

**ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA CÔNG NGHỆ THÔNG TIN**



**PBL4 - DỰ ÁN HỆ ĐIỀU HÀNH &
MẠNG MÁY TÍNH**

**Phát triển một mã độc (Keylogger/ Botnet) thu thập dữ liệu và
kiểm soát người dùng**

SINH VIÊN THỰC HIỆN:

Giáp Thanh Hữu LỚP: 23T_DT3 NHÓM: 23Nh12B

Đặng Ngọc Gia Bảo LỚP: 23T_DT3 NHÓM: 23Nh12B

Đoàn Đình Hoàng LỚP: 23T_DT3 NHÓM: 23Nh12B

GIẢNG VIÊN HƯỚNG DẪN: Ths Đặng Thiên Bình

MỤC LỤC

CHƯƠNG 1: CƠ SỞ LÝ THUYẾT	7
1.1. TCP/IP là gì? Kiến thức về giao thức mạng TCP/IP	7
1.1.1. TCP/IP là gì?.....	7
1.1.2. Lịch sử giao thức TCP/IP.....	7
1.1.3. Giao thức TCP/IP hoạt động như thế nào?	8
1.1.4. Các tầng của TCP/IP	8
1.1.5. Ưu điểm của TCP/IP	9
1.2. Keylogger	9
1.2.1. Keylogger là gì?.....	9
1.2.2. Cách thức hoạt động của Keylogger.....	10
1.2.3. Phân loại Keylogger.....	10
1.3. Botnet.....	11
1.3.1. Botnet là gì?	11
1.3.2. Mục đích tấn công của Botnet?.....	12
1.3.3. Quy trình hoạt động của Botnet	13
1.3.4. Phân loại Botnet	13
1.3.5. 7 loại tấn công Botnet phổ biến hiện nay [4]	13
1.3.6. Giải pháp phòng vệ Botnet FortiGuard.....	16
1.4. Hệ điều hành	16
1.5. Remote Desktop (RDP)	17
1.6. Window defender.....	17
CHƯƠNG 2: THIẾT KẾ VÀ XÂY DỰNG HỆ THỐNG	19
2.1. Tổng quan chức năng chính của hệ thống	19
2.1.1. SystemInfo (Thông tin hệ thống)	19
2.1.2. Remote Shell (Shell từ xa).....	19
2.1.3. File Manager (Quản lý tệp tin)	19
2.1.4. Keylogger (Ghi lại phím).....	19

2.1.5. Task Manager (Quản lý tiến trình)	19
2.1.6. Remote Desktop (Màn hình từ xa).....	20
2.2. Các thành phần của hệ thống	20
2.2.1. Botnet Client (Nạn nhân Botnet)	20
2.2.2. Botnet Server (Máy chủ Botnet)	20
2.2.3. Triển khai chi tiết hệ thống	21
CHƯƠNG 3: DEMO ÚNG DỤNG VÀ ĐÁNH GIÁ KẾT QUẢ.....	41
3.1. Kết quả thực thi của chương trình	41
3.1.1. Giao diện quản lý chung	41
3.1.2. Giao diện các chức năng hệ thống	41
3.1.3. Giao diện các chức năng theo dõi hệ thống	42
3.1.4. Giao diện các chức năng người dùng.....	42
3.1.5. Giao diện các chức năng client	43
3.1.6. Giao diện thông tin hệ thống.....	44
3.1.7. Giao diện quản lý tệp tin.....	44
3.1.8. Giao diện các tác vụ	45
3.1.9. Giao diện shell từ xa	46
3.1.10. Giao diện Keylogger	46
3.1.11. Giao diện Remote Desktop	47
3.1.12. Giao diện hiển thị thông báo	48
3.2. Kết quả của việc vượt qua sự kiểm tra của Window Defender	49
3.3. Đánh giá kết quả	50
CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN.....	51
4.1. Kết luận.....	51
4.2. Hướng phát triển	51

DANH SÁCH HÌNH ẢNH

Hình 1: So sánh giữa OSI và TCP/IP	8
Hình 2: Quy trình hoạt động của Botnet.....	12
Hình 3: Quy trình phân tán	14
Hình 4: Quá trình phát tán dữ liệu	16
Hình 5: Quy trình hoạt động Remote Desktop	17
Hình 6: Kết nối mạng.....	22
Hình 7: Sơ đồ hoạt động của System Information.....	23
Hình 8: Sơ đồ hoạt động Remote Shell	24
Hình 9: Sơ đồ hoạt động File Management.....	25
Hình 10: Sơ đồ hoạt động GetDrivesPacket.....	26
Hình 11: Sơ đồ hoạt động GetDirectoryPacket	27
Hình 12: Sơ đồ hoạt động PathRenamePacket	28
Hình 13: Sơ đồ hoạt động PathDeletePacket.....	29
Hình 14: Sơ đồ hoạt động FileTransferRequestPacket.....	30
Hình 15: Sơ đồ hoạt động FileTransferChunkPacket.....	31
Hình 16: Sơ đồ hoạt động của Keylogger.....	32
Hình 17: Sơ đồ hoạt động Task Manager	33
Hình 18: Sơ đồ hoạt động ProcessActionPacket	34
Hình 19: Sơ đồ hoạt động ShowMessengerBoxPacket	35
Hình 20: Sơ đồ hoạt động GetDesktopPacket	36
Hình 21: Sơ đồ hoạt động GetMonitorPacket	37
Hình 22: Sơ đồ hoạt động MouseEvenPacket	37
Hình 23: Sơ đồ hoạt động KeyBoardEventPacket.....	38
Hình 24: Sơ đồ hoạt động ClientReconnectPacket.....	39
Hình 25: Sơ đồ hoạt động AskElavatePacket	40
Hình 26: Sơ đồ hoạt động ShutdownActionPacket	40
Hình 27: Giao diện quản lý chung	41
Hình 28: Giao diện các chức năng hệ thống.....	42

Hình 29: Giao diện các chức năng theo dõi hệ thống.....	42
Hình 30: Giao diện các chức năng người dùng	43
Hình 31: Giao diện các chức năng client.....	43
Hình 32: Giao diện thông tin hệ thống	44
Hình 33: Giao diện quản lý tệp tin.....	45
Hình 34: Giao diện các tác vụ.....	45
Hình 35: Giao diện Shell từ xa	46
Hình 36: Giao diện Keylogger.....	47
Hình 37: Giao diện remote desktop	48
Hình 38: Giao diện hiển thị thông báo.....	48
Hình 39: File trò chơi Pikachu đính kèm mã độc	49
Hình 40: Giao diện trò chơi	49
Hình 41: Mã độc đang chạy ngầm	49

MỞ ĐẦU

Trong thời đại chuyển đổi số diễn ra mạnh mẽ như hiện nay, công nghệ thông tin đã và đang trở thành nền tảng cốt lõi định hình mọi lĩnh vực của đời sống xã hội. Từ kinh tế, giáo dục, y tế cho đến an ninh – quốc phòng, các hệ thống công nghệ thông tin không chỉ giúp tối ưu hóa hoạt động mà còn tạo ra những mô hình mới, phương thức mới để con người làm việc, giao tiếp, học tập và giải trí. Sự bùng nổ của các công nghệ như trí tuệ nhân tạo (AI), blockchain, điện toán đám mây, Internet vạn vật (IoT)... đã mang đến những cơ hội phát triển vượt bậc, đồng thời đặt ra nhiều thách thức về an toàn và bảo mật thông tin.

Song hành với sự phát triển đó, các mối đe dọa mạng cũng ngày càng tinh vi và khó lường hơn. Trong số đó, các loại mã độc (malware) – đặc biệt là Keylogger và Botnet – là những công cụ nguy hiểm thường được tin tặc sử dụng để thu thập thông tin nhạy cảm, chiếm quyền điều khiển hệ thống hoặc tấn công các mục tiêu quy mô lớn. Mã độc không chỉ gây thiệt hại về kinh tế mà còn đe dọa đến sự an toàn dữ liệu, quyền riêng tư của người dùng và tính ổn định của hạ tầng mạng.

Xuất phát từ nhu cầu tìm hiểu sâu hơn về bản chất, cơ chế hoạt động cũng như mức độ nguy hiểm của các loại mã độc phổ biến này, nhóm chúng em thực hiện đề tài “Phát triển một mã độc (Keylogger/ Botnet) thu thập dữ liệu và kiểm soát người dùng”. Mục tiêu của đề tài này là nghiên cứu cách hoạt động của Keylogger, Botnet và giao thức truyền thông TCP/IP – từ đó xây dựng một mô hình minh họa thực tế giúp mô phỏng các hành vi thu thập dữ liệu và điều khiển máy tính từ xa.

Trong quá trình thực hiện, nhóm đã phân tích nguyên lý của giao thức TCP/IP, tìm hiểu cách thức thiết lập kết nối, truyền tải dữ liệu, đồng thời áp dụng vào việc xây dựng một chương trình thử nghiệm có khả năng giao tiếp giữa máy chủ và máy khách. Sản phẩm thu được không nhằm mục đích gây hại, mà là một công cụ mang tính học thuật, phục vụ nghiên cứu, giúp người học hiểu rõ hơn về cách thức mã độc vẫn hành để từ đó có khả năng phòng thủ, phát hiện và xử lý các mối đe dọa tương tự trong thực tế.

Đề tài không chỉ góp phần cung cấp kiến thức về lập trình mạng, bảo mật và hệ thống, mà còn giúp nâng cao nhận thức về tầm quan trọng của việc bảo vệ thông tin trên môi trường số, đặc biệt trong bối cảnh an ninh mạng đang ngày càng trở thành vấn đề cấp thiết toàn cầu.

CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

1.1. TCP/IP là gì? Kiến thức về giao thức mạng TCP/IP [1]

1.1.1. TCP/IP là gì?

TCP/IP hoặc Transmission Control Protocol/ Internet Protocol (Giao thức điều khiển truyền vận/ giao thức mạng) là một bộ các giao thức trao đổi thông tin được sử dụng để kết nối các thiết bị mạng trên Internet. TCP/IP có thể được sử dụng như là một giao thức trao đổi thông tin trong một mạng riêng (intranet hoặc extranet).

Toàn bộ bộ giao thức Internet – một tập hợp các quy tắc và thủ tục – thường được gọi là TCP/IP, mặc dù trong bộ cũng có các giao thức khác.

TCP/IP chỉ định cách dữ liệu được trao đổi qua Internet bằng cách cung cấp thông tin trao đổi đầu cuối nhằm mục đích xác định cách thức nó được chia thành các gói, được gắn địa chỉ, vận chuyển, định tuyến và nhận ở điểm đến. TCP/IP không yêu cầu quản lý nhiều và nó được thiết kế để khiến mạng đáng tin cậy hơn với khả năng phụ hồi tự động.

Có hai giao thức mạng chính trong bộ giao thức mạng phục vụ các chức năng cụ thể.

+ TCP xác định cách các ứng dụng tạo kênh giao tiếp trong mạng. Ngoài ra, nó cũng quản lý cách các tin được phân thành các gói nhỏ trước khi được chuyển qua Internet và được tập hợp lại theo đúng thứ tự tại địa chỉ đến.

+ IP xác định cách gán địa chỉ và định tuyến từng gói để đảm bảo nó đến đúng nơi. Mỗi gateway trên mạng kiểm tra địa chỉ IP này để xác định nơi chuyển tiếp tin nhắn.

1.1.2. Lịch sử giao thức TCP/IP

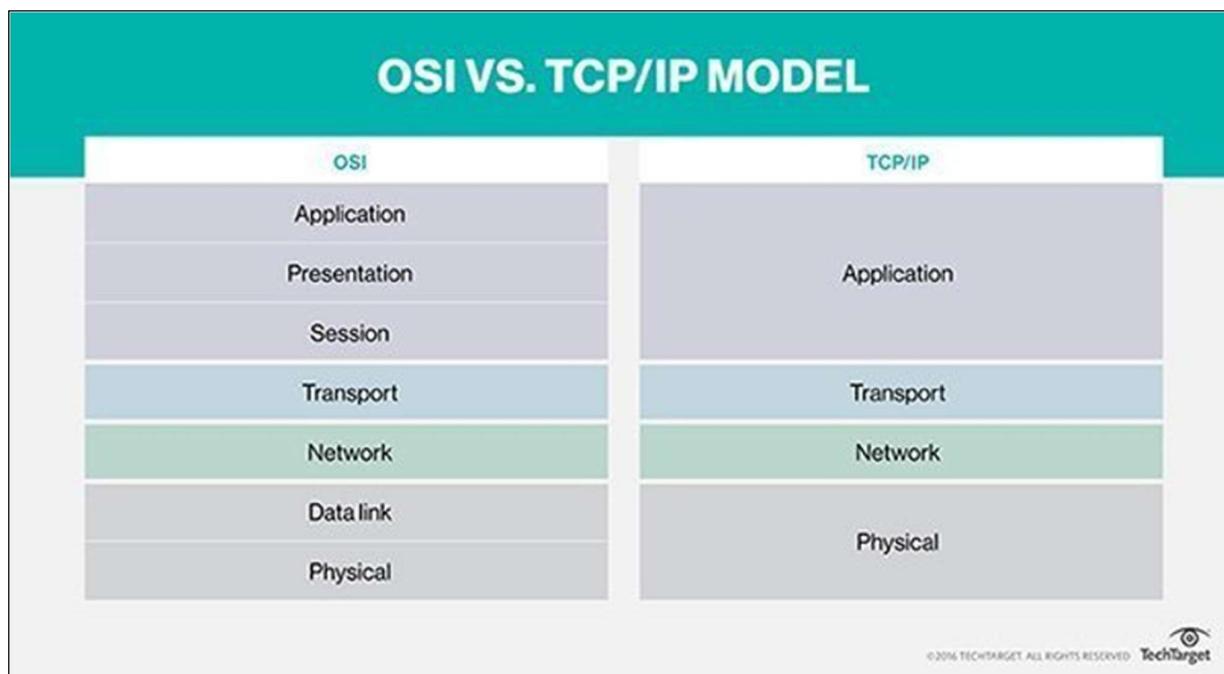
Cơ quan chỉ đạo các dự án nghiên cứu Quốc phòng tiên tiến (Defense Advanced Research Projects Agency – DARPA), chi nhánh nghiên cứu của Bộ Quốc phòng Mỹ, đã tạo ra model TCP/IP trong những năm 1970 để sử dụng trong ARPANET, một mạng diện rộng có trước Internet. TCP/IP ban đầu được thiết kế cho hệ điều hành Unix và được tích hợp vào tất cả các hệ điều hành sau nó. Model TCP/IP và các giao thức liên quan hiện được Internet Engineering Task Force duy trì.

