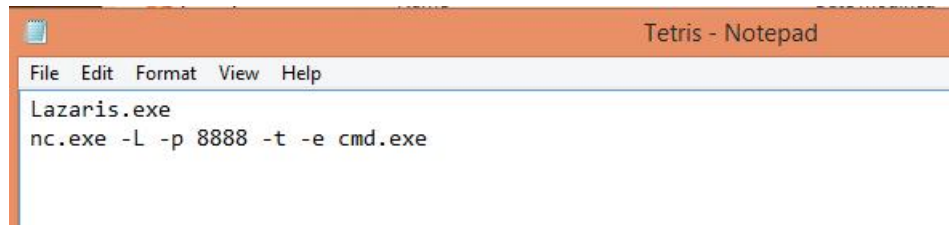


MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỰA
MAHP: CT22202

THỰC HÀNH - AN TOÀN HỆ THỐNG

Bài 04:

* Remote Access Trojans (RATs):



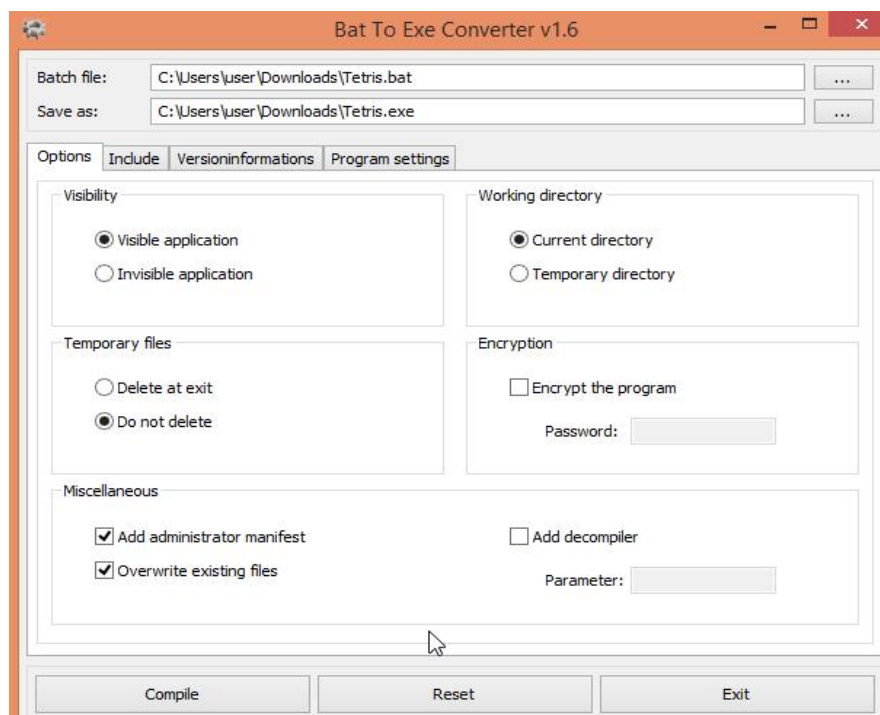
Hình 1: Nội dung kịch bản

- Bước 1: Đóng gói (Wrapper)

Chọn file Tetris.bat lưu thành Tetris.exe

+) Chọn các Options:

- 1) *Visible application*: Cho hiển thị ứng dụng (Nên sử dụng *Invisible application*);
- 2) *Current directory*: Chọn nơi lưu trữ gần nhất;
- 3) *Do not delete*: Không cho xóa dấu vết (Nên sử dụng *Delete at exit*);
- 4) *Add administrator manifest*: Sử dụng với quyền Quản trị;
- 5) *Overwrite existing files*: Cho phép ghi đè lên các file đã tồn tại.



