

**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP THỰC PHẨM TP.HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

🙜🙢🙠🙞



**Bài lab**

**Bài thực hành 2: Ứng cứu sự cố mã độc mã hóa (ransomware)**

:

1. Nguyễn vũ hoàng phong-2033210960

TP. HỒ CHÍ MINH – 2020

**Thực hành 2: Ứng cứu sự cố mã độc mã hóa (ransomware)**

Tình huống 1:

Một số nhân viên trong hệ thống nhận được mail yêu cầu kiểm tra tài liệu về thuế của

công ty trong năm 2023. Tuy nhiên, tài liệu pdf này đã bị nhiễm mã độc được tạo bằng

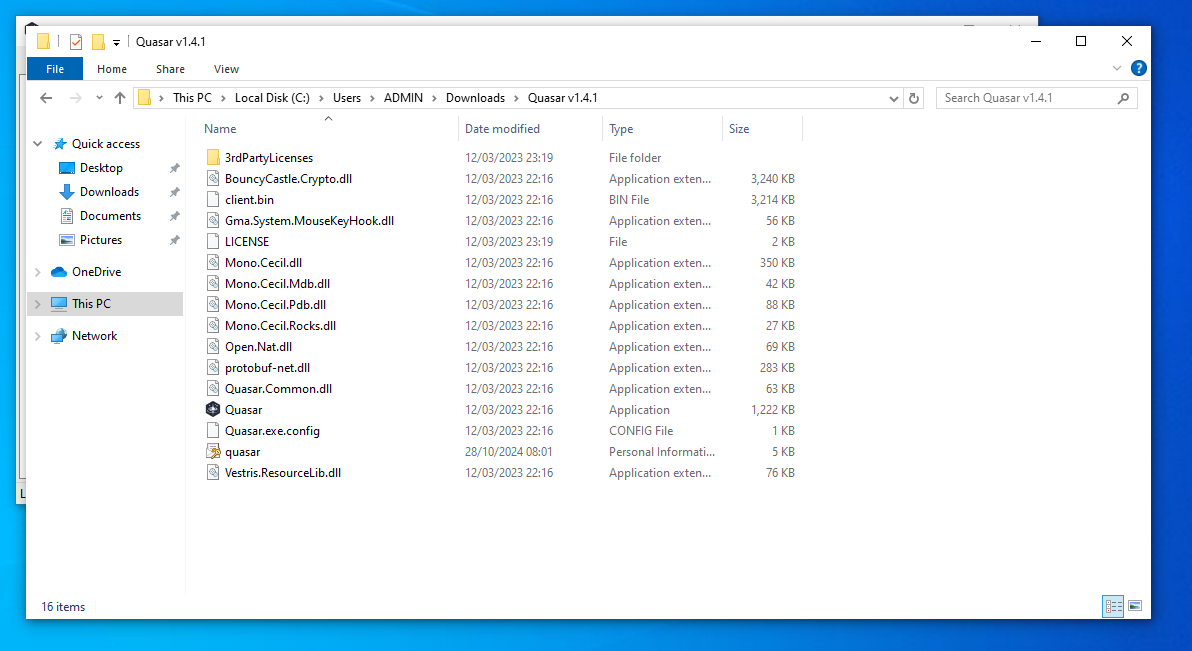
QuasarRAT (link tải https://github.com/YSCHGroup/QuasarRAT). Khi nhân viên mở

file pdf thì sẽ vô tình thực thi mã độc và bị chiếm quyền kiểm soát bởi Attacker.