1.1.3. Giao thức TCP/IP hoạt động như thế nào?

TCP/IP sử dụng mô hình giao tiếp máy khách/ máy chủ, trong đó người dùng hoặc thiết bị (máy khách) được một máy tính khác (máy chủ) cung cấp một dịch vụ (giống như gửi một trang web) trong mạng.

Nói chung, bộ giao thức TCP/IP được phân loại là không có trạng thái, có nghĩa là mỗi yêu cầu của máy khách được xem là mới bởi vì nó không liên quan đến yêu cầu trước. Việc không có trạng thái này giúp giải phóng đường mạng, do đó chúng được sử dụng liên tục.

Tuy nhiên, tầng vận chuyển lại có trạng thái. Nó truyền một tin nhắn duy nhất và kết nối của nó vẫn giữ nguyên cho đến khi nhận được tất cả các gói trong tin nhắn và tập trung tại điểm đến.



Hình 1: So sánh giữa OSI và TCP/IP

Mô hình TCP/IP hơi khác so với mô hình OSI (Open Systems Interconnection – Mô hình kết nối các hệ thống mở) bảy lớp được thiết kế sau đó, nó xác định cách các ứng dụng giao tiếp trong một mạng.

1.1.4. Các tầng của TCP/IP

TCP/IP được chia thành bốn tầng, mỗi tầng bao gồm các giao thức cụ thể.

+ **Tầng ứng dụng:** cung cấp các ứng dụng với trao đổi dữ liệu được chuẩn hóa. Các giao thức của nó bao gồm Giao thức truyền tải siêu văn bản (HTTP), Giao thức truyền tập tin (File

Transfer Protocol – FTP), Giao thức POP3, Giao thức truyền tải thư tín đơn giản (Simple Mail Transfer Protocol – SMTP) và Giao thức quản lý mạng đơn giản (Simple Network Management Protocol – SNMP).

+ **Tầng giao vận:** chịu trách nhiệm duy trì liên lạc đầu cuối trên toàn mạng. TCP xử lý thông tin liên lạc giữa các máy chủ và cung cấp điều khiển luồng, ghép kênh và độ tin cậy. Các giao thức giao vận gồm giao thức TCP và giao thức UDP (User Datagram Protocol), đôi khi được sử dụng thay thế cho TCP với mục đích đặt biệt.

+ **Tầng mạng:** còn được gọi là tầng Internet, có nhiệm vụ xử lý các gói và kết nối các mạng độc lập để vận chuyển các gói dữ liệu qua các ranh giới mạng. Các giao thức tầng mạng gồm IP và ICMP (Internet Control Message Protocol), được sử dụng để báo cáo lỗi.

+ **Tầng vật lý:** bao gồm các giao thức chỉ hoạt động trên một liên kết – thành phần mạng kết nối các nút hoặc các máy chủ trong mạng. Các giao thức trong lớp này bao gồm Ethernet cho mạng cục bộ (LAN) và giao thức phân tách địa chỉ (Address Resolution Protocol – ARP).

1.1.5. Ưu điểm của TCP/IP

TCP/IP không thuộc và chịu sự kiểm soát của bất kỳ công ty nào, do đó bộ giao thức mạng này có thể dễ dàng sửa đổi. Nó tương thích với tất cả các hệ điều hành, vì vậy có thể giao tiếp với các hệ thống khác. Ngoài ra, nó còn tương thích với tất cả các loại phần cứng máy tính và mạng.

TCP/IP có khả năng mở rộng cao và như một giao thức có thể định tuyến, nó có thể xác định đường dẫn hiệu quả nhất thông qua mạng.

1.2. Keylogger

1.2.1. Keylogger là gì?

Keylogger là phần mềm hoặc thiết bị phần cứng có khả năng ghi lại các thao tác phím bấm trên máy tính hoặc điện thoại của người dùng. Thông qua việc ghi nhận từng ký tự được nhập, phần mềm này có thể thu thập thông tin cá nhân quan trọng như mật khẩu tài khoản, dữ liệu đăng nhập ngân hàng, email hoặc thông tin định danh.

Ở dạng phần mềm, keylogger thường chạy ngầm trong hệ điều hành và rất khó bị phát hiện bằng các thao tác thông thường. Trong khi đó, keylogger phần cứng có thể tồn tại dưới dạng cổng kết nối hoặc thiết bị trung gian gắn vào máy. Dù tồn tại ở hình thức nào, keylogger đều có nguy cơ gây giật lag thiết bị và làm thất thoát dữ liệu cá nhân của bạn. [2]

Keylogger “chiếm đoạt” thông tin của người dùng và lưu trữ định kỳ trên ổ cứng, hoặc chuyển về một địa chỉ được chỉ định trước. Theo đó, những thông tin thường bị đánh cắp là:

- + Toàn bộ mật khẩu đã đăng nhập và lưu lại trên thiết bị.
- + Thông tin website từng truy cập.
- + Chụp ảnh màn hình thiết bị theo chu kỳ cố định.
- + Chụp ảnh email đã gửi và chuyển đến địa chỉ email, FPT, HTTP... được thiết lập sẵn.
- + Chụp ảnh bản ghi màn hình của tất cả tin nhắn từ Zalo, Messenger, Instagram,...
- + Ghi lại các ứng dụng đang chạy trên thiết bị.
- + Ghi lại tất cả thao tác phím.

1.2.2. Cách thức hoạt động của Keylogger

Keylogger phần mềm có thể được cài đặt bằng nhiều cách khác nhau. Trong một số trường hợp, keylogger có thể được cài đặt bằng cách gửi một tệp đính kèm trong một email lừa đảo hoặc thông qua một trang web độc hại. Trong khi đó, keylogger phần cứng cần được cắm vào máy tính trực tiếp.

Một khi keylogger đã được cài đặt, nó sẽ bắt đầu ghi lại tất cả các phím được bấm trên bàn phím của máy tính. Các thông tin này sẽ được lưu trữ trong một tệp tin hoặc được gửi đến một địa chỉ email được chỉ định. Keylogger có thể hoạt động ngầm kín mà không cần bất kỳ sự chú ý nào từ người dùng. [3]

1.2.3. Phân loại Keylogger

Keylogger bao gồm hai loại, một loại keylogger phần cứng và một loại là phần mềm. Bài viết này nói đến loại phần mềm.

Theo những người lập trình, keylogger viết ra với chỉ có một loại duy nhất là giúp các bạn giám sát con cái, người thân xem họ làm gì với PC, với internet, khi chat với người lạ nhưng cách sử dụng và chức năng của Keylogger, hiện tại trên thế giới khiến người ta thường hay phân loại keylogger theo mức độ nguy hiểm bằng các câu hỏi:

- + Nhiễm vào máy không qua cài đặt/ Cài đặt vào máy cực nhanh?
- + Có thuộc tính ẩn/ giấu trên trình quản lý tiến trình và trình cài đặt và gỡ bỏ chương trình?

- + Theo dõi không thông báo/PC bị nhiễm khó tự phát hiện?
- + Có thêm chức năng CaptureScreen hoặc ghi lại theo tác chuột?
- + Khó tháo gỡ?
- + Có khả năng lây nhiễm, chống tắt (kill process)?

Cứ mỗi câu trả lời “Có” cho một điểm. Điểm càng cao, keylogger càng vượt khỏi mục đích giám sát đến với mục đích đo thám (spying) và tính nguy hiểm nó càng cao. Keylogger có thể được phân loại theo số điểm:

Loại số 1 (Không điểm): chạy công khai, có thông báo cho người bị theo dõi, đúng với mục đích giám sát.

Loại số 2 (Một đến hai điểm): keylogger nguy hiểm, chạy ngầm, hướng đến mục đích đo thám nhiều hơn là giám sát.

Loại số 3 (Ba đến năm điểm): keylogger loại rất nguy hiểm, ẩn giấu hoàn toàn theo dõi trên một phạm vi rộng, mục đích đo thám rõ ràng.

Loại số 4 (Sáu điểm): keylogger nguy hiểm nghiêm trọng, thường được mang theo bởi các trojan-virus cực kỳ khó tháo gỡ, là loại keylogger nguy hiểm nhất. Chính vì vậy (và cũng do đồng thời là “đồng bọn” của trojan-virus) nó thường hay bị các chương trình chống virus tìm thấy và tiêu diệt.

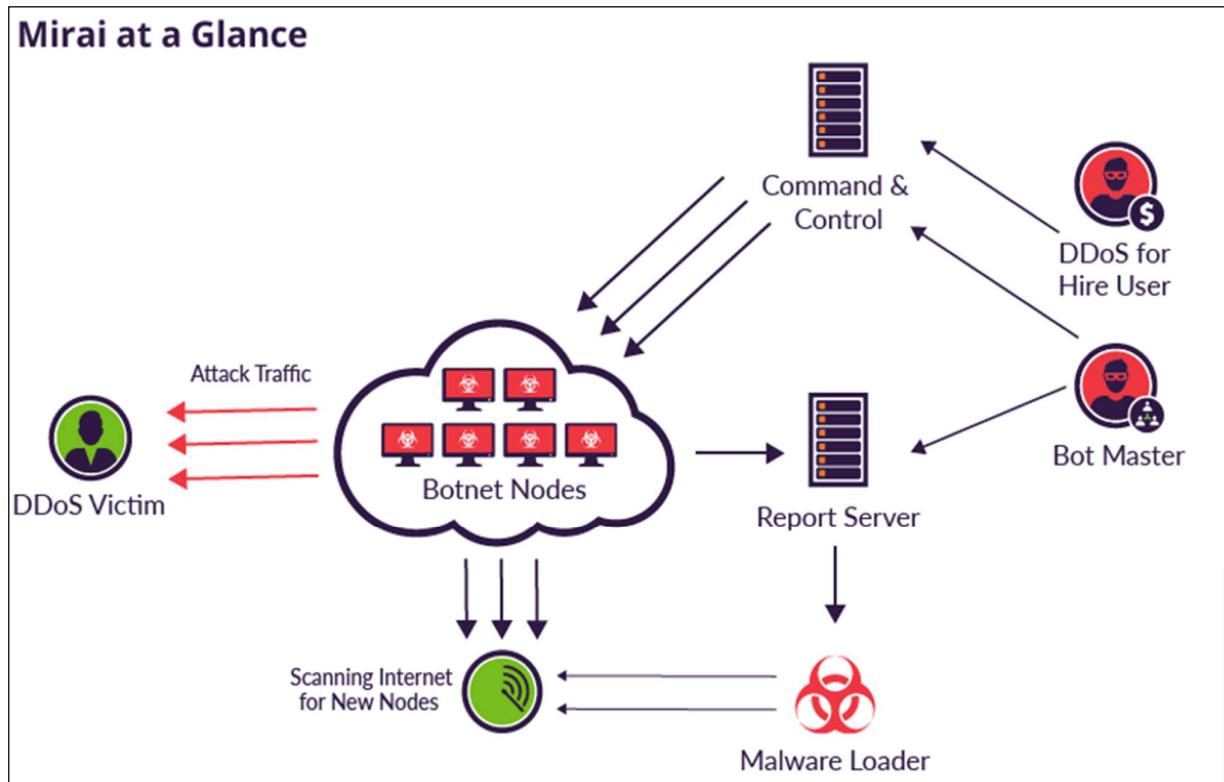
1.3. Botnet

1.3.1. Botnet là gì?

Botnet là mạng lưới các máy tính bị nhiễm mã độc và chiếm quyền điều khiển bởi kẻ tấn công. Sau đó, những máy tính này bị lợi dụng để thực hiện các cuộc tấn công mạng như đánh cắp dữ liệu, gây sự cố server, phát tán phần mềm độc hại,... [4]

Các máy tính trong botnet, thường được gọi là bot hoặc zombie, hoạt động âm thầm và nhận lệnh điều khiển từ một máy chủ trung tâm. Nhờ số lượng lớn và khả năng hoạt động đồng thời, botnet có thể tạo ra sức ảnh hưởng lớn, gây thiệt hại nghiêm trọng cho hệ thống mạng và người dùng. Do đó, botnet được xem là một trong những mối đe dọa phổ biến và nguy hiểm trong lĩnh vực an toàn thông tin hiện nay.

1.3.2. Mục đích tấn công của Botnet?



Hình 2: Quy trình hoạt động của Botnet

Người tạo lập ra các mạng lưới Botnet đều có những mục đích chiếm đoạt riêng nào đó, không hẳn là mục đích chiếm đoạt sử dụng mà cũng có thể chiếm đoạt xong một lượng thông tin đáng kể rồi giao bán cho những đối tượng cần để kiếm tiền. Do đó đặc thù của Botnet là một mạng lưới các Bot, nên Hacker dùng Botnet để tấn công Ddos, sau đó điều khiển tất cả các máy tính từ xa, có thể cùng lúc hàng ngàn, hàng nghìn chiếc máy tính cùng truy cập vào một website chỉ định, tạo ra lưu lượng quá tải trong website đó và gây tình trạng nghẽn mạng, treo máy.