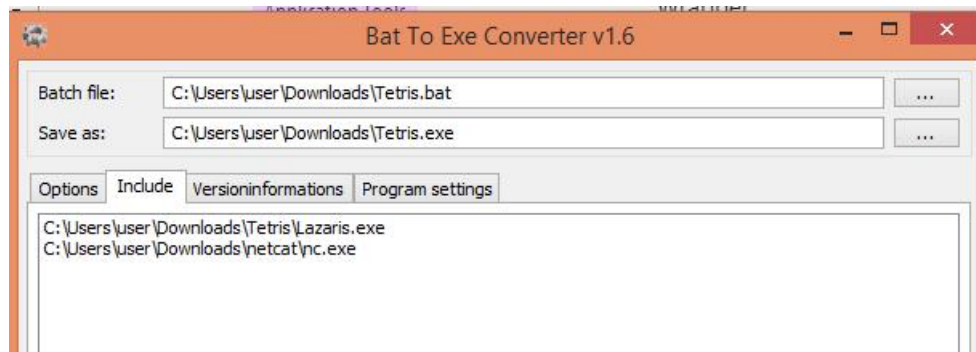
Hình 2: Nội dung Options

MSSV: B1910408

Họ Tên: LÊ THỊ YẾN LỰA

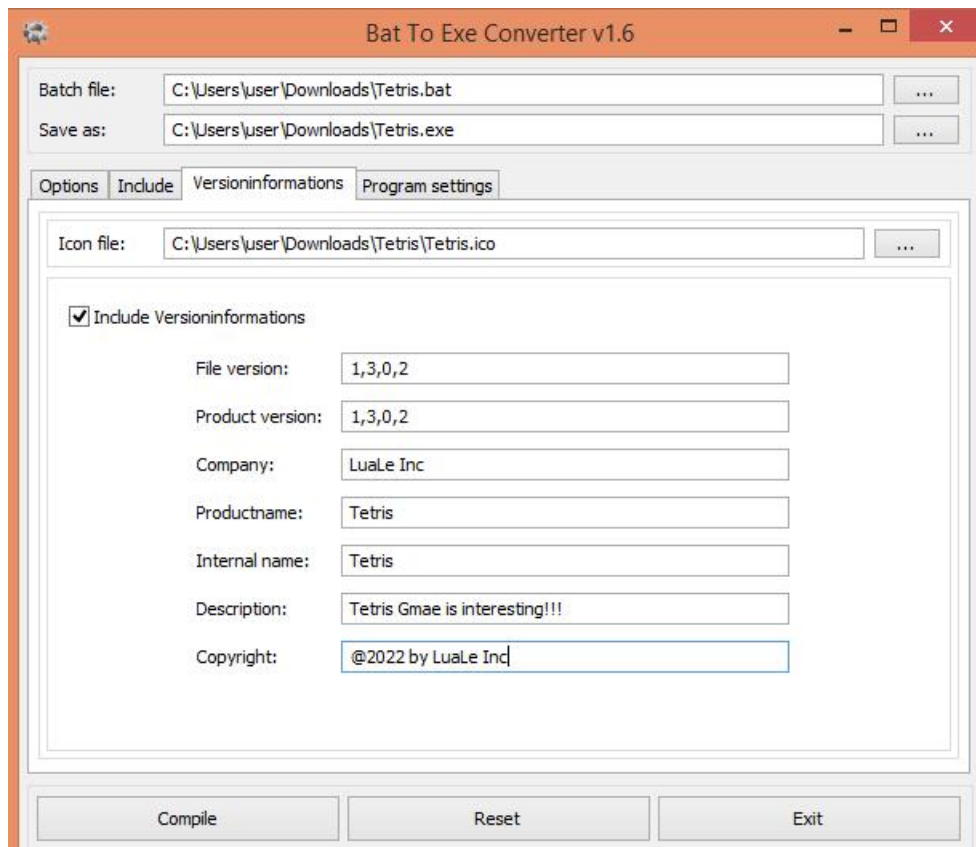
MAHP: CT22202

+) Đóng gói Tetris/Lazaris.exe và netcat/nc.exe:



Hình 3: Nội dung Include

+) Tạo lớp ngụy trang cho ứng dụng:

