เรื่อง ซอฟต์แวร์เรียกค่าไถ่บน TeamViewer, MBR และ ช่องโหว่ของเซิร์ฟเวอร์
ทดสอบและเรียบเรียงโดย กิติศักดิ์ จิรวรรณกูล และ ปณิธาน เขินอำนวย
เรียบเรียงวันที่ 31 มีนาคม 2559
ปรับปรุงวันที่ 8 เมษายน 2559

กล่าวนำ

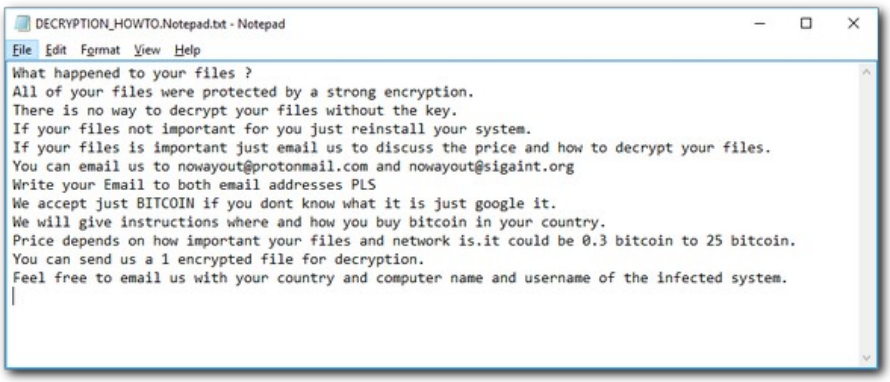
จากบทความฉบับก่อนเรื่องซอฟต์แวร์เรียกค่าไถ่ที่ชื่อ Locky จะเห็นได้ว่าปัจจุบันซอฟต์แวร์เรียกค่าไถ่แพร่กระจายและสร้างความเสียหายเป็นวงกว้างอย่างมาก ซึ่งซอฟต์แวร์เรียกค่าไถ่ส่วนใหญ่มักแพร่กระจายตัวเองผ่านทางอีเมล์โดยการส่งเป็นไฟล์แนบพร้อมข้อความที่จะหลอกล่อให้เหยื่อหลงเชื่อและเปิดไฟล์ดังกล่าว จากนั้นจึงเข้ารหัสไฟล์ต่างๆ ในเครื่องของเหยื่อ และรีดไถ่เงินจากเหยื่อ อย่างไรก็ตามบทความนี้จะนำเสนอเทคนิคอื่นๆ ที่ซอฟต์แวร์เรียกค่าไถ่ใช้ในการแพร่กระจายหรือหลบซ่อนตัวเองเพื่อทำให้ยากต่อการตรวจจับและแก้ไขอีกด้วย

ซอฟต์แวร์เรียกค่าไถ่ที่แพร่กระจายผ่านทาง TeamViewer

TeamViewer เป็นซอฟต์แวร์ที่เปิดให้มีการเข้าถึงจากระยะไกล ซึ่งสามารถใช้ในการเข้าถึงเครื่องอื่นๆ ที่ติดตั้งซอฟต์แวร์นี้ได้ด้วย อีกทั้งสามารถรอรับการเชื่อมต่อจากเครื่องอื่นๆ อีกด้วย ด้วยความสามารถของซอฟต์แวร์นี้เอง ทำให้นักเจาะระบบได้สร้างซอฟต์แวร์เรียกค่าไถ่ชื่อ Surprise เมื่อถูกซอฟต์แวร์นี้คุกคามแล้วจะมีการสร้างไฟล์

- `%Desktop%\surprise.bat`
- `%Desktop%\DECRYPTION_HOWTO.Notepad.txt`
- `%Desktop%\Encrypted_Files.Notepad`