Thực nghiệm

❖ Tấn công

1. Attacker download tools và sử dụng công cụ Quasar.exe như bên dưới



1. Khi ấn vào Quasar.exe sẽ hiển thị như bên dưới

A screenshot of a computer

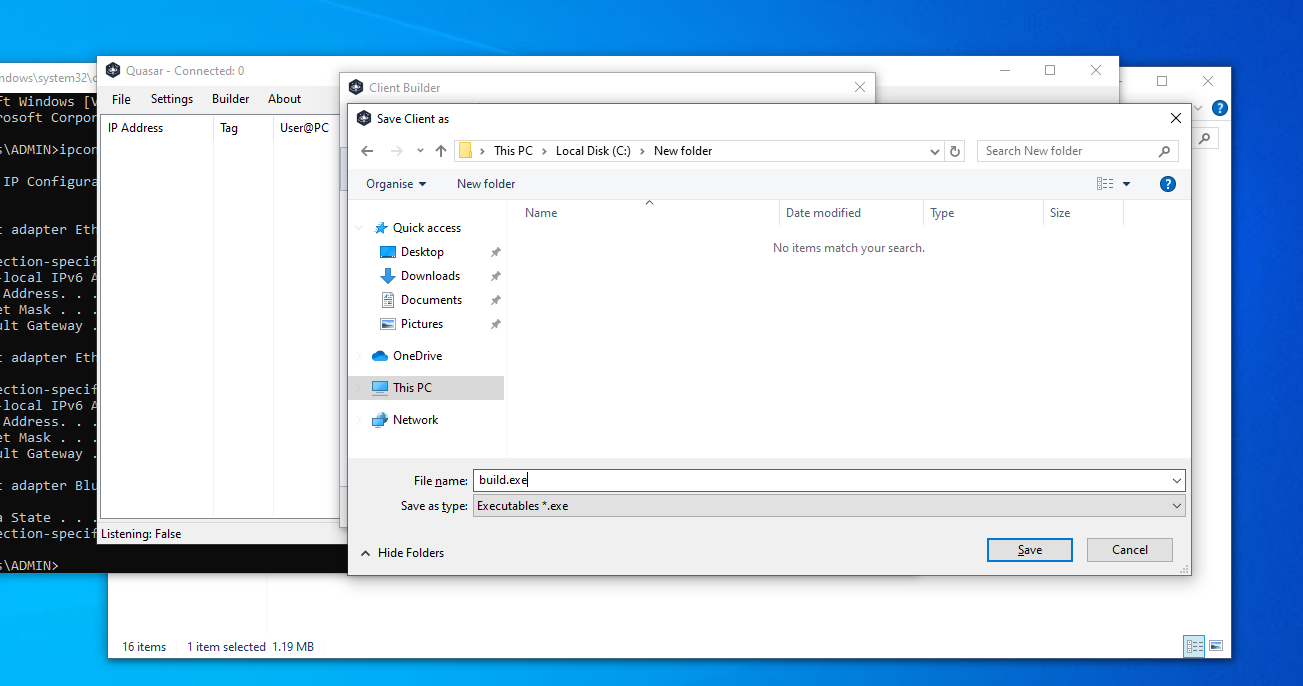
Description automatically generated

1. Trong cửa sổ Client Builder, tại tab Connection Settings. Nhập IP máy Attacker

A screenshot of a computer

Description automatically generated

1. Chọn Build Client và chọn vị trí để lưu file mã độc vừa tạo (build.exe)



1. Sau khi hoàn thành việc build chương trình sẽ hiển thị bảng thông báo build thành công và vị trí lưu file mã độc

A computer screen with a message box

Description automatically generated

1. Quay lại Quasar.exe chọn Settings > chọn Start Listening để lắng nghe trên phía attacker

A screenshot of a computer

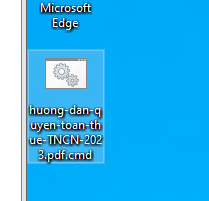
Description automatically generated

1. Attacker tạo file .txt và đổi thành file .cmd (Đây là dạng file thực thi, dạng file này sẽ tự động thực hiện các lệnh trên cmd)