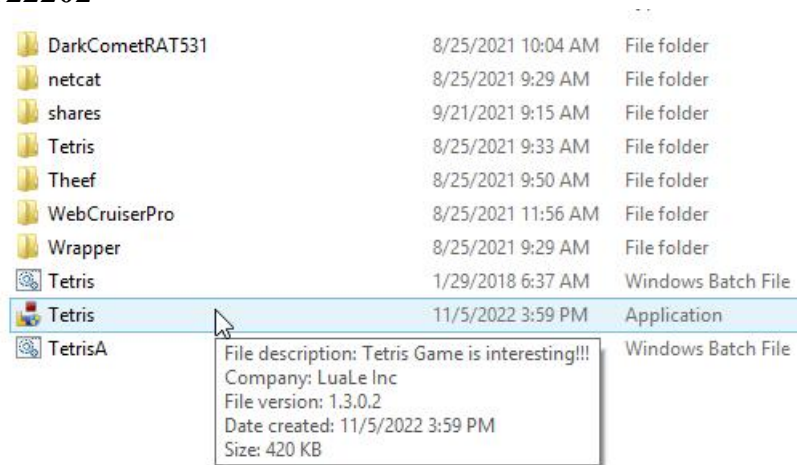


Hình 4: Nội dung Versioninformations

MSSV: B1910408

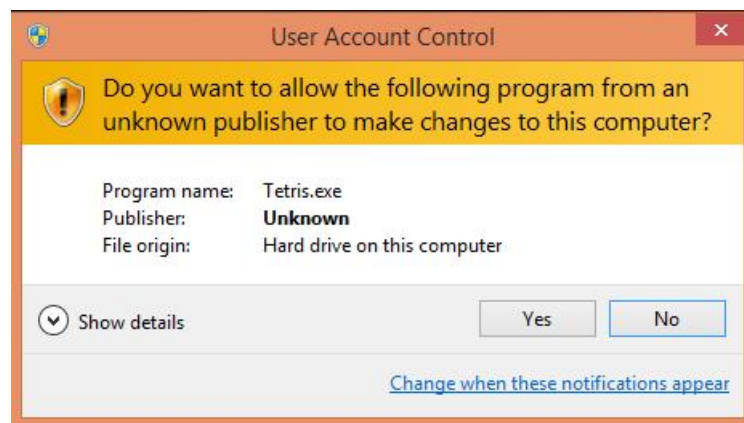
Họ Tên: LÊ THỊ YẾN LỰA

MAHP: CT22202

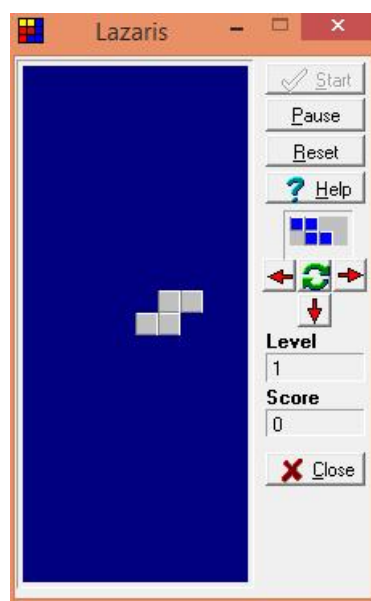


Hình 5: Tạo Game Tetris thành công

- Bước 2: Chạy ứng dụng



Hình 6: Chạy Game Tetris bằng quyền Admin

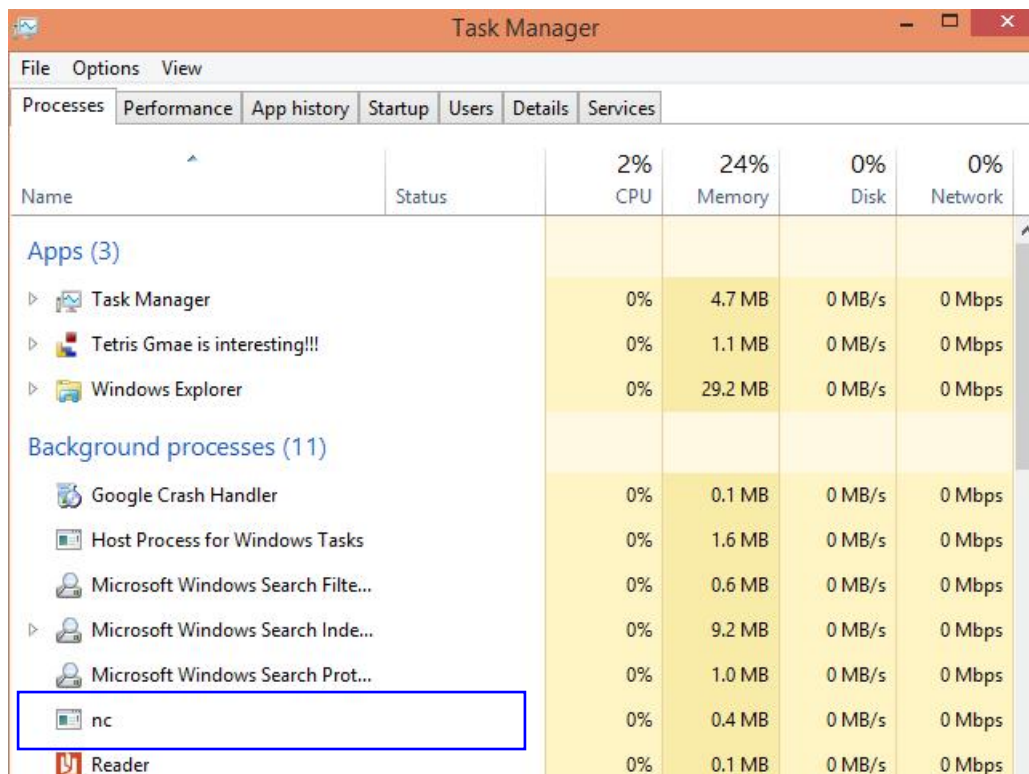


