



## สำนักภาษาต่างประเทศ

งานแปลข่าวรอบโลก			
ประเทศ	สหราชอาณาจักร (อังกฤษ)	หมวด	สังคม
ข่าวประจำวัน	๑๕ พฤษภาคม ๒๕๖๐		
หัวข้อข่าว	การโจมตีทางไซเบอร์จากซอฟต์แวร์เรียกค่าไถ่แพร่กระจายไปทั่วโลก : ข้อควรรู้		

ลอนดอน : เครื่องคอมพิวเตอร์กว่า ๑๕๐ ประเทศ ถูกโจมตีโดยสิ่งที่ผู้เชี่ยวชาญเรียกว่าเป็นการโจมตีทางไซเบอร์ด้วยการเรียกค่าไถ่ซึ่งเป็นสิ่งที่ยังไม่เคยเกิดขึ้นมาก่อน ผู้เชี่ยวชาญต่างวิเคราะห์กันว่าใครเป็นผู้ที่อยู่เบื้องหลังการกระทำเพื่อแสวงหาผลประโยชน์จากข้อบกพร่องด้านความปลอดภัยของซอฟต์แวร์ระบบปฏิบัติการไม่โครซอฟต์วินโดวส์รุ่นเก่าครั้งนี้

ต่อไปนี้เป็นข้อควรรู้เกี่ยวกับการโจมตีด้วยการเรียกค่าไถ่ทางไซเบอร์

### เกิดอะไรขึ้น?

เริ่มต้นจากเครื่องคอมพิวเตอร์ทั่วโลกถูกเจาะระบบในวันศุกร์โดยอาศัยข้อบกพร่องของระบบปฏิบัติการไม่โครซอฟต์วินโดวส์ เอ็กซ์พี รุ่นเก่าที่ไม่รองรับเทคโนโลยีหลักจากบริษัทยักษ์ใหญ่ของสหรัฐอเมริกาแล้ว

การโจมตีระบบปฏิบัติการคอมพิวเตอร์ด้วยการเรียกค่าไถ่ในครั้งนี้ถูกเรียกว่า “WannaCry” ด้วยการปิดกั้นการเข้าถึงข้อมูลของผู้ใช้และเรียกค่าไถ่เป็นเงินเพื่อใช้ในการถอดรหัส ในรูปแบบสกุลเงินเสมือนที่เรียกว่า “บิทคอยน์” (Bitcoin)

### มีกี่ประเทศที่ได้รับผลกระทบ?

หัวหน้าสำนักงานตำรวจยุโรป หรือยูโรโพล (Europol) กล่าวว่า มีเหยื่อมากกว่า ๒๐๐,๐๐๐ ราย ที่ถูกโจมตีใน ๑๕๐ ประเทศ นับเป็นการโจมตีทางไซเบอร์ครั้งใหญ่ที่สุดในประวัติศาสตร์

เหยื่อหลายรายเป็นหน่วยงานที่มีความสำคัญ เช่น โรงพยาบาลในอังกฤษ บริษัทเทเลโฟนีกา ซึ่งเป็นหน่วยงานโทรคมนาคมขนาดใหญ่ในประเทศสเปน บริษัทผลิตรถยนต์เรโนลต์ บริษัทจัดส่งพัสดุ FedEx ประเทศสหรัฐอเมริกา กระทรวงมหาดไทยรัสเซีย และบริษัทจัดการขนส่งระบบราง Deutsche Bahn ของเยอรมนี

### การโจมตีแพร่ขยายไปทั่วโลกได้อย่างไร?

ผู้เชี่ยวชาญกล่าวว่า โปรแกรมเรียกค่าไถ่ดังกล่าวนี้สามารถรองรับได้หลากหลายภาษา ซึ่งแสดงให้เห็นว่ากลุ่มแฮกเกอร์ต้องการทำลายเครือข่ายคอมพิวเตอร์ทั่วโลก

ข้อมูลจากนักวิจัยศูนย์ปฏิบัติการด้านความปลอดภัยทางคอมพิวเตอร์ แคนเซอร์สก็แลป ในกรุงมอสโกกล่าวว่า ไวรัสนี้แพร่กระจายอย่างรวดเร็วเนื่องจากกลุ่มผู้ร้ายนั้นใช้รหัสติดจอตที่เชื่อกันว่าถูกพัฒนาโดยสำนักงานความมั่นคงแห่งสหรัฐอเมริกา (the US National Security Agency) และได้รั่วไหลออกมาเนื่องจากเป็นส่วนหนึ่งของเอกสารที่ถูกทิ้ง