Botnet có thể vào bằng nhiều đường và ở nhiều dạng thù khác nhau nhưng những mục đích của nó có thể là:

- ❖ Gửi mail spam: cách thức kiếm tiền phổ biến của các Spammer. Hơn nữa các Botnet cũng tạo ra các web gian lận chèn bổ sung quảng cáo chạy trên nền web, người sử dụng tương tác click vào link quảng cáo sẽ tạo ra tiền cho các Hacker.
- ❖ Các cuộc tấn công DDoS dùng Botnet xảy ra liên tục. Bot Herder sẽ lập trình ra một link website bất kỳ nào đó và điều khiển tất cả các máy tính là nạn nhân của Bot truy cập

vào website đó, tạo ra tình trạng nghẽn mạng, dẫn đến không truy cập được nữa. Gửi hăm dọa, làm gian lận và tống tiền người dùng.

- ❖ Botnet đào tiền ảo từ một máy tính lớn, giúp chúng thu về tiền ảo như Bitcoin và các chi phí khác sẽ bị chịu bởi người dùng.
- ❖ Botnet cũng tạo và phát tán các loại virut, malware đến máy tính bạn và dùng nó tiếp tục lây lan sang các máy tính khác để tạo một mạng lưới Botnet lớn rộng để thu được nhiều lợi nhuận hơn.

1.3.3. Quy trình hoạt động của Botnet

Đánh vào những lỗ hổng an ninh, những mảng vá cũ hay những server lỗi thời hết hạn, các Bot nằm ẩn mình trong các máy tính của khách hàng – kết nối sẵn với Botmaster, chỉ đợi lệnh và điều khiển từ Bot Master để tiến hành hoạt động của mình. Sau khi nhận lệnh từ Hacker, mỗi Bot có một hoạt động riêng tùy theo sự điều khiển từ phía ngoài. Nó có thể tấn công theo nhiều cách như là: Tạo Spam, tấn công DDoS, chiếm giữ hệ thống, lừa đảo ăn cắp Bitcon. Dù cách tấn công như nào thì mục đích cuối cùng của nó cũng chỉ là điều khiển hoạt động của máy tính bị nhiễm, bắt buộc người dùng phải làm theo mệnh lệnh của nó.

Nếu ta tấn công ngược lại mạng Bot thì chúng ta cũng không thể đánh sập lại hệ thống máy chủ, mà đôi khi chúng ta lại gặp những nạn nhân bị nhiễm khác, giống như hoạt động lặp lại pear – to – pear vậy. Các máy tính bị nhiễm liên kết với nhau lại tạo thành mạng Botnet và càng khó khăn hơn trong việc tìm ra mạng điều hành phía sau.

1.3.4. Phân loại Botnet

Botnet có 2 loại cơ bản là DNS và IRC. Mỗi loại có một chức năng riêng và ưu điểm riêng:

- + **DNS Bot:** dễ thực hiện và điều khiển đơn giản không quá cầu kỳ, được dùng để chạy Bot trên nền Web. Nhưng vẫn bị hạn chế trong việc trao đổi thông tin giữa Bot master và các Bot.
- + **IRC Bot:** Giúp trao đổi thông tin giữa Bot Master và các Bot, điều khiển qua mạng chat IRC. Nhưng lại bị phụ thuộc vào các IRC và người quản trị Server.

1.3.5. 7 loại tấn công Botnet phổ biến hiện nay [4]

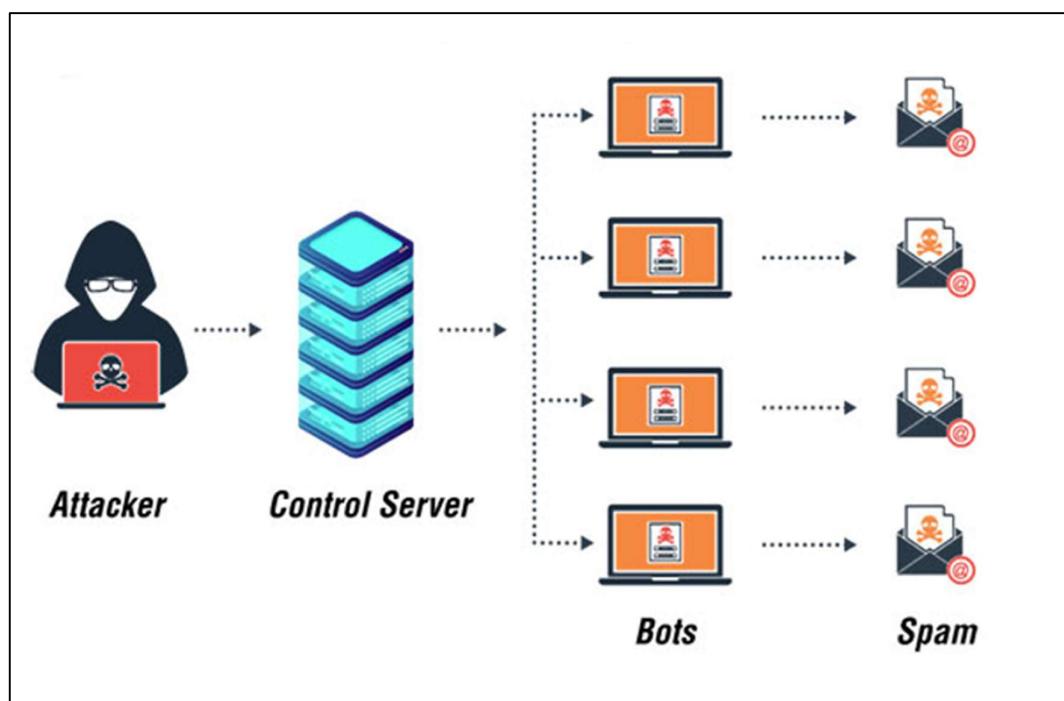
1.3.5.1 Loại thứ 1: Tấn công DDoS

DDoS (hay Distributed Denial of Operations Service) là tấn công từ chối dịch vụ phân tán. Lúc này, tin tặc có thể sử dụng một botnet để xâm nhập vào hàng loạt máy tính của người dùng khác nhau nhằm mục đích phá hủy kết nối và dịch vụ mạng đang sử dụng. Nguyên lý cơ bản của loại tấn công này là làm quá tải lượng tài nguyên máy chủ và tiêu tốn hết băng thông của nạn nhân dẫn đến các hoạt động bị đình trệ.

Một trong các cuộc tấn công DDoS lớn nhất là khi tin tặc đã từng sử dụng virus botnet Mirai. Đây được biết đến là một loại virus có khả năng nhắm mục tiêu cũng như giành quyền kiểm soát hàng chục ngàn thiết bị Internet, sau đó biến chúng thành những con bot tấn công DDoS vào hệ thống người dùng. Không chỉ vậy, loại virus này còn có khả năng mở rộng khiến cho cuộc tấn công DDoS trở nên phức tạp và gây ra hậu quả nghiêm trọng hơn.

1.3.5.2 Loại thứ 2: Tấn công phát tán thư rác

Đây là loại hình thức tấn công sử dụng botnet để xác định các dữ liệu nhạy cảm trong máy tính bị nhiễm. Các con bot này còn có thể mở được proxy SOCKS v4/v5 (giao thức proxy chung cho mạng dựa trên TCP/IP). Sau khi kích hoạt thành công Proxy SOCKS, nó sẽ sử dụng để phát tán thư rác (spamming) đến người dùng. Để theo dõi thông tin dữ liệu được truyền ở máy tính bị xâm nhập thì botnet sẽ sử dụng packet sniffer và sniffer để truy xuất thông tin nhạy cảm như tên người dùng, mật khẩu,...



Hình 3: Quy trình phân tán

1.3.5.3 Loại thứ 3: Keylogging

Loại tấn công Keylogging chính là việc botmaster với sự trợ giúp của chương trình Keylogging sẽ lấy thông tin nhạy cảm và đánh cắp dữ liệu của người dùng. Chương trình này còn giúp tin tặc có khả năng thu thập các phím được nhập trong PayPal, Yahoo,... của người dùng.

1.3.5.4 Loại thứ 4: Đánh cắp danh tính

Việc kết hợp nhiều loại botnet khác nhau giúp tin tặc có thể dễ dàng thực hiện hành vi trộm cắp danh tính ở quy mô lớn. Các bot này sẽ thực hiện gửi email spam hướng đến những người dùng truy cập vào những Website giả mạo, sau đó sẽ thực hiện thu thập thông tin cá nhân của người dùng. Thậm chí, các botnet này có thể giả danh tính của những tổ chức, doanh nghiệp pháp lý và yêu cầu người dùng cung cấp các thông tin cá nhân như thẻ tín dụng, tài khoản ngân hàng, mã số thuế,...

1.3.5.5 Loại thứ 5: Lợi dụng việc trả tiền cho mỗi lần nhấp

AdSense của Google là chương trình cho phép hiển thị quảng cáo Google trên các Website và Google sẽ trả tiền cho chủ sở hữu Website đó dựa trên số lần nhấp chuột vào quảng cáo. Trong trường hợp máy tính của người dùng bị nhiễm botnet sẽ tự động nhấp vào các quảng cáo trên Website đó. Điều này làm cho lưu lượng truy cập đến Website được quảng cáo là ảo, gây hiểu lầm cho Google và doanh nghiệp được quảng cáo.

1.3.5.6 Loại thứ 6: Lây lan Botnet

Tin tặc có thể lan truyền các botnet bằng việc thuyết phục người dùng tải xuống các chương trình có nhiễm virus. Những chương trình này có thể được thực thi thông qua Email, HTTP hay FTP,...

1.3.5.7 Loại thứ 7: Phần mềm quảng cáo

Máy tính người dùng có thể xuất hiện những quảng cáo không mong muốn hay quảng cáo gốc bị thay thế bởi những phần mềm quảng cáo lừa đảo. Đây là những phần mềm không được người dùng cho phép và lây nhiễm vào hệ thống của họ khi nhấp vào những mẫu quảng cáo đó.

Thoạt nhìn các phần mềm quảng cáo này có vẻ là những quảng cáo vô hại nhưng chúng đã được cài đặt sẵn những phần mềm gián điệp để thu thập và đánh cắp dữ liệu trình duyệt của người dùng. Để chống lại các cuộc tấn công này, người dùng có thể sử dụng các phần mềm

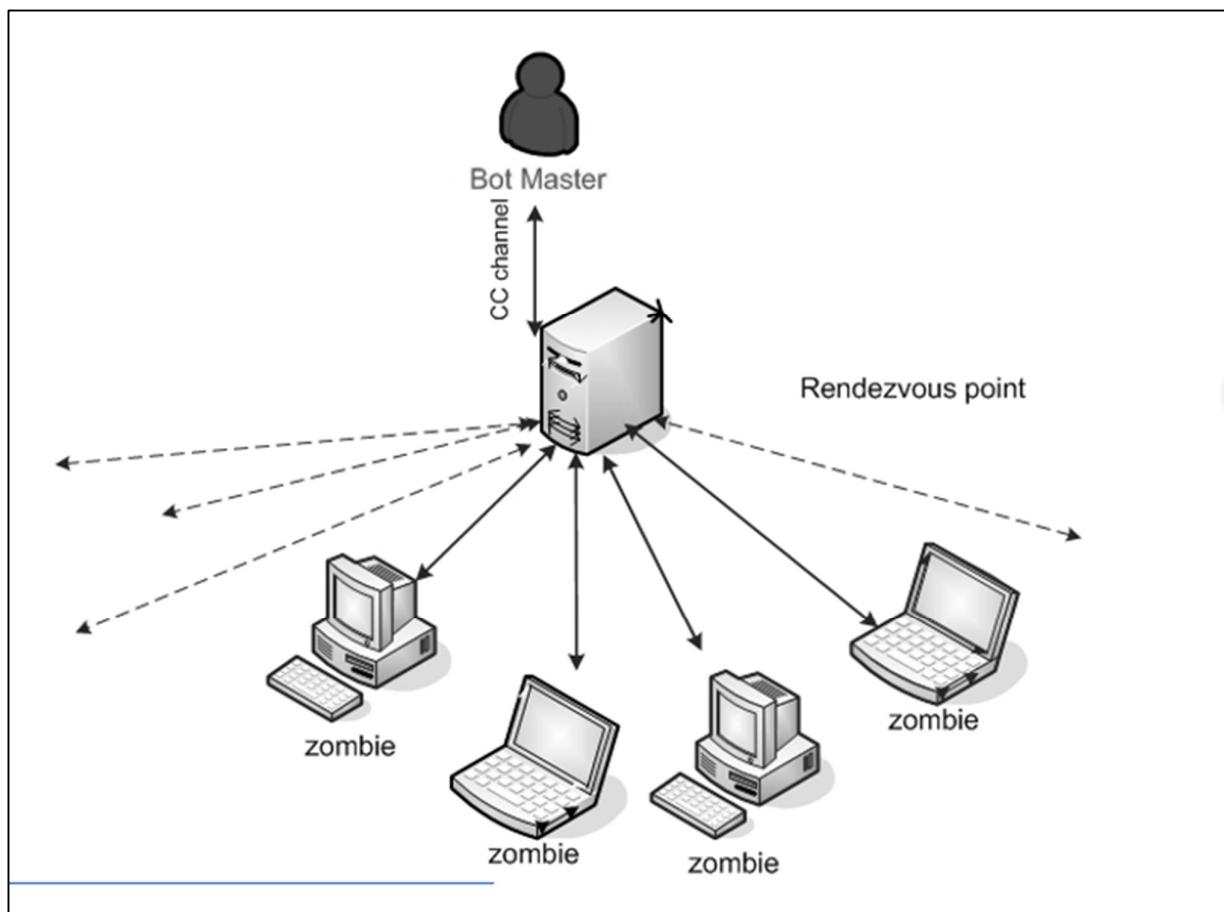
chặn quảng cáo. Những phần mềm chặn quảng cáo này có thể chặn không cho botnet xâm nhập vào máy tính, lây nhiễm trên ổ cứng hay lưu lượng mạng, đồng thời trực xuất chúng ra khỏi hệ thống máy tính của người dùng.