Hình 7: Chạy Game Tetris thành công

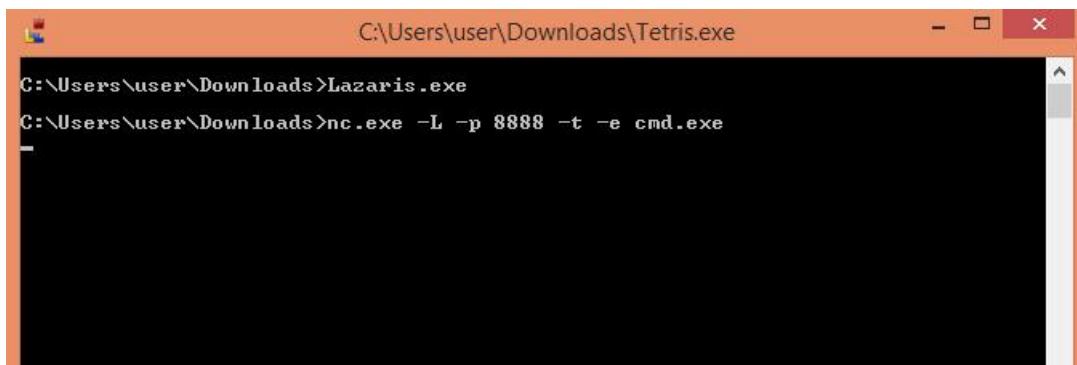
MSSV: B1910408

Họ Tên: LÊ THỊ YẾN LỰA

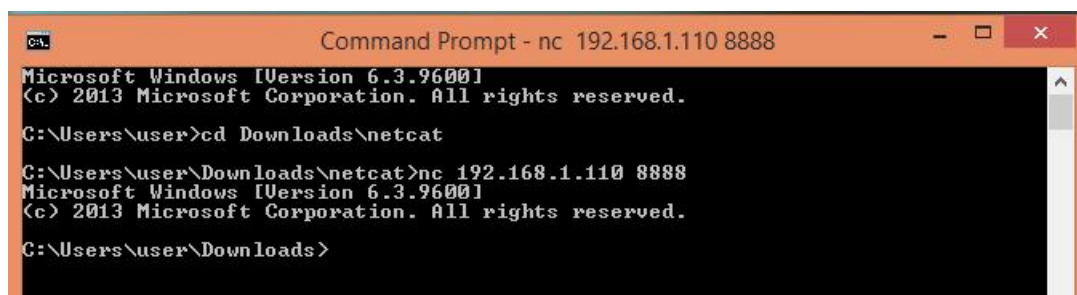
MAHP: CT22202



Hình 8: nc.exe chạy ngầm thành công



Hình 9: Tetris.exe chạy được nội dung kịch bản



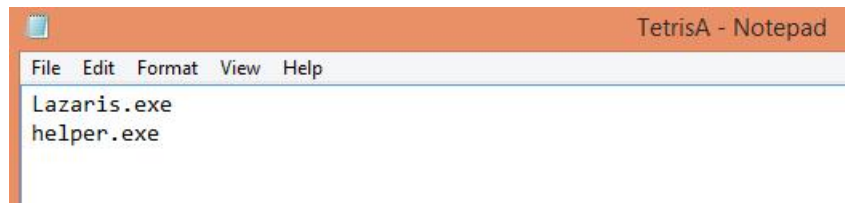
Hình 10: Kết nối với Máy nạn nhân thành công

