



TROJAN + PHISHING

รายวิชา SC362006 Information and Communication Technology Security
อาจารย์ประจำวิชา ศศ.ดร.จักรชัย ไสอินทร์

หลักการและเหตุผล

ปัจจุบันเทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น มีการซื้อสินค้าผ่านแพลตฟอร์มออนไลน์มากขึ้น และมักเกิดเหตุการณ์ผู้บริโภคได้รับความเสียหายจากการหลอกลวงออนไลน์ เช่น ทำธุรกรรมทางการเงิน โดยมีการผูกบัญชีบัตรเครดิตไว้กับผู้ให้บริการร้านค้า และถูกตัดเงินอัตโนมัติเพื่อชำระสินค้าอยู่หลายครั้ง โดยที่เจ้าของบัญชีไม่รู้ตัว เพื่อหลอกให้เหยื่อข้อมูลความลับต่าง ๆ

ทำให้เห็นว่าผู้คนในสมัยนี้มองข้ามการใช้งานความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และไม่ได้คำนึงถึงความอันตรายบนโลกไซเบอร์ เป็นสาเหตุทำให้เกิดช่องโหว่นำไปสู่การก่ออาชญากรรมทางคอมพิวเตอร์ได้ ทางคณะผู้จัดทำจึงนำวิธีการโจมตีแบบฟิชซิงและโทรจันมาประยุกต์เข้าด้วยกันเพื่อเป็นแนวทางการศึกษาวิธีป้องกันการโจมตีแบบฟิชซิงและโทรจัน และให้รู้ทันกลโกงไม่ให้ตกเป็นเหยื่อของมิจฉาชีพโลกไซเบอร์

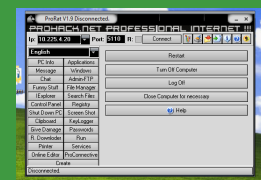
วัตถุประสงค์

1. เพื่อนำความรู้เกี่ยวกับ โทรจัน และฟิชซิงมาประยุกต์ใช้ร่วมกัน
2. เพื่อศึกษาวิธีป้องกันการโจมตีแบบฟิชซิง และโทรจัน
3. เพื่อให้รู้ทันกลโกง และไม่ตกเป็นเหยื่อของมิจฉาชีพ