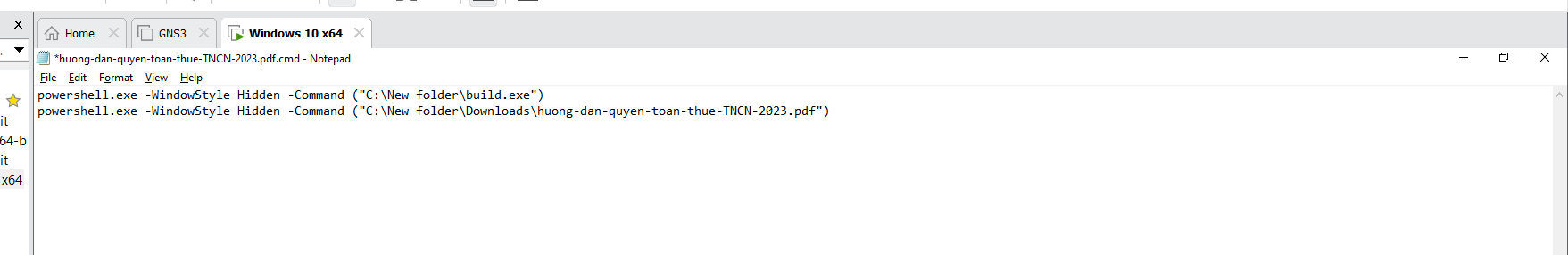
A blue screen with a piece of paper

Description automatically generated

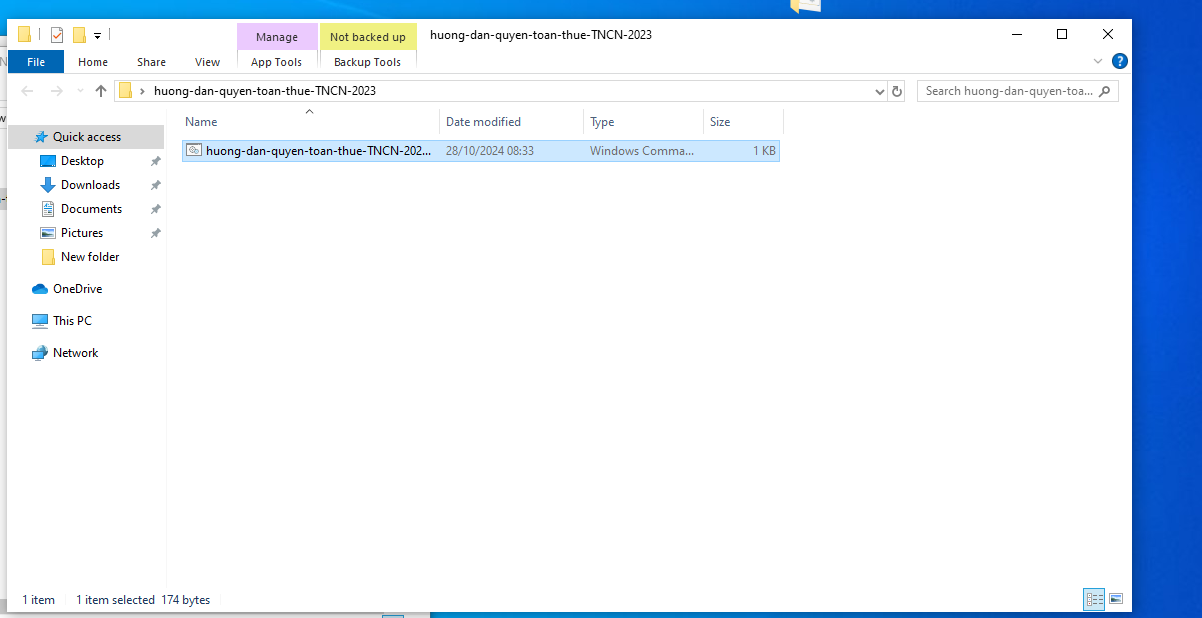
1. Sau khi chuyển đổi thành file .cmd Attacker tiến hành chèn Script



1. Attacker mở file .cmd dưới dạng chỉnh sửa và tiến hành chèn script vào file .cmd như bên dưới



1. Tạo 1 folder chứa file chuyển đổi vừa tạo với tên (Huong-dan-quyet-toan-thue-TNCN-2023)



1. Tạo 1 folder với tên (Thue\_2023)

A computer screen shot of a folder

Description automatically generated

1. Attacker tiến hành đưa folder chứa file chuyển đổi vào folder vừa tạo

A screenshot of a computer

Description automatically generated

13.Attacker tiến hành đính kèm file pdf vào folder (Huong-dan-quyet-toan-thue-

TNCN-2023) để giải nén

A screenshot of a computer

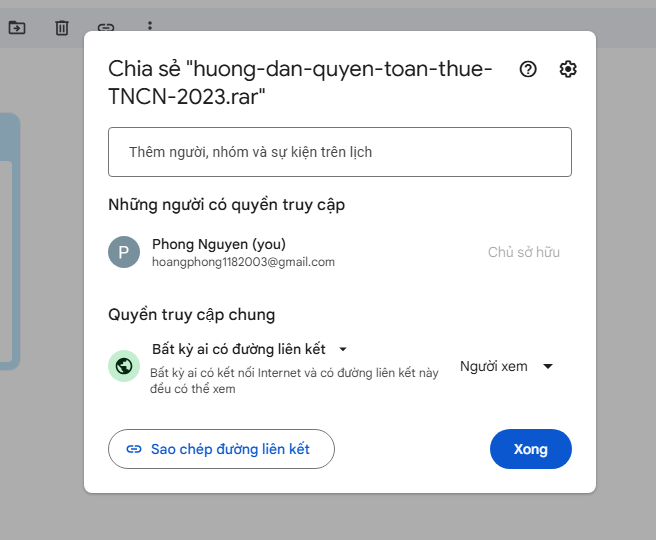
Description automatically generated

1. Dưới đây là kết quả sau khi nén

A screenshot of a computer

Description automatically generated

1. Attacker tiến hành gửi file đã nén cho nạn nhân thông qua ứng dụng mạng xã hội (Gmail, Facebook,...). Thông qua lỗ hổng CVE 2023-40477 cho phép attacker có thể chèn mã độc vào trong winrar đối với các phiên bản winrar 6.23trở xuống.
2. Attacker có thể để file dưới dạng link drive hoặc các dạng khác đáng tin cậy để có thể có thể lừa được nạn nhân.