MSSV: B1910408

Họ Tên: LÊ THỊ YẾN LỰA

MAHP: CT22202

*** Trojan chuyên dụng (Theef):**



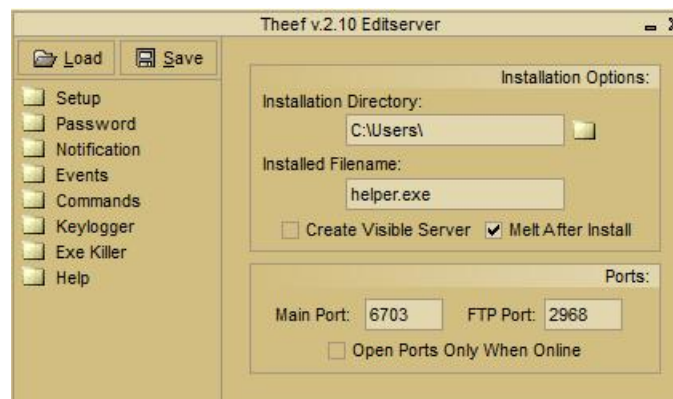
Hình 11: Nội dung kịch bản

- Bước 1: Bắt đầu Editserver

+) Nạp Server210;

- 1) Chọn nơi lưu trữ dễ dàng (máy nào cũng có);
- 2) Đặt tên cho file helper.exe;
- 3) Có cổng sau: 6703;
- 4) Cổng FTP: 2968 (ngẫu nhiên để đánh lừa);
- 5) Server Name: helper;

+) Save: Lưu chỉnh sửa



Hình 12: Nội dung chỉnh sửa



Hình 13: Nội dung chỉnh sửa

MSSV: B1910408

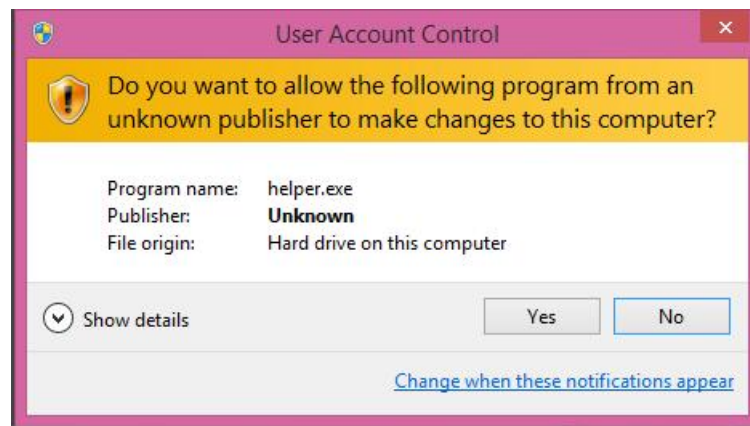
Họ Tên: LÊ THỊ YẾN LỰA

MAHP: CT22202

Name	Date modified	Type	Size
Captures	11/5/2022 8:22 PM	File folder	
cgiparam	3/7/2004 8:25 PM	Configuration sett...	1 KB
Client210	9/8/2014 6:59 PM	Application	522 KB
Editserver210	9/8/2014 6:59 PM	Application	236 KB
helper	11/5/2022 8:27 PM	Application	684 KB
pass.dll	9/8/2014 6:59 PM	Application extens...	42 KB
readme	12/1/2005 10:03 AM	Text Document	4 KB
Scanner.dll	8/23/2002 5:01 PM	Application extens...	60 KB
Server210	11/5/2022 8:27 PM	Application	684 KB
start_network	8/25/2021 9:50 AM	Text Document	1 KB
thief	11/5/2022 8:26 PM	Configuration sett...	1 KB
upx	11/7/2002 5:13 PM	Application	92 KB
zip.dll	10/20/2004 8:44 PM	Application extens...	48 KB