จากนั้นจะค้นหาบัญชีผู้ใช้งานของโปรแกรม TeamViewer ที่มีรหัสผ่านในการเข้าถึงเครื่องอื่นๆ จากนั้นจะทำการแพร่กระจายตัวเองไปยังเครื่องนั้นๆ อีกด้วย และจะแสดงข้อความเรียกค่าไถ่ ดังรูปที่ 1



รูปที่ 1 แสดงข้อความเรียกค่าไถ่ของ Surprise

วิธีการป้องกัน

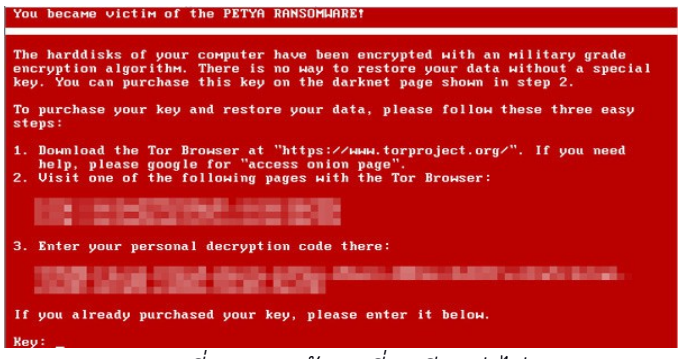
ใช้ระบบยืนยันตัวเอง 2 ชั้นเพื่อป้องกันไม่ใช่ซอฟต์แวร์เรียกค่าไถ่นี้ ตามคำแนะนำของ TeamViewer https://www.teamviewer.com/en/help/402-How-do-I-activate-deactivate-two-factor-authentication-for-my-TeamViewer-account.aspx

ซอฟต์แวร์เรียกค่าไถ่ที่ฝังตัวเองอยู่ในส่วนแรกของฮาร์ดดิสก์ หรือ Masterboot record (MBR)

ส่วนแรกของฮาร์ดดิสก์ หรือ Masterboot record (MBR) เป็นส่วนที่ทำหน้าที่เก็บข้อมูลสำหรับการทำงานที่จำเป็นก่อนการเริ่มต้นบูตระบบปฏิบัติการ ในอดีตมัลแวร์มักจะฝังตัวเองใน MBR เมื่อไม่นานมานี้มีซอฟต์แวร์เรียกค่าไถ่ชื่อ Petya จะส่งอีเมล์แนบลิงค์เพื่อเข้าสู่หน้า Dropbox เพื่อให้ดาวน์โหลดประวัติ (CV) ดังรูปที่ 2 เมื่อเหยื่อหลงเชื่อดาวน์โหลดและรันแล้วซอฟต์แวร์เรียกค่าไถ่นี้จะเข้ารหัสไฟล์ต่างๆ ในเครื่อง และฝังตัวที่ MBR เพื่อแสดงหน้าสำหรับเรียกค่าไถ่ตั้งแต่ตอนเปิดเครื่อง (ก่อนบูตเข้าระบบปฏิบัติการวินโดวส์) ดังรูปที่ 3 และ 4