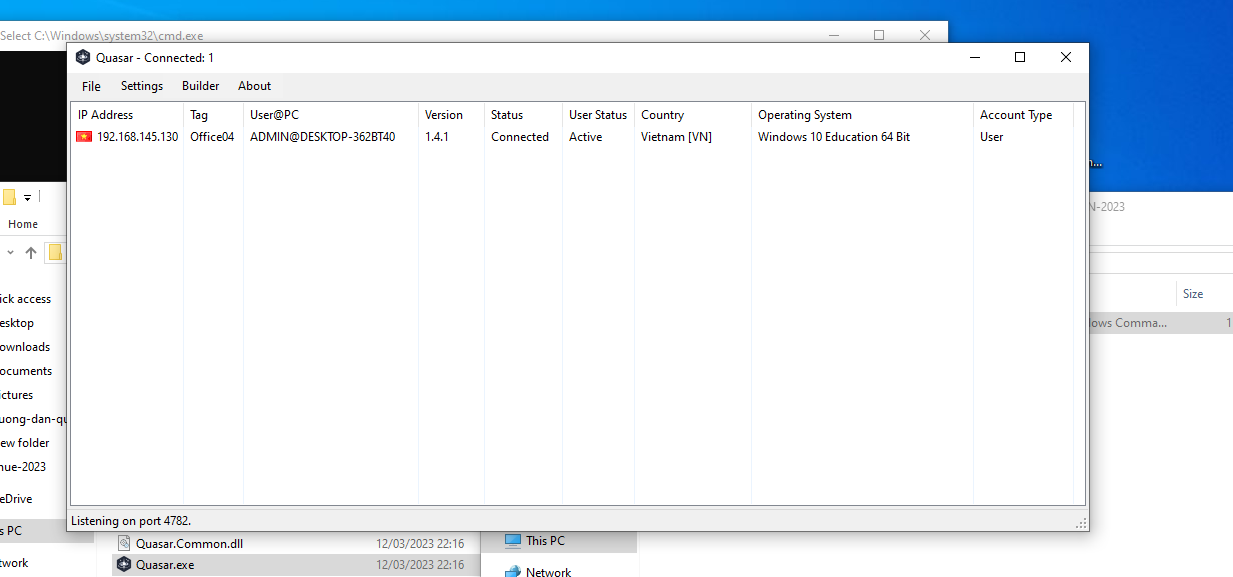


1. Attacker tiến hành gửi mail phishing cho nạn nhân với thông tin (HƯỚNG DẪN THỰC HIỆN QUYẾT TOÁN THUẾ) như bên dưới.

**Bước này em xin bỏ qua vì em dung usb thay cho tình huống gửi mail nhưng vẫn là trong tình huống gửi mail vì sắp hết giờ**

1. Nạn nhân tiến hành mở file pdf để xem nội dung
2. Khi nạn nhân mở file pdf, tình cờ đã thực thi mã độc và tạo 1 kết nối tớiAttacker

**Bước này do em sài 1 máy vừa là attacket vừa thử nghiệm nên ip attacker và máy bị tấn công là 1**

****

1. Các options mà công cụ Quasar cung cấp
2. **Remote Desktop: Cho phép điều khiển máy tính từ xa**

**A screenshot of a computer

Description automatically generated**

**2. Remote Webcam: Cho phép xem webcam từ xa**

**3. Password Recovery: Cho phép khôi phục mật khẩu từ xa**

**4. Keylogger: Cho phép khi lại tất cả các phím được nhấn từ bàn phím**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

Tình huống 2: Một số nhân viên trong hệ thống tỉnh báo cáo tình hình một số máy

tính bị nhiễm mã độc ransomware không thể truy xuất dữ liệu trên ổ đĩa.Máy tính xuất

hiện cảnh báo bằng tiếng Việt và tiếng Anh yêu cầu chuyển tiền đến một tài khoản

Bitcoin thông qua kênh truyền mã hóa TOR để giải mã dữ liệu. Một số mã độc chèn

vào nội dung website, tài liệu và tiến trình thực hiện đào tiền ảo làm quá tải hệ thống.

Lab Environment

➢ Windows 10

➢ Mail Server (Zimbra 8.8.9)