1.3.6. Giải pháp phòng vệ Botnet FortiGuard

- + Phần mềm chống Virus mới nhất
- + Nâng cấp tường lửa
- + Cập nhật phần mềm mới và cài đặt các mảng vá lỗi liên tục
- + Làm theo hướng dẫn về bảo mật cho máy tính bạn

1.4. Hệ điều hành

- + Cấu trúc hệ điều hành: Đi sâu vào cấu trúc và nguyên tắc hoạt động của hệ điều hành, bao gồm lập lịch, quản lý bộ nhớ, và truy cập tài nguyên hệ thống.
- + Quy trình nạp chương trình: Nghiên cứu về quy trình mà hệ điều hành sử dụng để nạp và thực thi các chương trình mới.



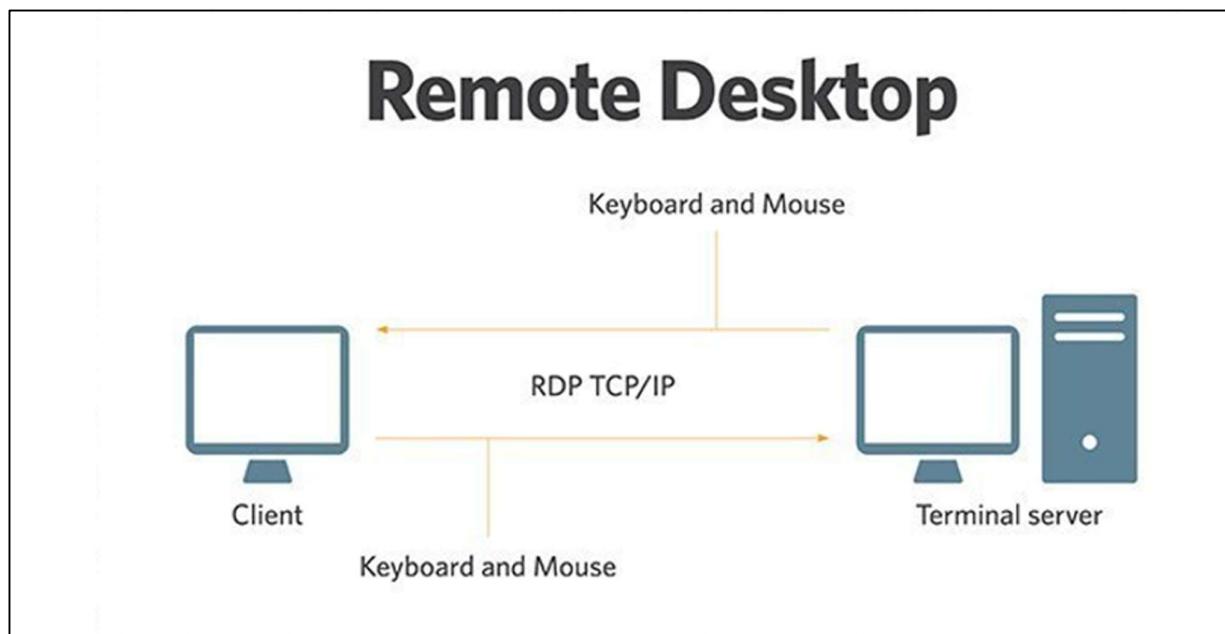
Hình 4: Quá trình phát tán dữ liệu

1.5. Remote Desktop (RDP)

Remote Desktop là một thuật ngữ thường được sử dụng để chỉ một loại phần mềm hoặc một tính năng của hệ điều hành được sử dụng để loại kết nối giao diện đồ họa đến máy chủ, máy tính từ xa. Với mục đích chạy các ứng dụng hay thực hiện lệnh trên máy tính ở xa.

Những lệnh hay những phím bấm được nhập vào và cả click chuột cũng sẽ được gửi đến máy tính xa này và hình ảnh thực thi sẽ gửi lại người dùng tương tự dùng thao tác trực tiếp trên máy tính của mình.

Lợi ích của Remote Desktop: Bạn có thể kết nối vào môi trường giao diện làm việc của máy tính, máy chủ từ một nơi rất xa, chỉ cần có Internet. Giúp bạn thực hiện các thao tác quản trị, sử dụng hệ điều hành hoặc bảo trì hệ thống từ xa.



Hình 5: Quy trình hoạt động Remote Desktop

1.6. Window defender

Window defender là phần mềm diệt virus được tích hợp sẵn trong hệ điều hành Windows 10 và 11. Không chỉ hoạt động hoàn toàn miễn phí, công cụ này còn giúp bảo vệ máy tính của bạn trước các mối đe dọa như virus, ransomware, spyware và phần mềm độc hại khác mà không cần cài thêm phần mềm bên ngoài.

Các điểm nổi bật của window defender:

- + Chống virus và phần mềm độc hại theo thời gian thực: luôn quét hệ thống và phát hiện sớm các tệp nguy hiểm.
- + Tường lửa thông minh: giám sát kết nối mạng, ngăn chặn truy cập trái phép.
- + Bảo vệ trình duyệt và ứng dụng: cảnh báo các trang web giả mạo, kiểm soát quyền truy cập phần mềm.
- + Bảo vệ danh tính và tài khoản: tăng cường bảo mật thông tin cá nhân khi đăng nhập hoặc giao dịch online.
- + Tích hợp tốt – nhẹ - miễn phí: không làm nặng máy, hoạt động mượt mà và được cập nhật tự động qua windows update. [5]

CHƯƠNG 2: THIẾT KẾ VÀ XÂY DỰNG HỆ THỐNG

2.1. Tổng quan chức năng chính của hệ thống

2.1.1. SystemInfo (Thông tin hệ thống)

- Mục tiêu: Cung cấp thông tin cơ bản về hệ thống đang sử dụng.

- Chức năng chi tiết:

- + Hiển thị thông tin về bộ xử lý (CPU), bộ nhớ (RAM), card đồ họa (GPU), tên người dùng và các thông số quan trọng khác của máy tính.
- + Cung cấp cái nhìn tổng quan về tình trạng hiện tại của hệ thống.

2.1.2. Remote Shell (Shell từ xa)

- Mục tiêu: Cho phép người quản trị hoặc người dùng có thể thực hiện các lệnh từ xa thông qua một giao diện dòng lệnh.

- Chức năng chi tiết:

- + Hiển thị giao diện dòng lệnh cho người dùng.
- + Thực thi các lệnh từ xa và hiển thị kết quả trực tiếp trên giao diện người dùng.

2.1.3. File Manager (Quản lý tệp tin)

- Mục tiêu: Quản lý tệp tin và thư mục từ xa, bao gồm xem, tải xuống, tải lên và thực thi.

- Chức năng chi tiết:

- + Hiển thị cấu trúc thư mục và tệp tin từ xa.
- + Cho phép người dùng tải xuống và tải tệp tin lên.
- + Hỗ trợ thực thi các lệnh từ xa.

2.1.4. Keylogger (Ghi lại phím)

- Mục tiêu: Theo dõi và lưu trữ thông tin nhập phím từ người dùng.

- Chức năng chi tiết:

- + Ghi lại sự kiện nhập phím, bao gồm cả thông tin về thời gian và ứng dụng được nhập dữ liệu.
- + Lưu trữ thông tin ghi lại để phân tích sau này.

2.1.5. Task Manager (Quản lý tiến trình)

- Mục tiêu: Hiển thị và quản lý các tiến trình đang chạy trên máy tính.

- Chức năng chi tiết:

- + Liệt kê tất cả các tiến trình đang chạy cùng với thông tin chi tiết. Ví dụ như: tài nguyên sử dụng.
- + Cho phép người dùng kết thúc tiến trình không mong muốn.

2.1.6. Remote Desktop (Màn hình từ xa)

- Mục tiêu: Cho phép điều khiển máy tính từ xa, bao gồm cả hiển thị màn hình và thao tác chính.

- Chức năng chi tiết:

- + Hiển thị màn hình máy tính từ xa trên giao diện người dùng.
- + Cho phép thực hiện các thao tác trực tuyến trên màn hình từ xa.
- + Hỗ trợ tương tác toàn diện với máy tính từ xa.

2.2. Các thành phần của hệ thống

2.2.1. Botnet Client (Nạn nhân Botnet)

- Mục tiêu: Là phần mềm gián điệp được cài đặt và chạy trên máy tính của nạn nhân mà không được sự cho phép của họ.

- Chức năng chi tiết:

- + **Ngụy trang:** Botnet Client thường ẩn mình hoặc ngụy trang thành các tiến trình hợp lệ để tránh sự phát hiện từ phía người dùng và các chương trình bảo mật.
- + **Kết Nối Đến Botnet Server:** Botnet client kết nối đến botnet server, trở thành một phần của mạng botnet và sẵn sàng nhận lệnh từ botnet server.
- + **Chức Năng Cơ Bản:** Thực hiện các nhiệm vụ như ghi lại thông tin nhập phím, lấy dữ liệu định kỳ từ máy nạn nhân và thực hiện các hành động gián điệp khác.

2.2.2. Botnet Server (Máy chủ Botnet)

- Mục tiêu: Là trung tâm quản lý của mạng botnet, nơi mà tất cả các botnet client kết nối để nhận và thực hiện các lệnh.

- Chức năng chi tiết

- + Quản Lý Botnet: Theo dõi và quản lý trạng thái của các botnet client.

- + Gửi Lệnh: Gửi các lệnh đến botnet client để thực hiện các nhiệm vụ thu thập thông tin.
- + Thu Thập Dữ Liệu: Đánh cắp và lưu trữ thông tin từ các máy nạn nhân, bao gồm thông tin cá nhân, thông tin đăng nhập, và dữ liệu khác có giá trị
- + Ngụy Trang: Cố gắng ngụy trang trước các biện pháp phòng ngự bảo mật từ phía nạn nhân

2.2.3. Triển khai chi tiết hệ thống

2.2.3.1 Kết nối mạng

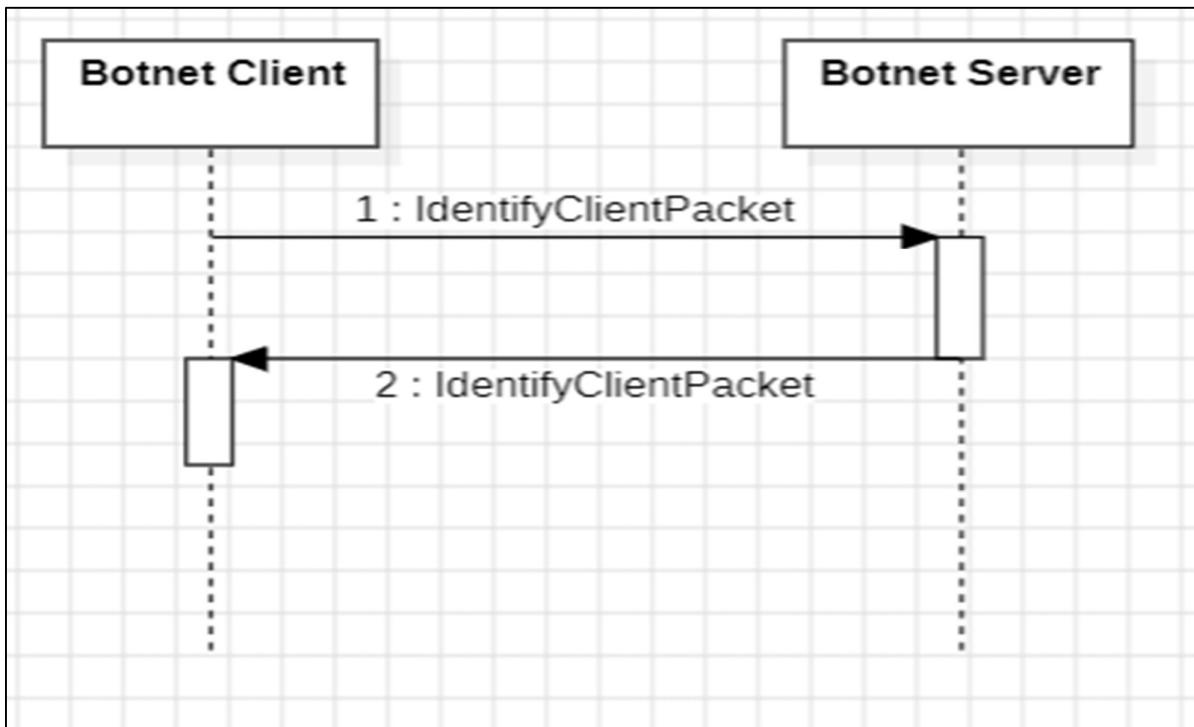
- Phương thức kết nối: TCP/IP
- Cấu hình gói tin:

Length (4 byte)	Id (4 byte)
Data	

- Các kiểu dữ liệu:

Tên kiểu dữ liệu	Mô tả dữ liệu	Độ dài	Cấu hình gửi
Byte	0x00 => 0xFF	1 byte	1 byte
Char	0x00 => 0xFF	1 byte	1 byte
Boolean	0x00, 0x01	1 byte	1 byte
Int	0x00000000 => 0xFFFFFFFF	4 byte	4 byte
Long	0x0000000000000000 => 0xFFFFFFFFFFFFFF	8 byte	8 byte
String	“Xin chào”	4 + N byte	4 byte (Length) + Data
Byte Array	N * Byte	4 + N byte	4 byte (Length) + Data

- Các bước bắt tay: Ngay khi kết nối TCP/IP được tạo, Botnet Client gửi gói tin IdentifyClientPacket đến Botnet Server nhằm cung cấp các thông tin định danh của hệ thống. Botnet Server tiếp nhận, xử lý và phản hồi lại bằng gói tin cùng loại để xác nhận kết nối thành công. Sau bước này, client chính thức được đưa vào danh sách quản lý của server và sẵn sàng nhận các lệnh điều khiển tiếp theo.