ไวรัสชนิดนี้มีความเฉพาะตัวเนื่องจากเป็นไวรัสที่รวมการเรียกค่าไถ่เข้ากับการทำงานแบบหนอนคอมพิวเตอร์ ซึ่งหมายความว่าหากมีเครื่องใดเครื่องหนึ่งที่ติดไวรัสนี้ ระบบเครือข่ายภายในจะถูกทำการวิเคราะห์และเครื่องคอมพิวเตอร์ที่เหลือจะติดไวรัสทั้งหมด

หน่วยงานความมั่นคงแห่งสหรัฐไซแมนเทค (Symantec) กล่าวว่า มันเป็นไวรัสที่มีลักษณะไม่เฉพาะเจาะจง

### ใครเป็นผู้อยู่เบื้องหลังการโจมตีครั้งนี้?

จนถึงในปัจจุบันนี้ยังไม่ทราบว่าใครเป็นกลุ่มผู้ร้าย แต่หน่วยงานความมั่นคงของประเทศที่ได้รับผลกระทบจากไวรัสที่กำลังดำเนินการสืบหาอยู่

ผู้เชี่ยวชาญคิดว่าเป็นไปได้ที่จะมีกลุ่มผู้ร้ายมากกว่าหนึ่งคน เนื่องจากกลุ่มผู้ก่ออาชญากรรมทางไซเบอร์ในปัจจุบันนั้นตามจับกุมได้ยาก และมีการใช้รหัสลับที่ซับซ้อนมากขึ้นเพื่อหลบซ่อนในการปฏิบัติการต่าง ๆ

### ประชาชนจะป้องกันเครื่องคอมพิวเตอร์ของตัวเองได้อย่างไร?

ในเดือนมีนาคมนี้ บริษัทไมโครซอฟต์ได้เริ่มใช้วิธีการพิเศษในการแก้ปัญหาด้านความปลอดภัยสำหรับระบบปฏิบัติการวินโดวส์ เอ็กซ์พี และระบบปฏิบัติการอื่น ๆ ในรูปแบบเก่าที่ยังคงใช้งานอยู่

ศูนย์ปฏิบัติการแคสเปอร์สกี ระบุว่า กำลังหาวิธีการพัฒนาเครื่องมือในการถอดรหัสลับ “ให้ได้โดยเร็วที่สุด”

สำนักงานตำรวจยุโรป หรือยูโรโพล (Europol) ได้เปิดให้เครื่องที่ตรวจพบไวรัสสามารถดาวน์โหลดโปรแกรมถอดรหัสไวรัสเรียกค่าไถ่นี้ได้ฟรี ถึงแม้ว่าเครื่องคอมพิวเตอร์เครื่องนั้นยังไม่ถูกโจมตีจากไวรัสนี้ก็ตาม

### มีผู้ถูกเรียกค่าไถ่ไปแล้วจำนวนเท่าไร?

ข้อความที่ส่งมายังคอมพิวเตอร์ของเหยื่อจะระบุว่า เหยื่อจะต้องจ่ายค่าไถ่จำนวน ๓๐๐ ดอลลาร์สหรัฐ (๒๗๕ ยูโร) ในรูปแบบของสกุลเงิน “Bitcoin” โดยเหยื่อจะต้องทำการจ่ายเงินค่าไถ่ภายใน ๓ วัน มิเช่นนั้นจำนวนเงินค่าไถ่จะเพิ่มเป็นสองเท่า และหากไม่ได้รับการจ่ายเงินค่าไถ่ภายใน ๗ วัน ข้อมูลทั้งหมดจะถูกทำลาย

ถึงแม้ว่าการโจมตีได้แพร่ระบาดไปทั่ว แต่มีผู้จ่ายค่าไถ่ในเวลาที่กำหนดไว้น้อยมาก และเหยื่อจำนวนไม่มากนักที่ต้องการจ่ายค่าไถ่

ผู้เชี่ยวชาญให้คำแนะนำว่า ประชาชนไม่จำเป็นต้องจ่ายเงินจำนวนนี้ เนื่องจากจะเป็นการสนับสนุนให้เกิดการโจมตีมากขึ้น และไม่มีอะไรที่จะรับประกันว่าเหล่าแฮกเกอร์จะปลดล็อคการเข้าถึงข้อมูลให้ นอกจากนี้ อาจทำให้เหล่ามิจฉาชีพเข้าถึงรายละเอียดข้อมูลทางบัญชีธนาคารของเหยื่อได้อีกด้วย

ที่มาของข่าว :	<a href="http://www.channelnewsasia.com/news/world/worldwide-ransomware-cyberattacks--what-we-know-8846622">http://www.channelnewsasia.com/news/world/worldwide-ransomware-cyberattacks--what-we-know-8846622</a>
วันที่พิมพ์ :	๑๕ พฤษภาคม ๒๕๖๐