Hình 14: Sao chép và đổi tên Server210

- Bước 2: Chạy ứng dụng



Hình 15: Chạy ứng dụng với quyền Admin

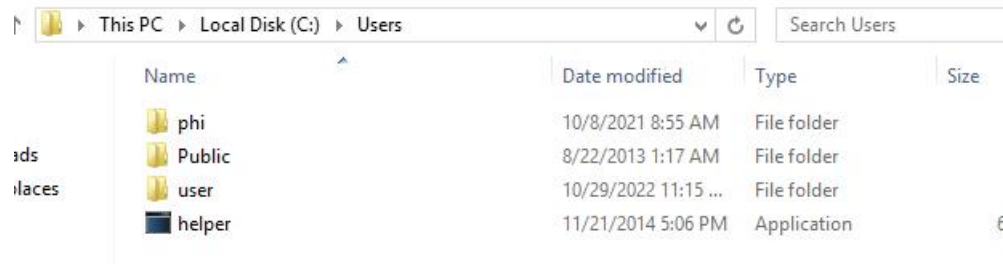
Task Manager					
File Options View					
Processes Performance App history Startup Users Details Services					
Name	Status	23% CPU	25% Memory	0% Disk	0% Network
Apps (2)					
Task Manager		2.7%	4.7 MB	0 MB/s	0 Mbps
Windows Explorer		12.3%	32.7 MB	0.1 MB/s	0 Mbps
Background processes (11)					
Google Crash Handler		0%	0.2 MB	0 MB/s	0 Mbps
helper		0%	1.4 MB	0 MB/s	0 Mbps
helper		0%	1.4 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	1.6 MB	0 MB/s	0 Mbps
Microsoft Windows Search Filte...		0%	0.6 MB	0 MB/s	0 Mbps

