PROJECT TROJAN 342 376

หลักการและเหตุผล

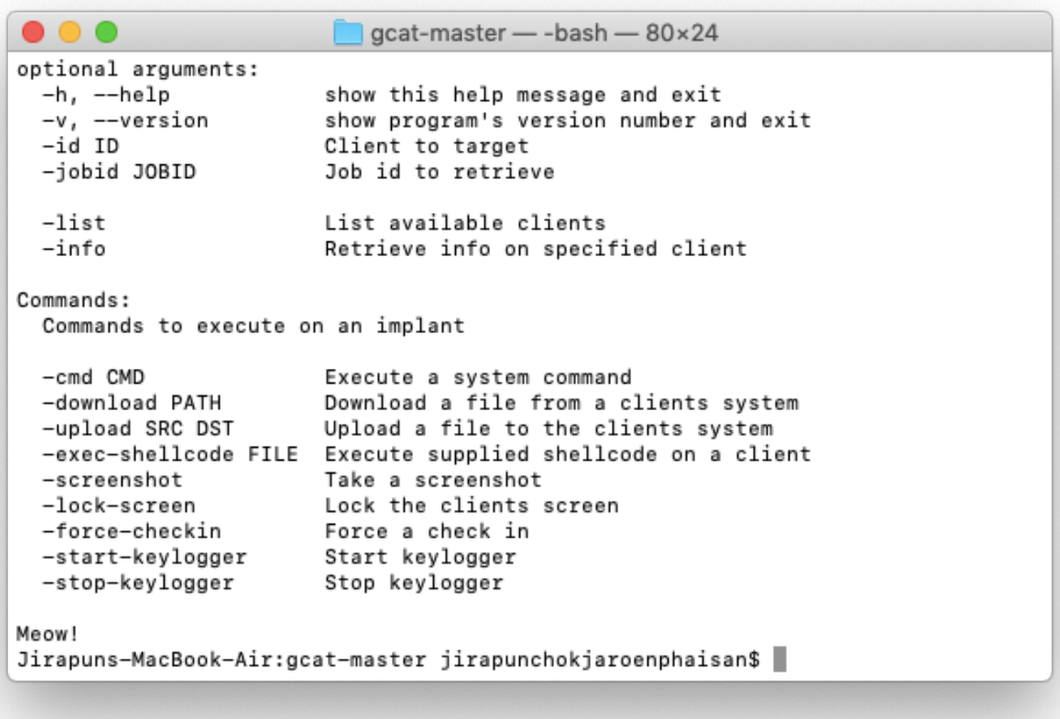
ในยุคปัจจุบันภัยคุกคามไซเบอร์มีมากมายหลายประเภท ไม่ว่าจะเป็น Ransomware, Web Attacks, Phishing หรือ DDoS แต่การโจมตีแบบไหนล่ะที่ส่งผลกระทบร้ายแรงมากที่สุด ซึ่งทางผู้จัดทำคำนึงถึงปัญหาและความสำคัญของภัยคุกคามทางไซเบอร์และต้องการศึกษาเกี่ยวโทรจัน (Trojan) ที่เป็นมัลแวร์อีกชนิดที่พบเห็นการแพร่ระบาดได้ทั่วไป มีลักษณะและพฤติกรรมไม่แพร่เชื้อไปติดไฟล์อื่นๆ

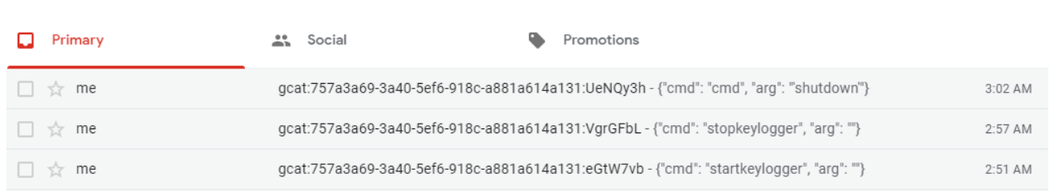
วัตถุประสงค์

1.ใช้เพื่อการศึกษาเกี่ยวกับ Computer Security เท่านั้น
2. เพื่อศึกษาวิธีการทำงานของ Trojan
3. เพื่อรู้และเข้าใจตระหนักถึงภัยคุกคามทางคอมพิวเตอร์
** ทางผู้จัดทำทราบดีเกี่ยวกับกฎหมาย พรบ.คอมพิวเตอร์
ไม่มีการนำไปใช้จริงหรือนำไปดึงข้อมูลจากผู้อื่นแต่อย่างใด
ใช้เพื่อการศึกษาเท่านั้น **

ขั้นตอนการทำงาน

1.แก้โค้ดใส่ Gmail และ รหัส gmail ที่ต้องการให้ส่งข้อมูลกลับมา
2.นำไฟล์ backdoor ไปปล่อยไว้ที่เครื่องเหยื่อ
3.เชค Gmail เพื่อดูว่า backdoor สามารถใช้งานได้
4.รันไฟล์ Server ใช้ -list เพื่อรับ id และเชคว่าไฟล์สารถทำงานได้
5.เปิดไฟล์ server สั่งงานผ่าน Cmd ตัวอย่าง -id ID -screenshot





ความสามารถ

1.สามารถเซฟหน้าจอของเหยื่อด้วยคำสั่ง -screenshot
2.สามารถดูเครื่องเหยื่อผมพิมพ์อะไร ด้วยคำสั่ง -start-keylogger
3.สามารถล็อคหน้าจอด้วย -lock-screen
4.สามารถสั่งงาน cmd ด้วยคำสั่งทั่วไป เช่น -cmd dir

เครื่องมือที่เกี่ยวข้อง

Gmail

Python

Reference

- https://www.youtube.com/watch?v=C7HESFRTLvo
- https://github.com/byt3bl33d3r/gcat/releases/tag/1.0.0
-https://www.mangoconsultant.com/th/news-knowledge/knowledge
https://www.gotoknow.org/posts/622755

จัดทำโดย

Section 3 Group 20
603021367-5 จิรพันธ์ โชคเจริญไพศาล
603021383-7 ธนพล กาฬปักษ์
603021398-4 ศิกานต์ สิงหาชารี
603021401-1 สิรวิชญ์ ทินแท่น
603021193-2 จีรพัฒน์ แก้วศรีสุข
603021224-7 ยศธร ศาสตรี

อาจารย์ที่ ปรึกษา รศ.ดร.จักรชัย โสอินทร์

เป็นส่วนหนึ่งของการศึกษาวิชา 342 376
Information and CommunicationTechnology Security
ภาคเรียน 2 ปีการศึกษา 2561
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์