ขั้นตอนการดำเนินการ / หลักวิชาการ :
๑. คัดเลือกข่าวที่น่าสนใจและทันสมัยจากแหล่งข่าวที่น่าเชื่อถือได้ อาทิ <a href="http://www.channelnewsasia.com">www.channelnewsasia.com</a>
๒. ค้นหาข้อมูลพื้นฐานและข้อมูลทั่วไปเกี่ยวกับเรื่องที่จะแปลจากแหล่งข้อมูลภาษาไทยหรือภาษาอังกฤษ โดยการค้นหาจากระบบสืบค้นอิเล็กทรอนิกส์ และจำกัดการค้นหาเฉพาะเว็บไซต์ที่ลงท้ายด้วย .go.th, .org, .edu เป็นต้น
๓. แปลข่าวจากภาษาอังกฤษเป็นภาษาไทย โดยใช้เครื่องมือช่วยแปล เช่น พจนานุกรมทั้งแบบเล่ม และแบบออนไลน์ คลังคำศัพท์ของสำนักภาษาต่างประเทศ การแลกเปลี่ยนความคิดเห็นกับนักวิเทศสัมพันธ์ในกลุ่มงานเดียวกันเฉพาะจุดที่ยากต่อการแปล

ผู้ปฏิบัติงาน	นางสาวนัสรี สัจดีประเสริฐ	นักวิเทศสัมพันธ์ชำนาญการ
กลุ่มงาน	ภาษาอังกฤษ	ลำดับที่/ ๖/๖๐
ผู้ทาน	นางสาวสิรินดา จันทรักษ์	ผู้บังคับบัญชากลุ่มงานภาษาอังกฤษ
ผู้ตรวจ	นางสินีนารถ ดุลยสุข	ผู้อำนวยการสำนักภาษาต่างประเทศ

World

## **Worldwide ransomware cyberattacks: What we know**

LONDON: Computers in more than 150 countries have been hit by what experts are calling an unprecedented mass cyberattack using ransomware.

Experts were scrambling to determine who was behind the attack, which exploited a security flaw in older versions of Microsoft's Windows operating software.

Here is what we know so far about the cyber ransom attacks:

### **WHAT HAPPENED?**

Computers around the globe were hacked beginning on Friday using a security flaw in Microsoft's Windows XP operating system, an older version that was no longer given mainstream tech support by the US giant.

The so-called WannaCry ransomware locks access to user files and demands money - in the form of the virtual currency Bitcoin - in order to decrypt them.

### **HOW MANY COUNTRIES AFFECTED?**

Europol chief Rob Wainwright said more than 200,000 victims had been hit in more than 150 countries.

It is the largest ransomware attack observed in history.

High-profile victims include hospitals in Britain, the Spanish telecoms giant Telefonica, French carmaker Renault, US package delivery company FedEx, Russia's interior ministry and the German rail operator Deutsche Bahn.

### **HOW DID ATTACK SPREAD WORLDWIDE?**

Experts said the ransomware programme appears to support dozens of languages, showing that the hackers wanted to corrupt networks worldwide.

The virus spread quickly because the culprits used a digital code believed to have been developed by the US National Security Agency -- and subsequently leaked as part of a document dump, according to researchers at the Moscow-based computer security firm Kaspersky Lab.

The attack is unique, according to Wainwright, because it combines ransomware with a worm function, meaning once one machine is infected, the entire internal network is scanned and other vulnerable machines are infected.

The US security firm Symantec said the attack appeared to be indiscriminate.

### **WHO WAS BEHIND THE ATTACK?**

So far, the culprits are unknown, as is the motivation. Security agencies in affected countries were racing to find out.

Experts think it unlikely to have been one person, with criminally minded cyber crime syndicates nowadays going underground and using ever more sophisticated encryption to hide their activities.

#### **HOW CAN PEOPLE PROTECT THEIR COMPUTERS?**

Microsoft took the unusual step of reissuing security patches first made available in March for Windows XP and other older versions of its operating system.

Kaspersky said it was seeking to develop a decryption tool "as soon as possible".

Europol provides free decryption downloads for most ransomware already detected, though not yet for this particular attack.

#### **HOW MUCH RANSOM WAS ASKED?**

Victims were asked for payment of US\$300 (€275) in the virtual currency Bitcoin.

Payment is demanded within three days or the price is doubled, and if none is received within seven days, the files will be deleted, according to the screen message.

Given the attack's widespread nature, even such a small sum would stack up quickly, though few victims seem to be paying up so far.

Experts advise people not to pay, as it would only encourage the attackers, there is no guarantee that they will unblock files, and may result in them gaining access to victims' bank details.

Source:AFP/de

Read more at <http://www.channelnewsasia.com/news/world/worldwide-ransomware-cyberattacks--what-we-know-8846622>