Hình 16: helper.exe chạy ngầm thành công

MSSV: B1910408

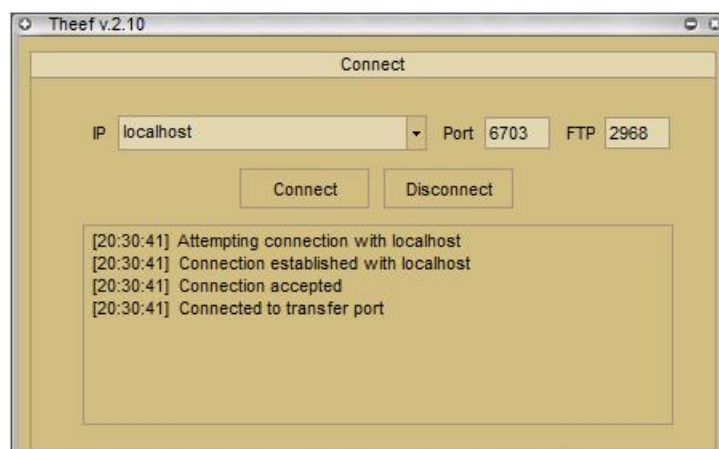
Họ Tên: LÊ THỊ YẾN LỰA

MAHP: CT22202



Hình 17: Ứng dụng helper xuất hiện trong Users

- Bước 3: Chạy Client210 để kết nối đến Máy nạn nhân để đọc dữ liệu, thông tin

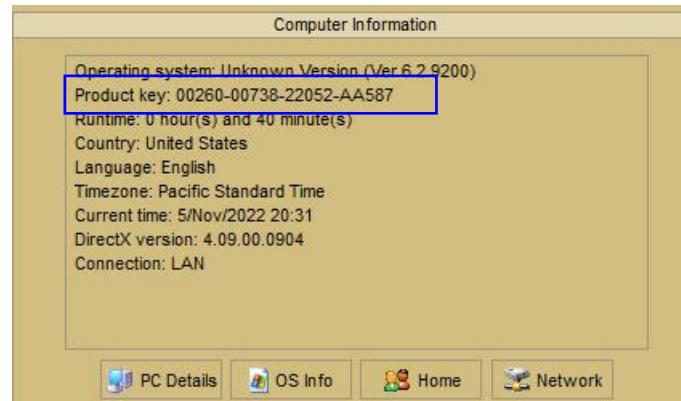


Hình 18: Kết nối thành công

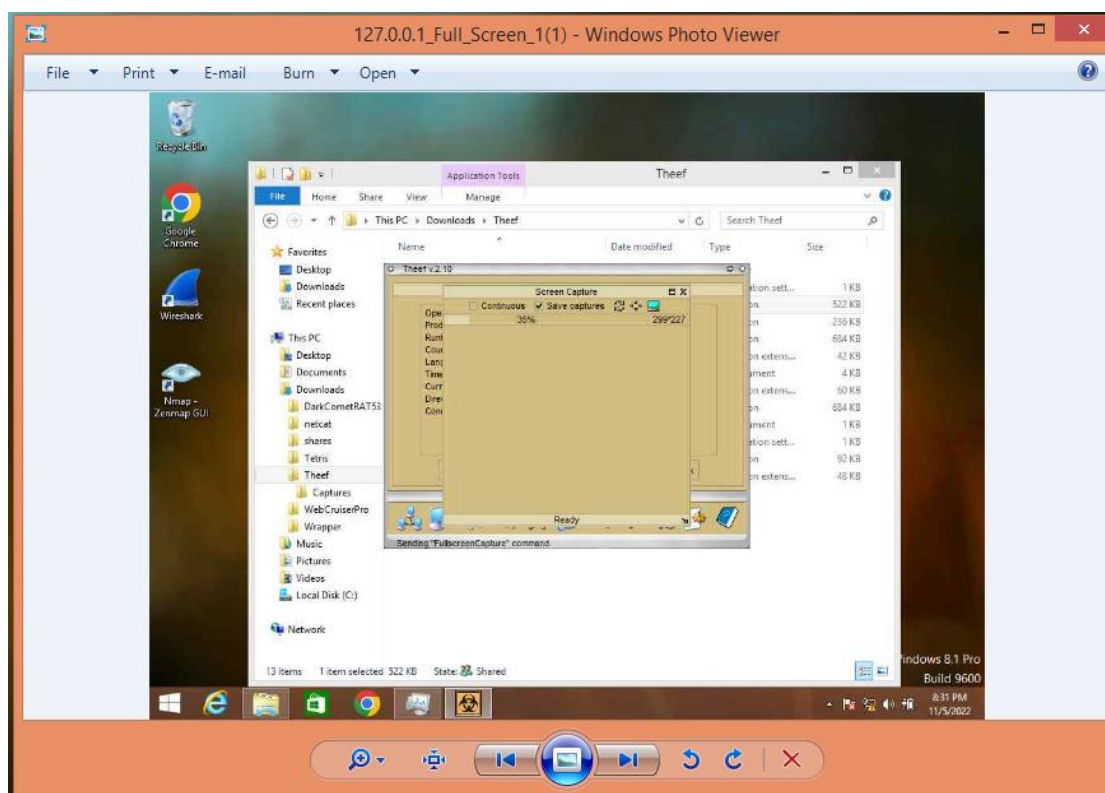


Hình 19: Thông tin chi tiết máy

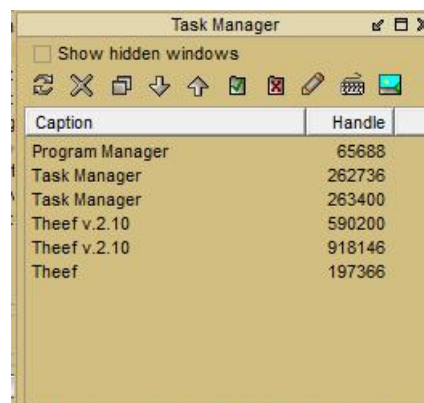
MSSV: B1910408
Họ Tên: LÊ THỊ YẾN Lụa
MAHP: CT22202