Hình 6: Kết nối mạng

- Mô tả gói tin:

+ IdentifyClientPacket (Server => Client)

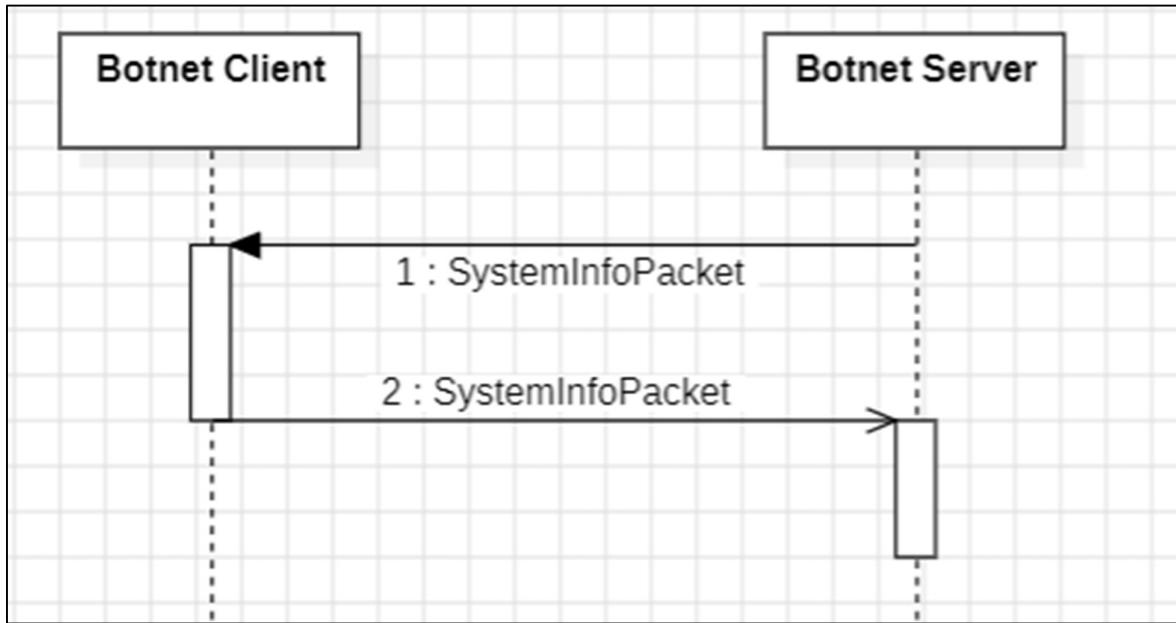
Id	0x01
----	------

+ IdentifyClientPacket (Client => Server)

Id	0x01
OperatingSystem	String
AccountType	String
Country	String
CountryCode	String
Username	String
PcName	String
HardwareId	String
IpAddress	String

2.2.3.2 System Information

Mô tả: Botnet Server gửi gói tin SystemInfoPacket để yêu cầu Client cung cấp thông tin hệ thống. Sau khi nhận yêu cầu, Client tiến hành thu thập các thông tin liên quan và phản hồi lại Server dưới dạng các cặp dữ liệu Key – Value.



Hình 7: Sơ đồ hoạt động của System Information

- Mô tả gói tin
- + SystemInfoPacket (Server => Client)

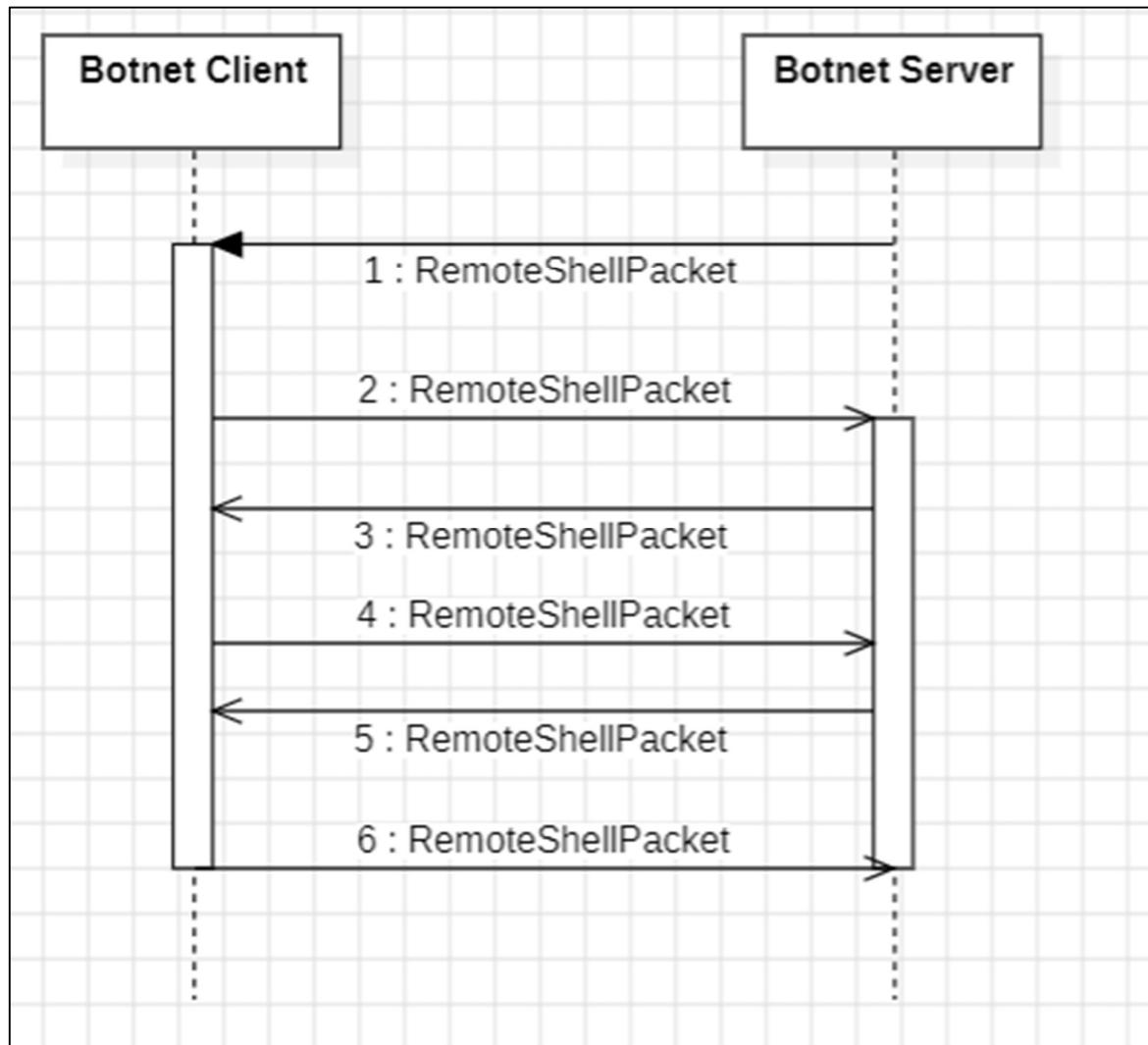
Id	0x10
----	------

- + SystemInfoPacket (Client => Server)

Id	0x10
Length	Int
Array(Key, Value)	Array(String + String)

2.2.3.3 Remote Shell

Mô tả: Server gửi gói tin RemoteShellPacket chứa lệnh cần thực thi đến Client, sau đó Client tiến hành thực thi lệnh trên hệ thống và phản hồi kết quả hoặc thông báo lỗi về Server. Quy trình này có thể lặp lại nhiều lần trong một phiên làm việc, tạo thành cơ chế điều khiển shell từ xa theo mô hình yêu cầu – phản hồi.



Hình 8: Sơ đồ hoạt động Remote Shell

- Mô tả gói tin:

+ RemoteShellPacket(Server=>Client)

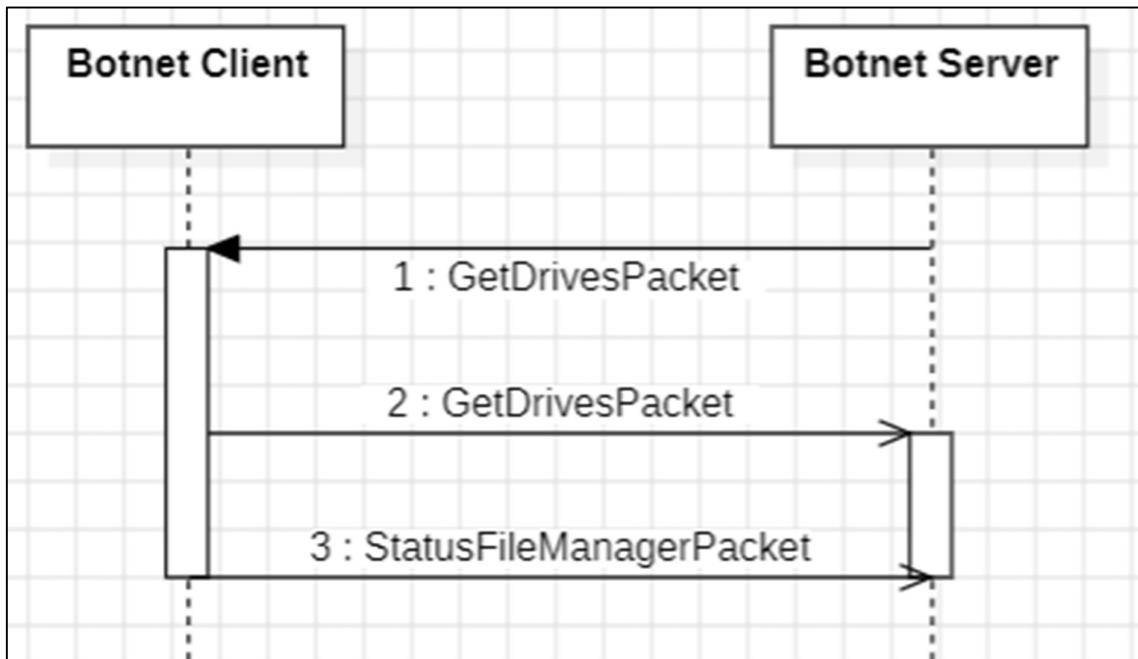
Id	0x20
Command	String

+ RemoteShellPacket(Client=>Server)

Id	0x20
IsError	Bool
Output	String

2.2.3.4 File Management

Mô tả: Botnet Server gửi gói tin GetDrivesPacket đến Botnet Client nhằm yêu cầu danh sách các ổ đĩa có sẵn trên hệ thống. Sau khi thu thập thông tin, Botnet Client phản hồi lại Server bằng gói tin GetDrivesPacket kèm theo dữ liệu các ổ đĩa. Tiếp theo, Botnet Client gửi gói tin StatusFileManagerPacket để thông báo trạng thái của module quản lý tệp tin.

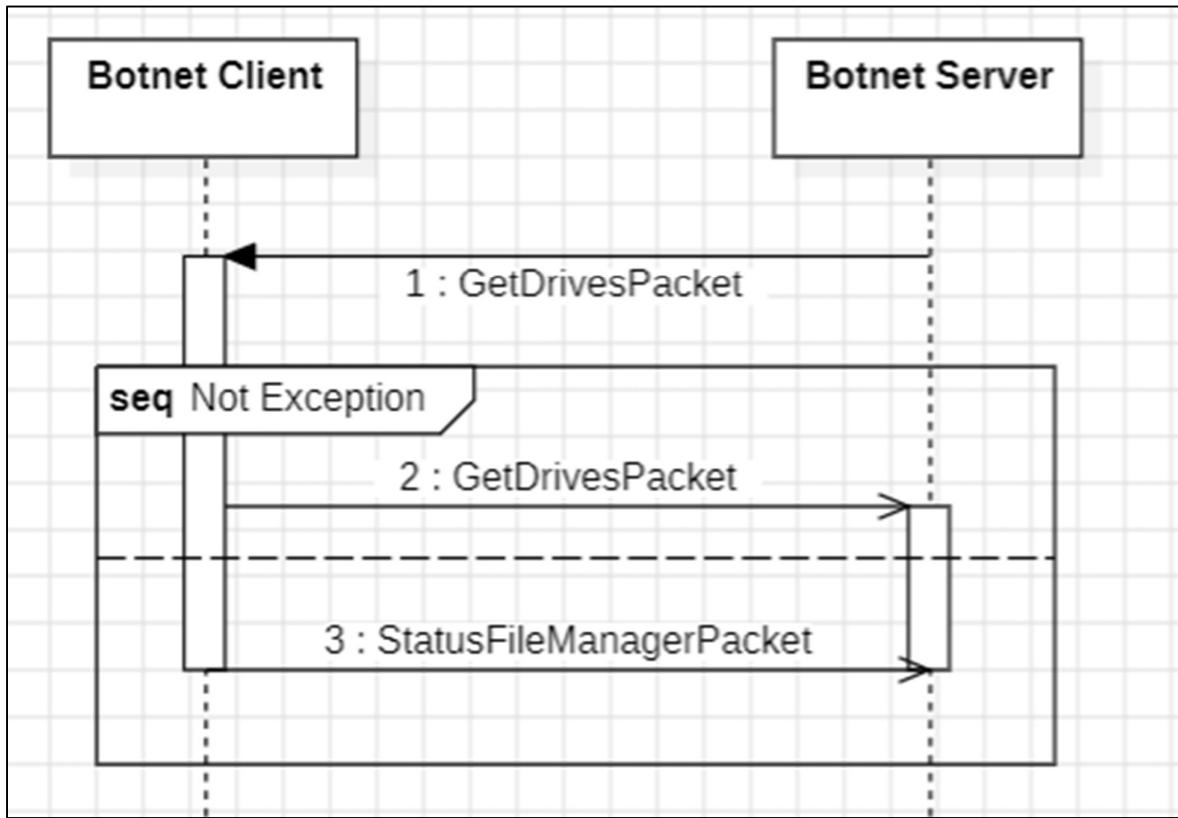


Hình 9: Sơ đồ hoạt động File Management

+Gói tin 1 (StatusFileManagerPacket) (Client => Server)

