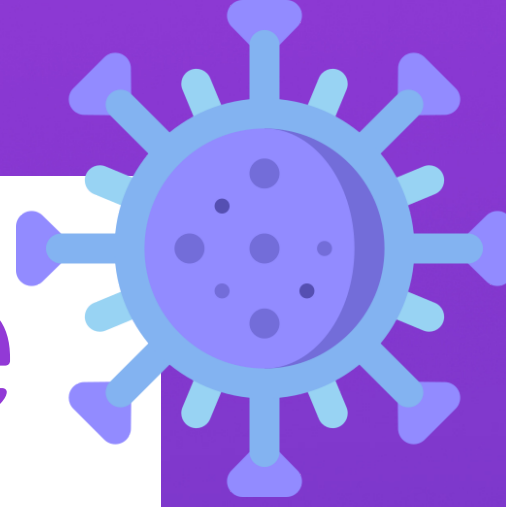


# Spy Everywhere

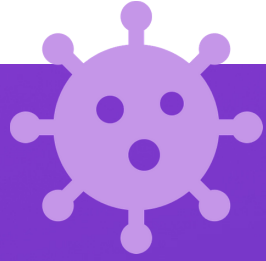
342376 Information and Communication Tachnology Security



## ขั้นตอนการทำงาน

- 1.เปิดโปรแกรม ngrok เพื่อสามารถเข้าใช้แอปพลิเคชันของเรา ผ่านเครื่องที่รันอยู่บน localhost ได้
- 2.เปิดโปรแกรม njrat เพื่อสร้างตัวไฟล์ไวรัสขึ้นมา แล้วส่งให้เหยื่อผ่าน Google Drive
- 3.พอเหยื่อดาวน์โหลดไฟล์ ก็จะไปสู่กระบวนการทำงานไวรัส
- 4.สั่งการทำงานผ่านโปรแกรม njrat เช่น Capture Desktop, Capture Webcam

## หลักการและเหตุผล

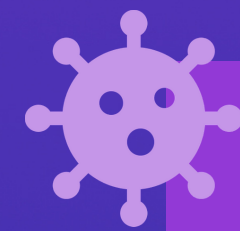
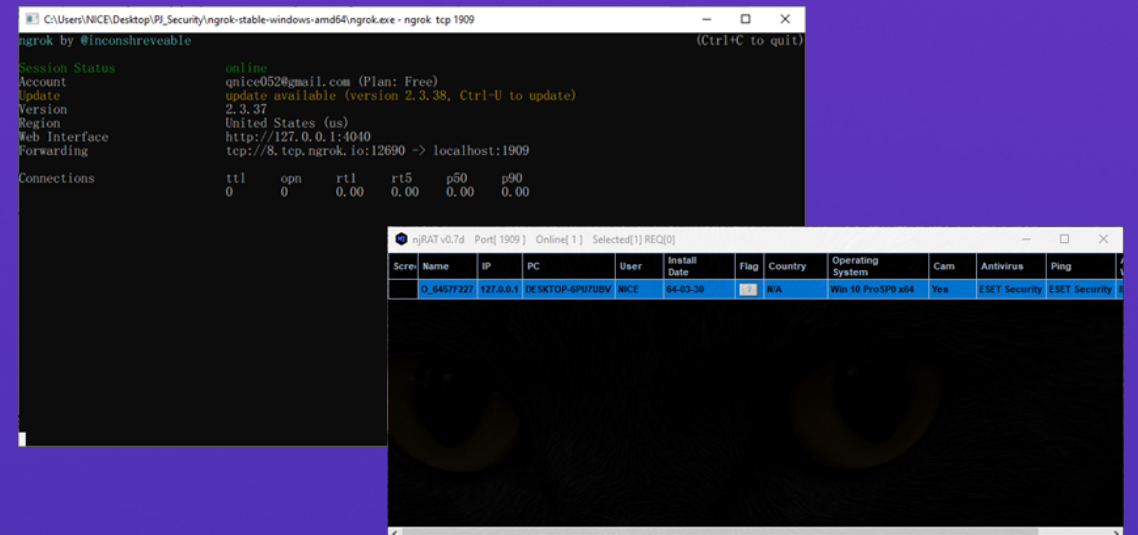


NJRat เป็นหนึ่งในภัยคุกคามเครื่องคอมพิวเตอร์อีกประเภทหนึ่งที่อันตรายมาก เมื่อติดตั้งเสร็จโปรแกรมก็จะเข้าถึงเครื่องคอมพิวเตอร์โดยปราศจากความยินยอม หลังจากติดตั้งเสร็จแล้ว ก็สามารถดำเนินการตามฟังก์ชันของตัวโปรแกรมได้

## วัตถุประสงค์



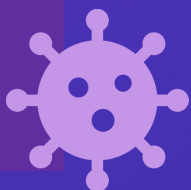
- 1.เพื่อศึกษาการใช้งานโปรแกรม NJRat
  - 2.เพื่อศึกษาและพัฒนาโปรแกรม NJRat
  - 3.เพื่อศึกษาวิธีการป้องกันการโจมตีของโปรแกรม NJRat
- \*\*ทางผู้จัดทำทราบดีเกี่ยวกับกฎหมาย พรบ.คอมพิวเตอร์ ไม่มีการนำไปใช้จริงหรือดึงข้อมูลจากผู้อื่นแต่อย่างใด ใช้เพื่อการศึกษาเท่านั้น\*\*



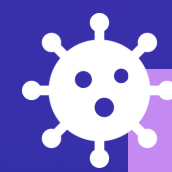
## สรุป

เมื่อเหยื่อทำการดาวน์โหลดไฟล์ในอีเมลลงเครื่องเรียบร้อยแล้ว ตัวโปรแกรมจะทำการควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ ไม่ว่าจะเป็นการเปิดกล้องพิมพ์คีย์บอร์ดก่อนเหยื่อ และดักฟังเสียงหรือขโมยรหัสผ่าน

## ผลการดำเนินงาน

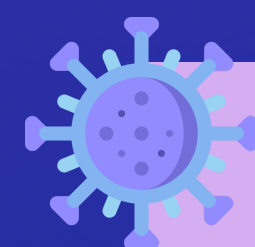


- 1.ดึงดูไฟล์ แก้ไขไฟล์หรืออัปโหลดไฟล์เข้าเครื่องเหยื่อ
- 2.รันไฟล์ผ่านเครื่องของเราเพื่อโจมตีเหยื่อ
- 3.บันทึกหน้าจอเดสก์ท๊อป เว็บแคมและการกดแป้นพิมพ์
- 4.ขโมยรหัสผ่านที่บันทึกไว้ในเบราว์เซอร์หรือแอปพลิเคชันอื่นๆ
- 5.เปิดหน้าต่างท๊อปหรือหน้าต่างที่ใช้งานอยู่ของเหยื่อ
- 6.ดักฟังเสียงผ่านไมโครโฟนของเครื่องเหยื่อ



## อ้างอิง

<https://github.com/AliBawazeEer/RAT-NjRat-0.7d-modded-source-code>  
<https://ngrok.com/docs>



จัดทำโดย  
Section3 Group18

## เครื่องมือที่เกี่ยวข้อง



- 623021071-8 นางสาวเกตุมณี ศรีสงสาร
- 623021091-2 นางสาวสิริวิมล เพชรเวียง
- 623021151-0 นางสาวศิวรตี มัญจางษ์
- 623021177-2 นายจิรพัฒน์ แก้วศรีสุข
- 623021178-0 นางสาวชนิภา สุธระณะนัย
- 623021181-1 นายยศธร ศาสตร์