannaCry ได้ทั้งจากในเครื่องและตอนพยายามแพร่กระจายทั่วเน็ตเวิร์ก ฟีเจอร์ System Watcher เป็นโมดูลบิ้วต์อิน ที่จะช่วยย้อนกลับการเปลี่ยนแปลงที่ไม่ต้องการได้ ซึ่งจะช่วยป้องกันการเข้ารหัสไฟล์ได้

โซลูชั่นของแคสเปอร์สกี้ แลป สามารถตรวจจับมัลแวร์ที่ใช้ในการโจมตี WannaCry ครั้งนี้ในชื่อต่างๆ ต่อไปนี้

- Trojan-Ransom.Win32.Scatter.uf
- Trojan-Ransom.Win32.Scatter.tr
- Trojan-Ransom.Win32.Fury.fr
- Trojan-Ransom.Win32.Gen.djd
- Trojan-Ransom.Win32.Wanna.b
- Trojan-Ransom.Win32.Wanna.c
- Trojan-Ransom.Win32.Wanna.d
- Trojan-Ransom.Win32.Wanna.f
- Trojan-Ransom.Win32.Zapchast.i
- Trojan.Win64.EquationDrug.gen
- Trojan.Win32.Generic (the System Watcher component must be enabled)

ความเสี่ยงต่อการติดไวรัสหรือการแพร่กระจาย

1. ไวรัสเรียกค่าไถ่ ransomware แพร่กระจายโดยอาศัยช่องโหว่ของ Microsoft Windows ในการโจมตี รวมถึง Windows ที่ไม่ได้รับการอัพเดทล่าสุด
อ้างอิง Microsoft Security Bulletin MS17-010

2. การเปิดไฟล์แนบหรือกดผ่านลิงก์ที่มาทางอีเมลที่ไม่ทราบแหล่งที่มาและไม่น่าเชื่อถือ

3. ในเครื่องไม่มีโปรแกรมป้องกันไวรัส และไม่มีระบบการป้องกันความปลอดภัยทางด้านระบบเครือข่าย

ข้อแนะนำเพื่อลดความเสี่ยงในการติดไวรัสเรียกค่าไถ่

1. ติดตั้ง patch ล่าสุดของ Microsoft เพื่อปิดช่องโหว่ที่ใช้ในการโจมตี the official patch

2. ตรวจสอบความปลอดภัยทุกส่วนของระบบเครือข่าย (Firewall)

3. อัพเดทโปรแกรมป้องกันไวรัสให้เป็นเวอร์ชั่นใหม่ล่าสุดหรืออัพเดท Database ให้เป็นปัจจุบัน

4. ทำการแสกนแบบ Critical Area Scan หรือ Full Scan ในโปรแกรม Kaspersky โดยเร็วที่สุด

5. Restart ระบบหลังจากตรวจพบ **MEM: Trojan.Win64.EquationDrug.gen**

6. ส่งข้อมูลมายังฝ่ายบริการ ส่ง Email มายัง **newvirus@kaspersky.com**

7. หากใช้โปรแกรม Kaspersky ควร เปิดใช้งาน Feature ดังต่อไปนี้

System Watcher ที่สามารถสแกนมัลแวร์ที่ไม่รู้จัก และคอยดูแลเครื่องว่ามีอะไรที่ผิดปกติไหม การโจมตีหรือพยายามเข้ารหัสที่น่าสงสัย รวมถึง กระตุ้นให้สำรองและคืนค่าข้อมูลอัตโนมัติ (พีเจอร์นี้มีใน Kaspersky ทุกรุ่น) **วิธีการตั้งค่า** http://www.icom.co.th/faq/forum_ans.php?FaqId=110

Data Encryption การตั้งรหัสผ่าน ให้กับไฟล์งานต่าง ๆ เพื่อป้องกันมัลแวร์เรียกค่าไถ่และการเปิดเผยข้อมูล
วิธีการตั้งค่า วิธีการใช้ Feature **Data Encryption**

Backup and Restore สำรองข้อมูลแบบอัตโนมัติตามกำหนดเวลาบน Dropbox , Local Disk, Map Drive รวมถึงการทำลายไฟล์แบบไม่สามารถกู้คืนได้
วิธีการใช้ Feature **Backup and Restore**

การตั้งค่า Kaspersky เพิ่มเติมเพื่อป้องกัน Ransomware ตามคู่มือในลิงก์นี้ค่ะ
Kaspersky Internet Security 2016/2017 https://support.kaspersky.com/12158#block1
Kaspersky Total Security https://support.kaspersky.com/13238#block1

แหล่งข้อมูลเพิ่มเติม เกี่ยวกับ Ransomware Securelist