Id	0x40
Message	String

+ Gói tin 2 (GetDrivesPacket)



Hình 10: Sơ đồ hoạt động GetDrivesPacket

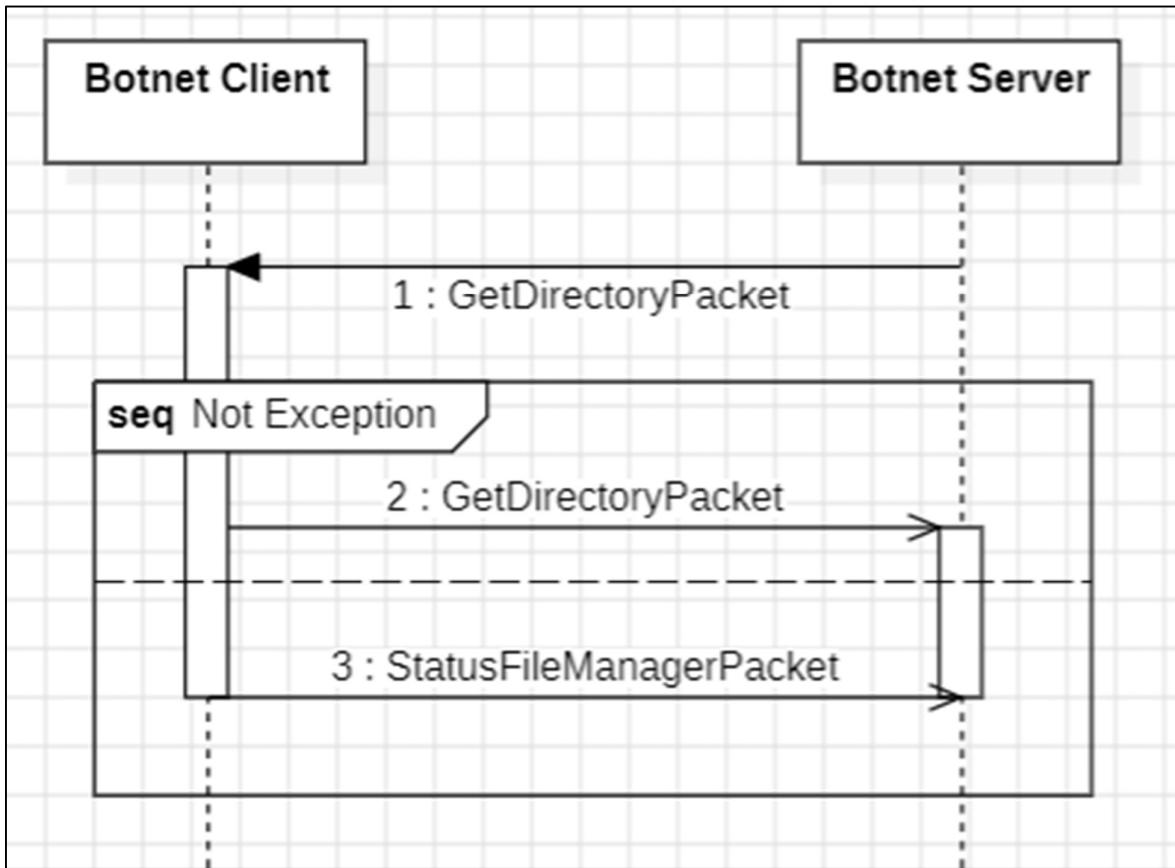
GetDrivesPacket(Server => Client)

Id	0x41
----	------

GetDrivesPacket(Client => Server)

Id	0x41
Length	int
DisplayName	String
RootDirectory	String

+ Gói tin 3 (GetDirectoryPacket)



Hình 11: Sơ đồ hoạt động GetDirectoryPacket

GetDirectoryPacket (Server =>Client)

Id	0x42
RemotePath	

GetDirectoryPacket (Client => Server)

Files	EntryType	Byte
	Name	String
	Size	Long
	LateAccessTimeUTC	String
	ContentType	Short

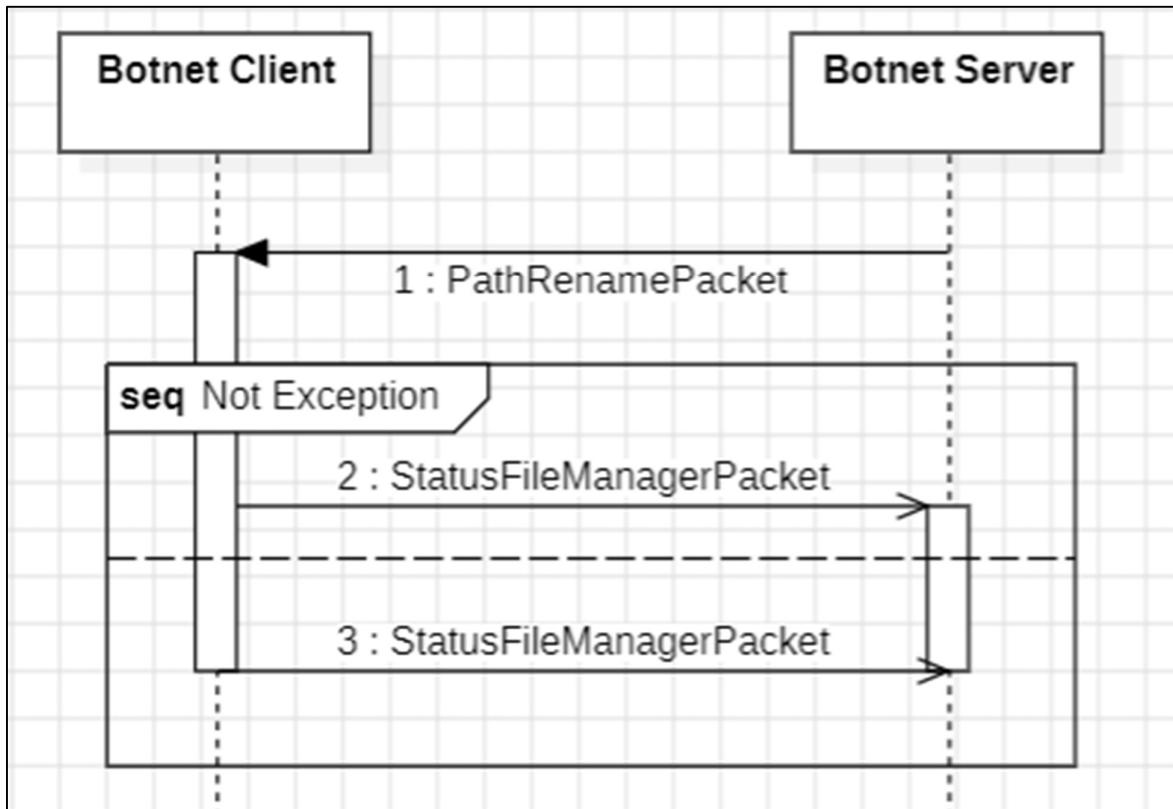
FileType (Byte)

enum	[File, Directory, Back]
------	-------------------------

```
ContentType( Byte){
```

```
    Blob = 2,  
    Application = 3,  
    Text = 4,  
    Archive = 5,  
    Word = 6,  
    PDF = 7,  
    Image = 8,  
    Video = 9,  
    Audio = 10,  
}
```

+ Gói tin 4 (PathRenamePacket)

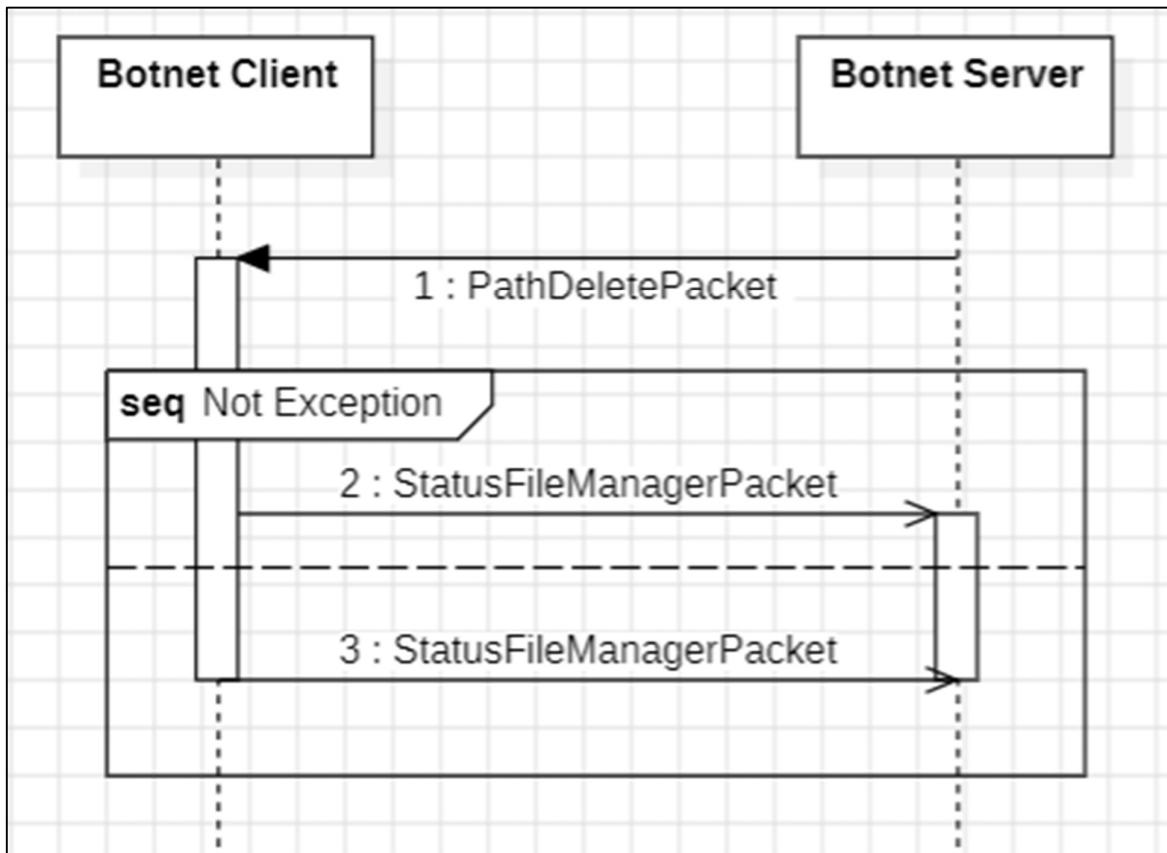


Hình 12: Sơ đồ hoạt động PathRenamePacket

PathRenamePacket (Server => Client)

Id	0x43
Path	String
NewPath	String
PathType	FileType(byte)

+ Gói tin 5 (PathDeletePacket)



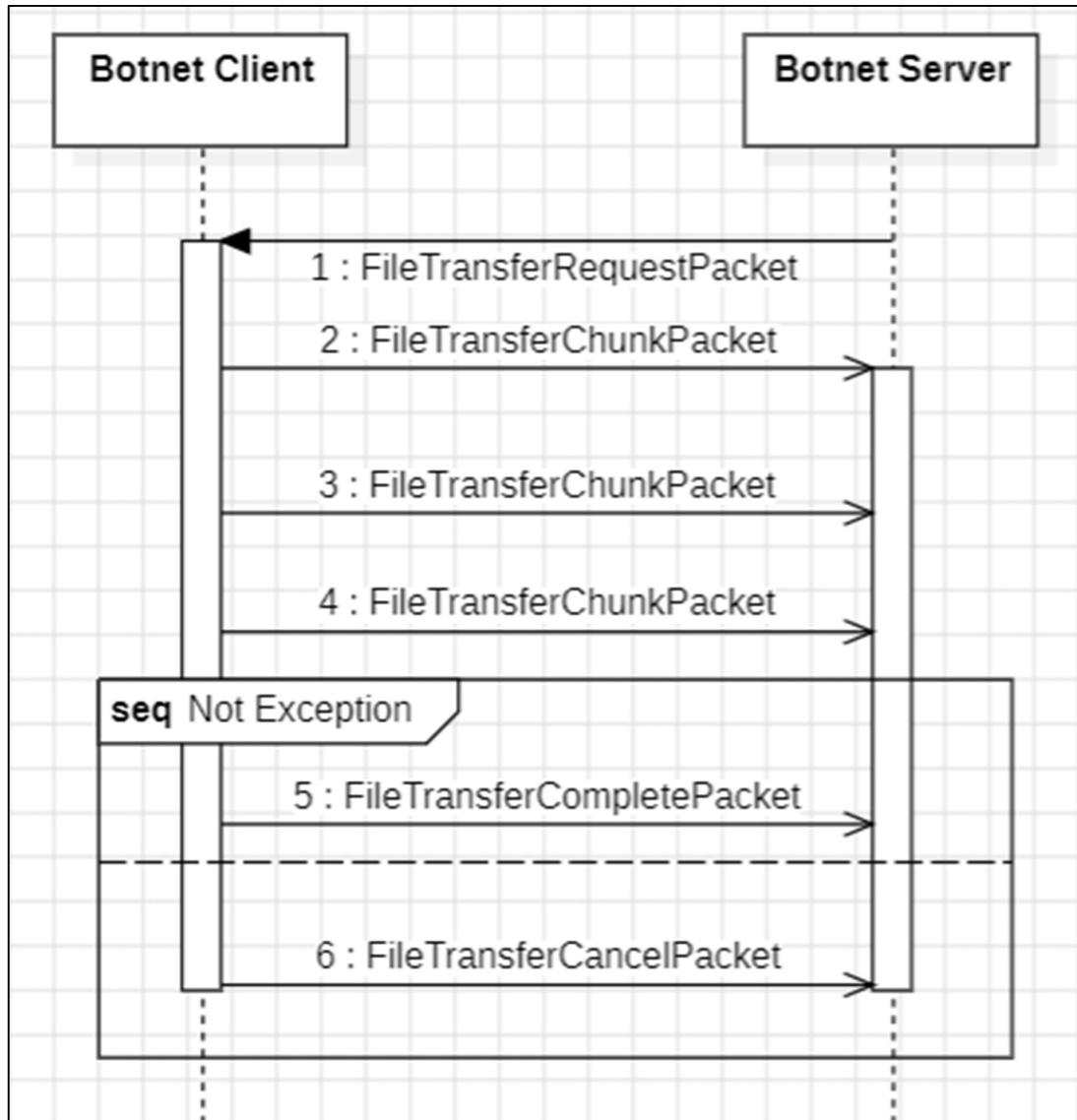
Hình 13: Sơ đồ hoạt động PathDeletePacket