ซอฟต์แวร์ที่ใช้ในการพัฒนา



vs code



Prorat



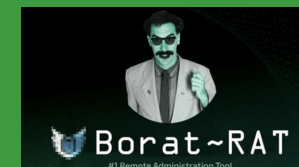
Gmail



WinRAR



HOSTINGER

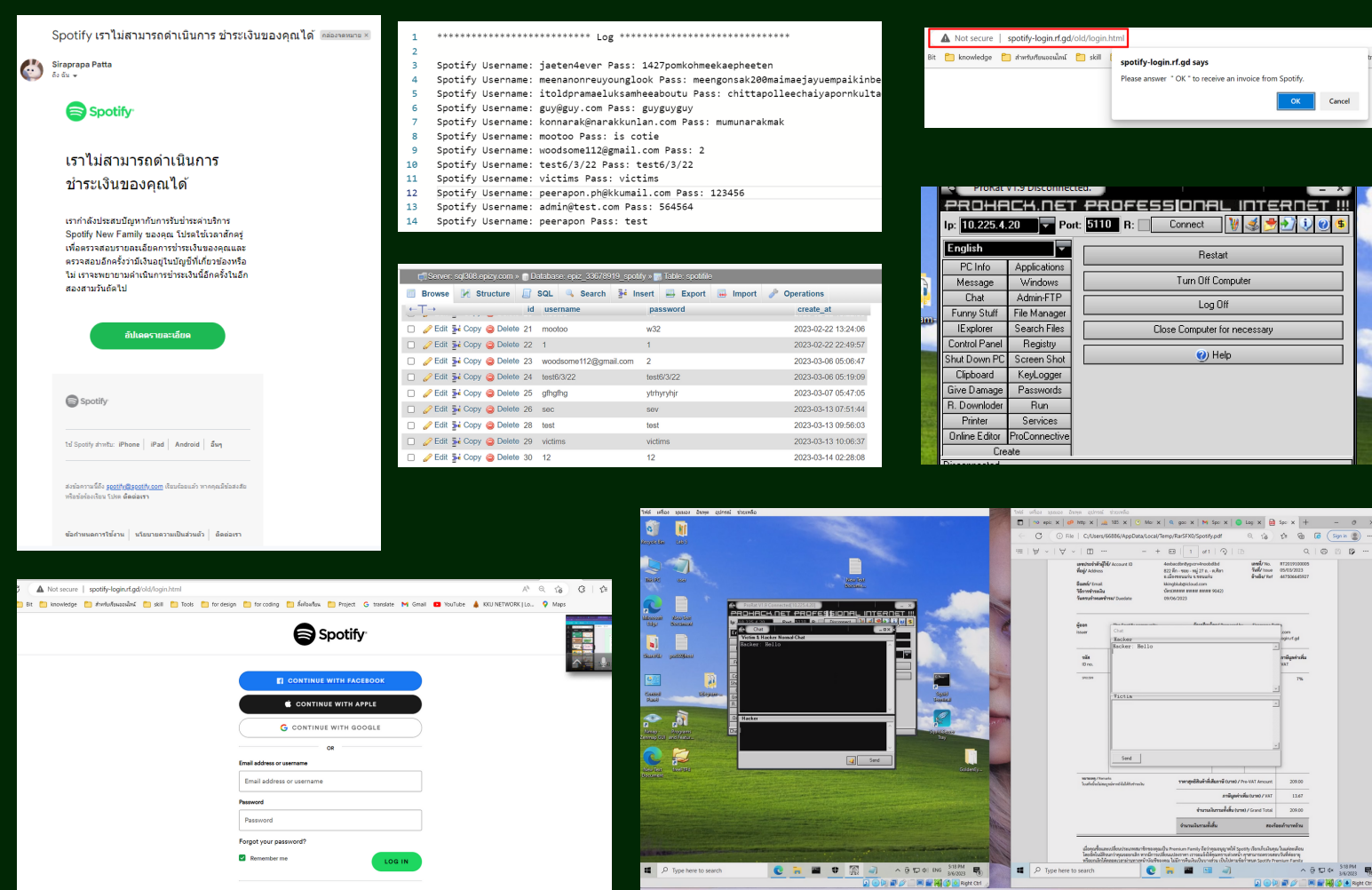


Borat-RAT

ขอบเขตการศึกษา

1. ศึกษาการใช้งานบริการ Hosting+ฐานข้อมูล
2. ศึกษาการโจมตี Trojan&Phishing

ตัวอย่างงาน



ATTACKER

VICTIMS

วิธีการใช้งาน

ทำการส่งอีเมลแจ้งค่าค่างชำระค่าบริการ Spotify พร้อมแนบปุ่มกดดูรายละเอียด เมื่อเหยื่อคลิกเปิดลิงก์ จะแสดงหน้าเว็บไซต์ Login ขึ้นมาให้กรอก username และ password และ popup ให้ดาวน์โหลดไฟล์(.pdf)ในแจ้งหนี้ ซึ่งเป็นหน้าphishingปลอมที่สร้างขึ้น มา เมื่อเหยื่อกรอกข้อมูลและกดปุ่ม Login จะเป็นการส่งข้อมูลที่เหยื่อกรอก เก็บไว้ที่ฐานข้อมูล และ.txtไว้ ขณะเดียวกันเมื่อเหยื่อเปิดไฟล์pdfในแจ้งหนี้ ซึ่งเป็นไฟล์.pdfปลอม จะเป็นการรันไฟล์ execute Trojan โดยที่เครื่องผู้ใช้ถูก phishing และถูกโจมตี ในรูปแบบ Trojan&Phishing ในเวลาช่วงเวลาใกล้ๆกัน

ผู้จัดทำ SEC 2 GROUP 15

- | | |
|------------------------------|-----------|
| 643020351-9 นางสาวกัลยารัตน์ | แก้วสำราญ |
| 643020352-7 นางสาวกาลแก้ว | อ่อนหวาน |
| 643020386-0 นายบรรณาวุฒิ | ดาหยา |
| 643020415-9 นางสาวศิริประภา | ปัตตะ |
| 643021109-1 นางสาวนิภา | สินโรสง |
| 643021113-0 นายพีรพา | โพร์คำ |

สรุปผลการดำเนินงาน

จากงานข้างต้นเป็นการสร้างหน้าเว็บไซต์ปลอมขึ้นมาเพื่อดัก phishing แล้วทำการส่งอีเมลโดยแนบปุ่มเพื่อลิงเว็บไซต์ปลอมไว้ในเว็บไซต์เมื่อผู้ใช้งานดาวน์โหลดไฟล์และเปิดไฟล์จะทำการติดตั้งโปรแกรมโทรจันและสามารถเข้าควบคุม โจมตี หรือดักฟังเครื่องของเหยื่อได้

เอกสารอ้างอิง:

- https://csperson.kku.ac.th/chakchai/images/342376_2022/4.pdf?fbclid=IwAR2iLSVfez6gpyOUW6bKR2hVKKM8UEQMOKcmgzX5Fc33uOLqFNVoOnQpcCQ
- https://csperson.kku.ac.th/chakchai/images/342376_2020/8.pdf?fbclid=IwAR3THbYmI--Oa-MINxpH4DG_6WvuHr0X9AFpQY5q40QZGsIetg21LHI-cjQ