



Red Trojan

Group 2

หลักการและเหตุผล

เมื่อผู้ใช้ทำการติดตั้งโปรแกรมของเรา Red Trojan จะซ่อนตัวอยู่ในเครื่องของเหยื่อ ทำการแอบแฝง พยายามเข้าถึงคอมพิวเตอร์และนำไปสู่การโจรกรรมข้อมูลในที่สุด

ทั้งนี้ก็เพื่อเป็นการสาธิตและแสดงให้เห็นถึงความอันตรายจากการใช้คอมพิวเตอร์ของผู้ใช้โดยไม่คำนึงถึงความปลอดภัย

หลักการทำงาน

เมื่อเหยื่อโหลดไฟล์ของเรา และติดตั้งสำเร็จ โปรแกรมก็จะทำงานอัตโนมัติ ทางเราจะสามารถดูว่ามีไฟล์อะไรบ้างในเครื่อง และสามารถลบไฟล์ได้ ดาวน์โหลดมาดูในเครื่องของเราได้

โปรแกรมที่ใช้

python
command

วัตถุประสงค์

1. เพื่อใช้ความรู้ในวิชา ความมั่นคง เทคโนโลยีสารสนเทศและการสื่อสาร มาประยุกต์ใช้
2. เพื่อศึกษาระบบการทำงานของ Trojan และ Backdoor
3. เพื่อศึกษาและตระหนักถึงภัยคุกคามทางคอมพิวเตอร์

ผลการทำงาน

```

C:\Windows\system32\cmd.exe -i 2024-11-08 11:31:11 (885 *192.168.43.26 bit [MS-DOS]) on win32
Type "help" for usage, "quit()" for more information.
>>>

===== REMOTE: C:\Users\aleto\Documents\Server\Server.py =====

Server is currently running @ 192.168.43.26
Waiting for connections...
[*]192.168.43.170, 54689 has connected to the server
View URL => https://www.4mat.com
Custom_dir -> %windir%\system32\cmd.exe
Viewing files...
view_files

Command >> view_dir
Command sent waiting for execution...
Command output: C:\trojan
Command >> custom_dir
Custom_dir: C:/
Command has been sent
Custom_dir Result: ['%SystemRoot%', '%SystemRoot%\system32', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe']
Command >> custom_dir
Command has been sent
Custom_dir: C:/
Command has been sent
Custom_dir Result: ['%SystemRoot%', '%SystemRoot%\system32', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe']
Command >> custom_dir
Custom_dir: C:/Users/aleto
Command has been sent
Custom_dir Result: ['%SystemRoot%', '%SystemRoot%\system32', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe', '%SystemRoot%\system32\cmd.exe']
Custom_dir: C:/Users/aleto

```

สรุป

เมื่อเหยื่อทำการติดตั้งไฟล์ Red Trojan ลงเครื่องคอมพิวเตอร์ Red Trojan จะสามารถควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้ โดยการดูไฟล์ที่มีอยู่ หรือลบไฟล์ออกจากเครื่องคอมพิวเตอร์เหยื่อได้ และสามารถดาวน์โหลดไฟล์ที่ต้องการจากเครื่องคอมพิวเตอร์ของเหยื่อมาได้

Members

623020684-0	นายธราเทพ เกินกลาง
623020956-3	นางสาวชญาดา เอกศิริพงษ์
623020411-5	นายอาร์ทเธอร์ เฉลิมเล่า
623020678-5	นางสาวกิตติพร พิศาลสุทธิกรรม
623020362-2	นางสาวกรมะณี เกศแพ่ง
623020410-7	นางสาวอลิษา ชินกร