PathDeletePacket (Server => Client)

Id	0x44
Path	String
PathType	FileType

+ Gói tin 6 (FileTransferRequestPacket, FileTransferChunkPacket, FileTransferCompletePacket)

FileTransferRequestPacket(Server => Client)



Hình 14: Sơ đồ hoạt động FileTransferRequestPacket

<code>IdRequest</code>	<code>Int</code>
<code>RemotePath</code>	<code>String</code>

FileTransferChunkPacket (Client => Server)

<code>IdRequest</code>	<code>Int</code>
<code>FilePath</code>	<code>String</code>
<code>FileSize</code>	<code>Long</code>
<code>Chunk</code>	<code>FileChunk { Offset: Long}</code>

	Data: Byte[] }
--	-------------------

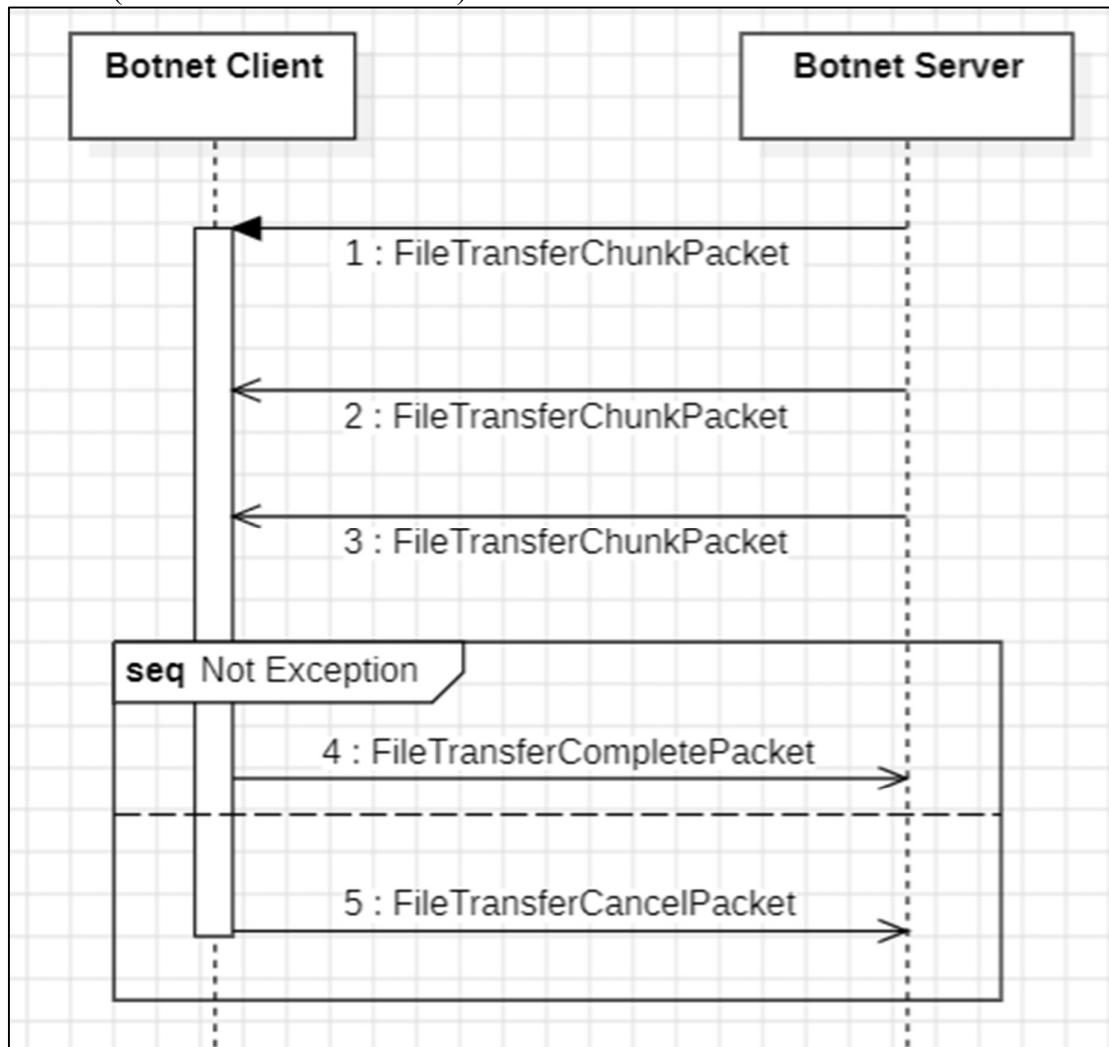
FileTransferCompletePacket

Id	0x46
IdRequest	Int
FilePath	String

Thất bại: FileTransferCancelPacket

Id	0x46
IdRequest	Int
Reason	“Error reading”

+ Gói tin 7: (FileTransferChunkPacket)



Hình 15: Sơ đồ hoạt động FileTransferChunkPacket

FileTransferChunkPacket

Id	0x48
IdRequest	Int
FilePath	String
FileSize	Long
Chunk	<pre>FileChunk { Offset: Long Data: Byte[] }</pre>

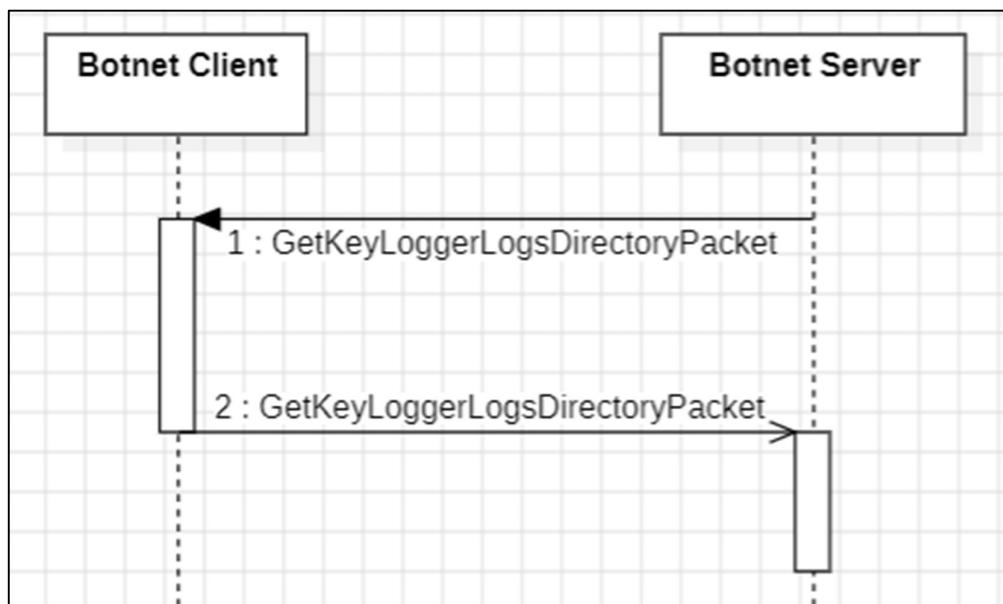
*Thất bại

FileTransferCancelPacket

Id	0x46
IdRequest	Int
Reason	“Error reading”

2.2.3.5 Keylogger

Mô tả: Botnet Server gửi gói tin GetKeyLoggerLogsDirectoryPacket đến Botnet Client để yêu cầu thông tin về thư mục lưu trữ log keylogger. Sau khi xử lý yêu cầu, Botnet Client phản hồi lại bằng gói tin cùng loại, kèm theo đường dẫn thư mục log tương ứng.



Hình 16: Sơ đồ hoạt động của Keylogger

Mô tả gói tin:

GetKeyLoggerLogsDirectoryPacket(Server=> Client)

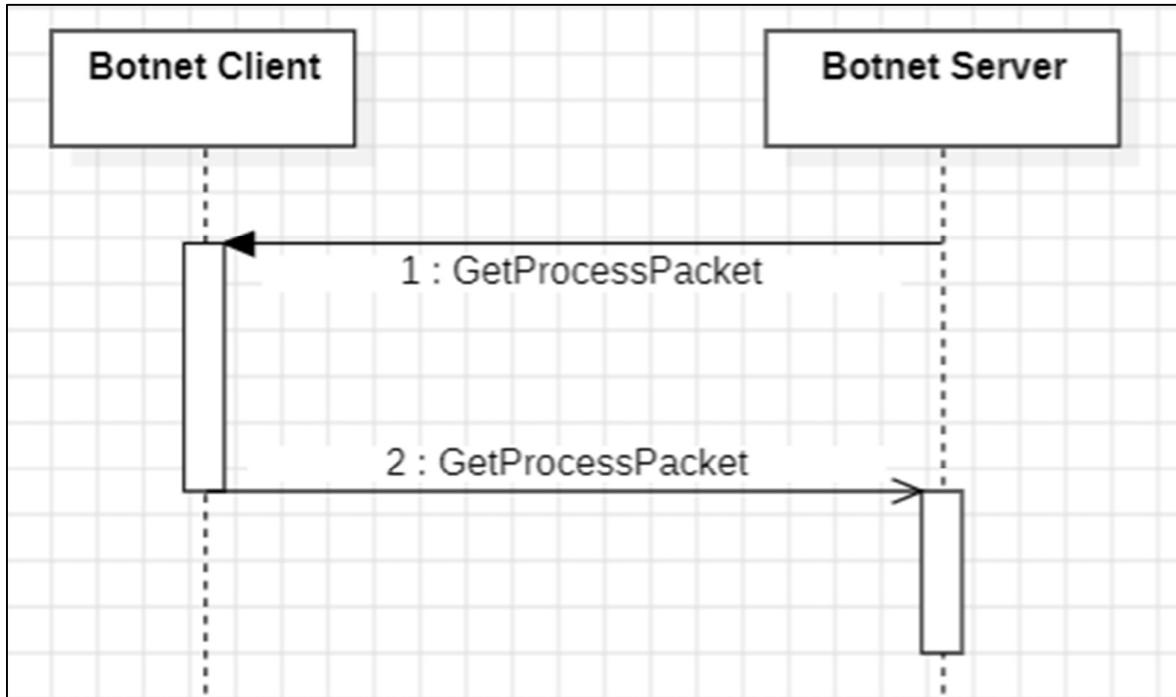
KeyLogger	0x60
-----------	------

GetKeyLoggerLogsDirectoryPacket(Client=> Server)

Id	0x60
LogsDirectory	String

2.2.3.6 Task Manager

Mô tả: Ở bước đầu tiên, Botnet Server gửi gói tin GetProcessPacket đến Botnet Client nhằm yêu cầu lấy danh sách các tiến trình đang chạy trên máy client. Sau khi nhận yêu cầu, Botnet Client tiến hành truy xuất thông tin tiến trình từ hệ điều hành và tổng hợp dữ liệu cần thiết. Tiếp theo, Botnet Client phản hồi lại Botnet Server bằng gói tin GetProcessPacket, kèm theo danh sách tiến trình.