รูปที่ 2 แสดงไฟล์ใน Dropbox เพื่อหลอกให้เหยื่อดาวน์โหลด

รูปที่ 3 หน้าแสดงสัญลักษณ์จะเรียกค่าไถ่ตั้งแต่บูตระบบปฏิบัติการ



รูปที่ 4 แสดงข้อมูลที่จะเรียกค่าไถ่

วิธีการป้องกัน

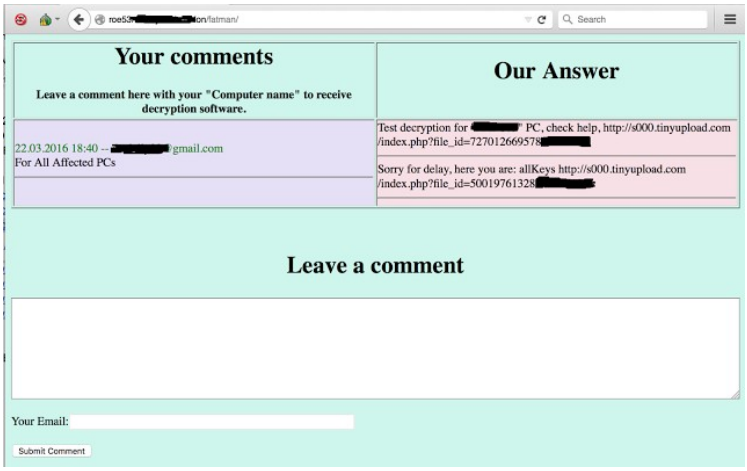
เนื่องจากส่วนแรกของฮาร์ดดิสก์นี้มักจะถูกโปรแกรมป้องกันไวรัสในปัจจุบันติดตั้ง ดังนั้นวิธีการป้องกันที่ดีที่สุดคือการติดตั้งโปรแกรมป้องกันไวรัส อัพเดต และหมั่นสแกนหามัลแวร์ในเครื่องบ่อยๆ รวมถึงไม่ดาวน์โหลดไฟล์ที่น่าสงสัยดังรูปที่ 2

ซอฟต์แวร์เรียกค่าไถ่ที่แพร่กระจายโดยการโจมตีช่องโหว่ของเซิร์ฟเวอร์

โดยทั่วไปซอฟต์แวร์เรียกค่าไถ่มักจะอาศัยการแพร่กระจายผ่านทางไฟล์แนบจากอีเมล์หรือเว็บไซต์ แต่ในช่วงที่ผ่านมาแฮกเกอร์ได้แพร่กระจายซอฟต์แวร์เรียกค่าไถ่สายพันธุ์ใหม่ ชื่อ Samsam และ Maktub ที่จะฝังตัวผ่านช่องโหว่ของเซิร์ฟเวอร์ที่ไม่ได้รับการปรับปรุงเพียงพอ อีกทั้งเฉพาะในโรงพยาบาลเท่านั้นที่เป็นเป้าหมายการแพร่กระจายของซอฟต์แวร์เรียกค่าไถ่สายพันธุ์นี้

Samsam เป็นซอฟต์แวร์เรียกค่าไถ่ที่ใช้กระบวนการเข้ารหัส RSA-2048 บิต และแพร่กระจายผ่านทางช่องโหว่ JBoss บนเซิร์ฟเวอร์ก่อนที่จะติดตั้งเว็บเชลล์ (Web shell) เผื่อฝังตัวเอง แล้วจึงเข้ารหัสไฟล์ต่างๆบนอุปกรณ์โดยไม่จำเป็นต้องติดต่อขอกุญแจในการเข้ารหัสจากเซิร์ฟเวอร์ควบคุม (Command and Control server) ของแฮกเกอร์ ซึ่งเป็นอีกจุดเด่นหนึ่งของ Samsam และ Maktub ด้วย ทำให้การเข้ารหัสและถอดรหัสรวดเร็วขึ้นอย่างมาก

รูปที่ 5 แสดงหน้าเรียกค่าไถ่ของ Samsam



รูปที่ 6 แสดงหน้าเรียกที่เหยื่อส่งข้อมูลให้แฮกเกอร์เพื่อจะจ่ายเงินค่าไถ่

วิธีการป้องกัน

1. ปรับปรุงเวอร์ชั่นของซอฟต์แวร์ต่างๆ ที่ใช้งานในเครื่องเซิร์ฟเวอร์
2. อัพเดตซอฟต์แวร์ด้านการรักษาความปลอดภัย เช่นโปรแกรมป้องกันไวรัส หรือโปรแกรมในการตรวจจับการบุกรุกต่างๆ เป็นต้น
3. ติดตั้งระบบและเตรียมแผนการสำรองข้อมูลรวมถึงการกู้คืนด้วย