Hình 20: Thông tin hệ điều hành

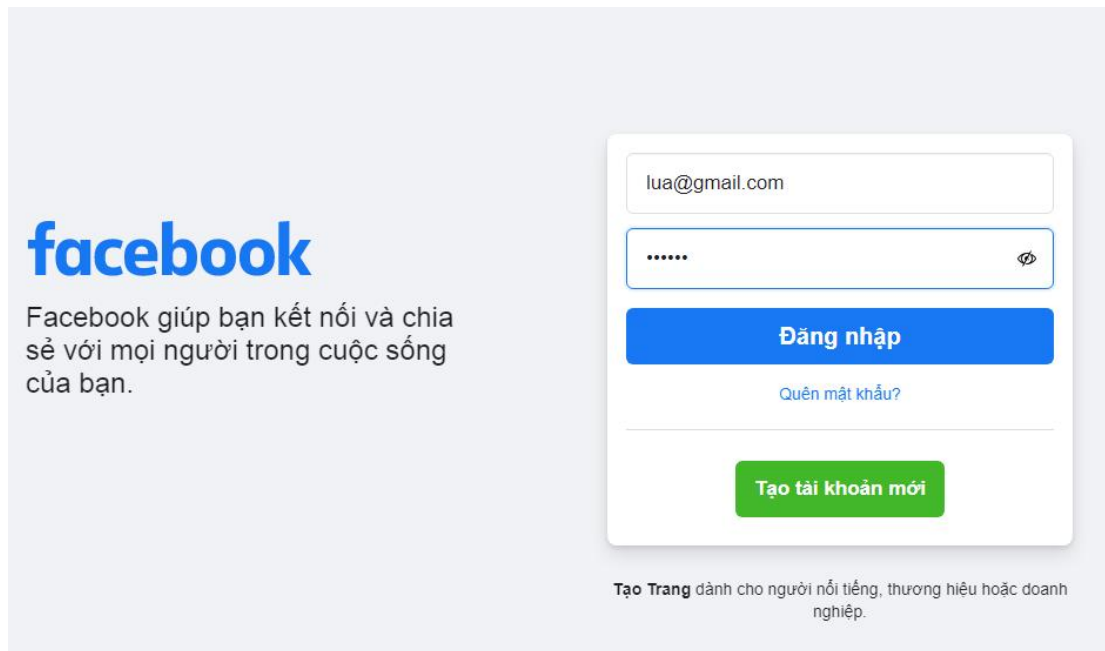


Hình 21: Capture màn hình

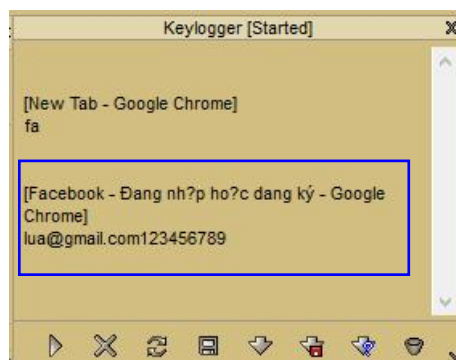


Hình 22: Xem các chương trình đang chạy

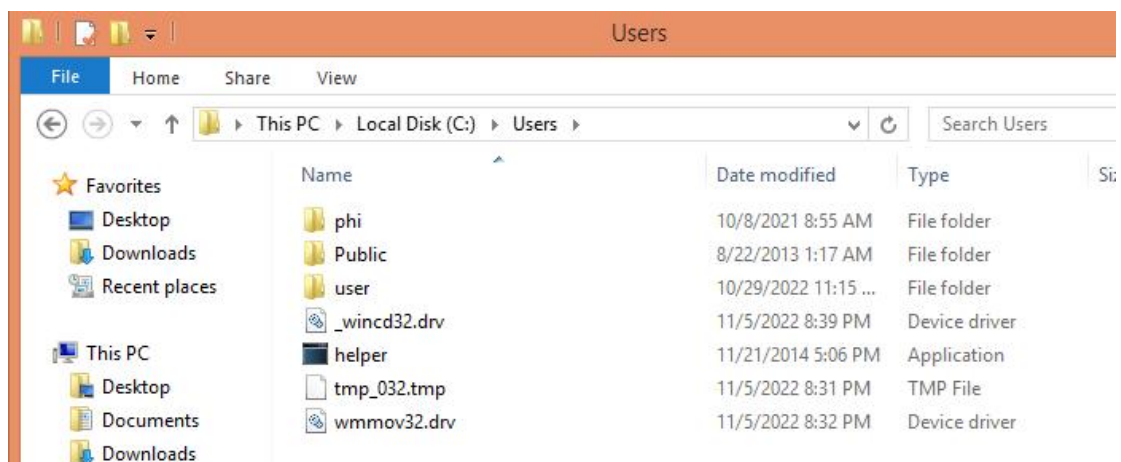
MSSV: B1910408
Họ Tên: LÊ THỊ YẾN LỰA
MAHP: CT22202



Hình 23: Đăng nhập tài khoản Facebook



Hình 24: Bắt được thông tin tài khoản Facebook



Hình 25: Các file độc hại xuất hiện trong Users