TROJAN
(NJRAT + NGROK)

หลักการและเหตุผล

ปัจจุบันผู้คนส่วนใหญ่ชอบความสะดวกสบาย ซึ่งความสะดวกสบายเหล่านี้ทำให้เราเคยชินและมองข้าม ความอันตรายของการใช้คอมพิวเตอร์จึงมักละเลยในการใช้ Anti-Virus ของแท้เพื่อที่จะป้องกันข้อมูลส่วนตัวภายใคอมพิวเตอร์จึงทำให้มีช่องโหว่ดังกล่าวพวกเราจึงต้องการศึกษาและสร้าง Virus Trojan เพื่อสาธิตหนึ่งในวิธีการโจรกรรมข้อมูล โดยที่ผู้คนเหล่านั้นไม่รู้ตัว

วัตถุประสงค์

1.เพื่อศึกษาวิธีการสร้างและพัฒนามัลแวร์
2.เพื่อศึกษาลักษณะการทำงานของโทรจัน เพื่อหาวิธีป้องกันการโจรกรรม
3.เพื่อนำความรู้ในวิชา 342376 INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY มาประยุกต์ใช้

ทางผู้จัดทำทราบดีถึงข้อกฎหมายเกี่ยวกับ พรบ.คอมพิวเตอร์ จึงไม่มีการนำไปใช้จริงหรือนำไปดึงข้อมูลของผู้อื่นแต่อย่างใด ใช้ในการศึกษาเท่านั้น

ผลการทำงาน

1.ดึงดูไฟล์ แก้ไขไฟล์หรืออัพโหลดไฟล์เข้า เครื่องเหยื่อ
2.รันไฟล์ผ่านเครื่องของเราเพื่อโจมตีเหยือ
3.บันทึกหน้าจอเดสก์ท็อป เว็ปแคมและการกด แป้น พิมพ์
4.ขโมยรหัสผ่านทีบันทึกไว้ในเบราว์เซอร์หรือ แอพพลิเคชันอื่นๆ
5.เปิด หน้าเดสก์ท็อปหรือหน้าต่างทีใช้งานอยู่ ของเหยื่อ
6.ดักฟังเสียงผ่านไมโครโฟนของเครืองเหยื่อ

ขั้นตอนการทำงาน

-โดยแฮกเกอร์ จะมีลิ้งในการโหลดโปรแกรมที่เหยื่อต้องการ ที่แฝงไวรัสไปกับโปรแกรมที่ติดตั้ง

-เมื่อเหยื่อทำการติดตั้งตั้งโปรแกรมไวรัสจะ

ทำการฝังเข้าไปทำงานในเครื่องโดยที่เหยื่อไม่รู้ตัว

-หลังจากนั้นแฮกเกอร์จะสามารถดูข้อมูลต่างๆ โดยที่เหยื่อไม่รู้ตัว

เครื่องมือใช้

ngrok

สรุป

เมื่อเหยื่อทำการดาวโหลดน์แล้วติดตั้งโปรแกรมจากแฮกเกอร์เรียบร้อยร้อยทางแฮกเกอร์สามารถเข้าไปดึงและอัปโหลดไฟล์ภายในเครื่องเหยื่อได้ และสามารถดูหน้าจอเดสก์ท็อปและเว็ปแคม แบะสามารถบันทึกการกดแป้นพิมพ์และการเข้ารหัสผ่านในการเข้าสู่ระบบต่างๆได้

อาจารย์ผู้สอน
ร.ศ.ดร.จักรชัย โสอินทร์

สมาชิกภายในกลุ่ม 4 Sec.1
1.นายนันฐวุฒิ ต้นสวรรค์ 633020303-9

2.นายรวิชญ์ วงศ์พล 633020322-5

3.นายอดิเทพ ปริปุรณะ 633020336-4

4.นายอัฐพล สุระโคตร 633020930-2

อ้างอิง : https://www.gotoknow.org/posts/622755