Hình 17: Sơ đồ hoạt động Task Manager

Mô tả gói tin:

+ Gói tin 1(GetProcessPacket)

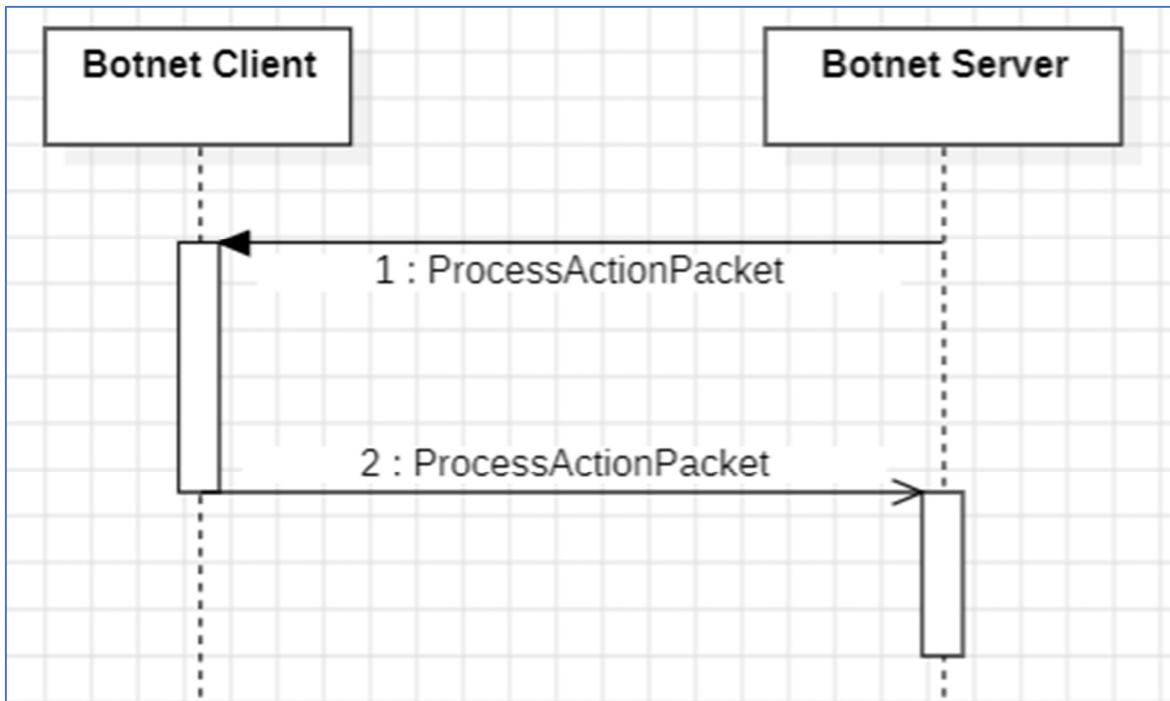
GetProcessPacket (Server=>Client)

Id	0x30
----	------

GetProcessPacket(Client=> Server)

Id	0x30
Length	Int
Array	{Name: String IdProcess: Int MainWindowTitle: String}

+ Gói tin 2(ProcessActionPacket)



Hình 18: Sơ đồ hoạt động ProcessActionPacket

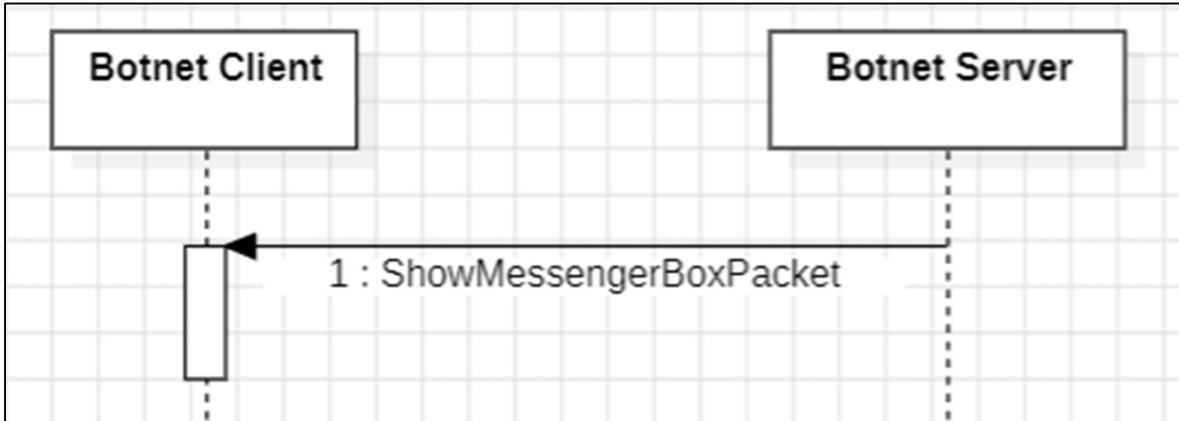
ProcessActionPacket(Server => Client)

Id	0x31
ProcessAction	Enum: [Start, End]
FilePath	String
Pid	Int

ProcessActionPacket(Client => Server)

Id	0x31
ProcessAction	Enum: [Start, End]
Result	Bool

+ Gói tin 3(ShowMessageBoxPacket)



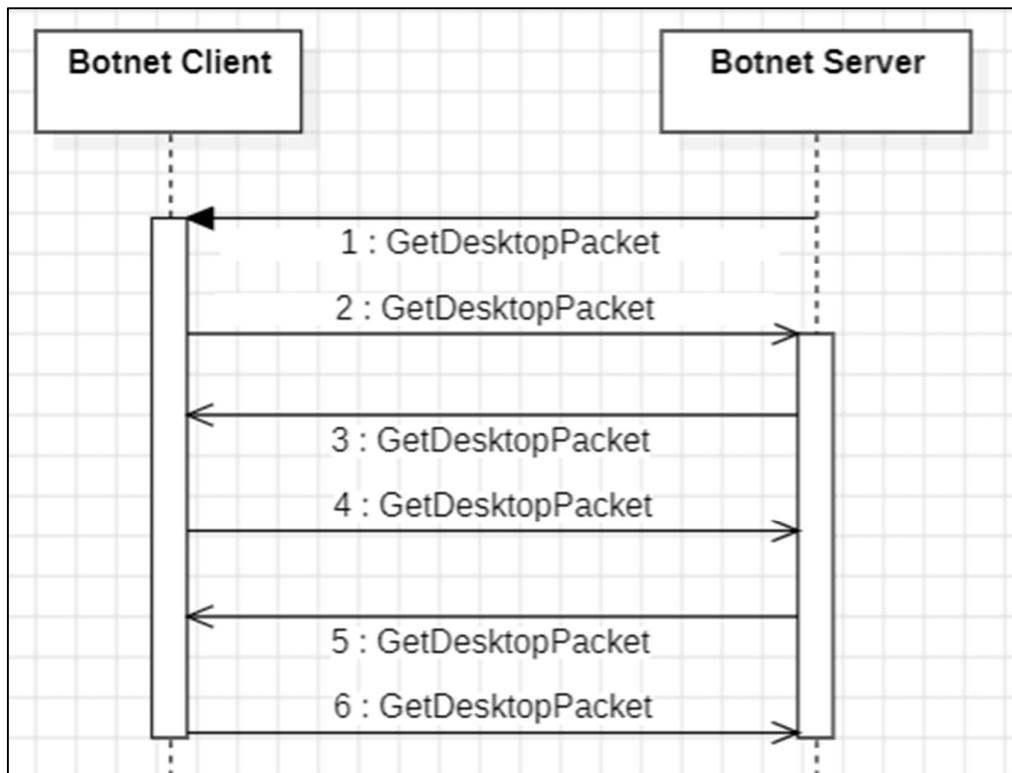
Hình 19: Sơ đồ hoạt động ShowMessageBoxPacket

ShowMessageBoxPacket(Server => Client)

Id	0x50
Caption	String
Text	String
Button	String
Icon	String

2.2.3.7 Remote Desktop

+ Gói tin 1(GetDesktopPacket)



Hình 20: Sơ đồ hoạt động GetDesktopPacket

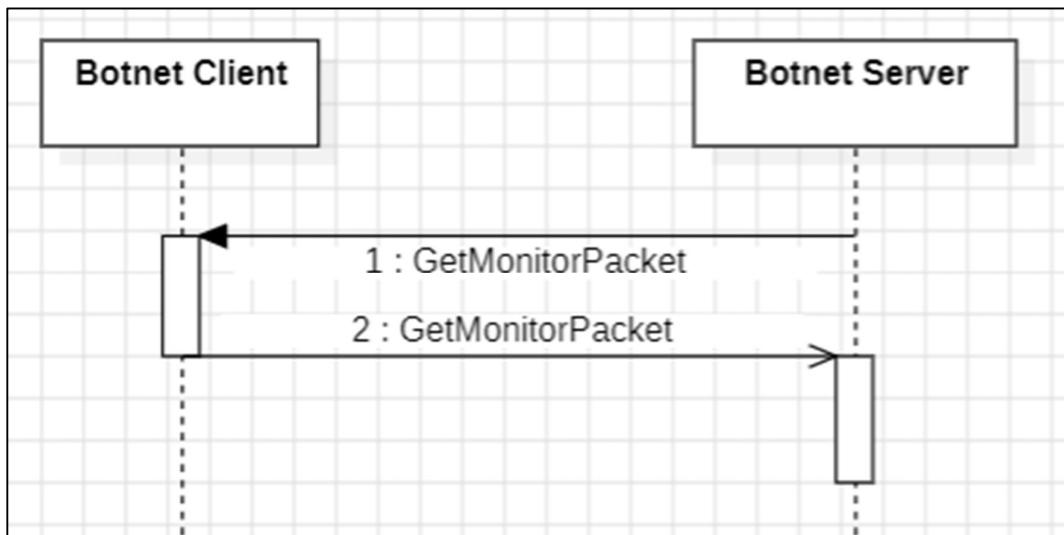
GetDesktopPacket(Server => Client)

Id	0x70
CreateNew	Bool
Quanlity	Int
DisplayIndex	Int

GetDesktopPacket(Client=> Server)

Id	0x70
Image	Byte[]
Quanlity	Int
Monitor	Int
Width	Int
Height	Int

+ Gói tin 2(GetMonitorPacket)



Hình 21: Sơ đồ hoạt động GetMonitorPacket

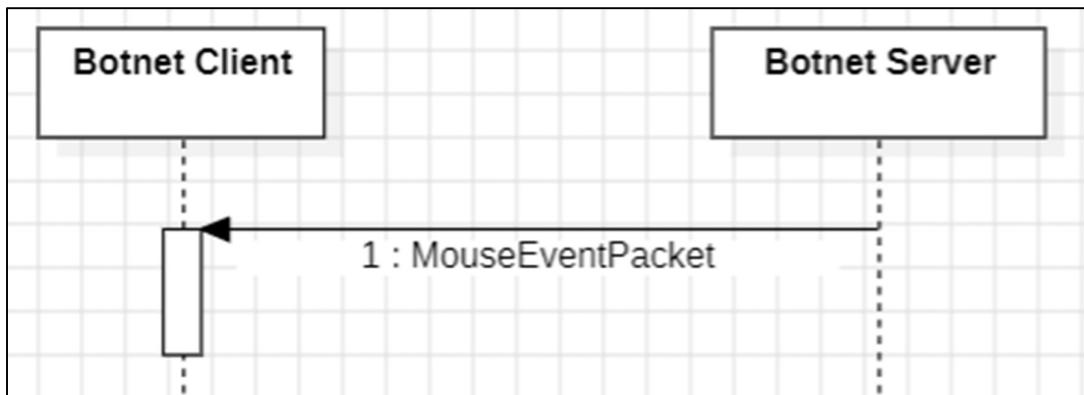
GetMonitorPacket(Client => Server)

Id	0x71
----	------

GetMonitorPacket(Server => Client)

Id	0x71
Number	Int

+ Gói tin 3(MouseEventPacket)



Hình 22: Sơ đồ hoạt động MouseEventPacket

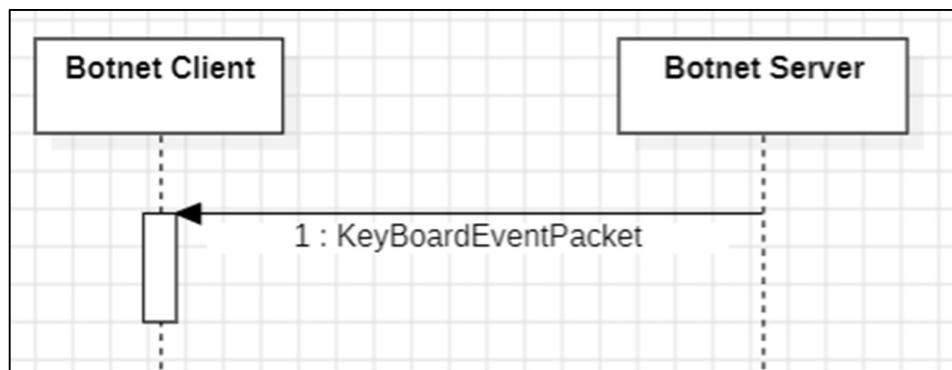
MouseEventPacket(Server=> Client)

Id	0x72
Action	Short: Enum: [MouseAction]
isMouseDown	Bool

X	Int
Y	Int
Monitor	Index

```
MouseAction{  
    LeftDown,  
    LeftUp,  
    RightDown,  
    RightUp,  
    MoveCursor,  
    ScrollUp,  
    ScrollDown,  
    None  
}
```

+ Gói tin 4(KeyBoardEventPacket)

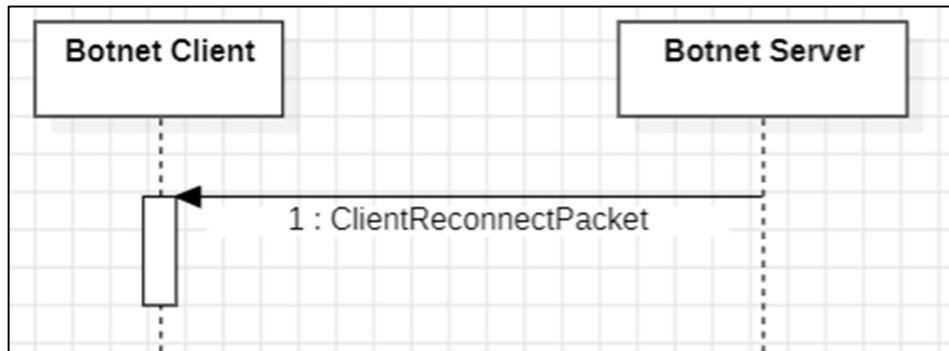


Hình 23: Sơ đồ hoạt động KeyBoardEventPacket

KeyBoardEventPacket(Server=> Client)

Id	0x73
Key	Byte
KeyDown	Bool

+ Gói tin 5(ClientReconnectPacket)

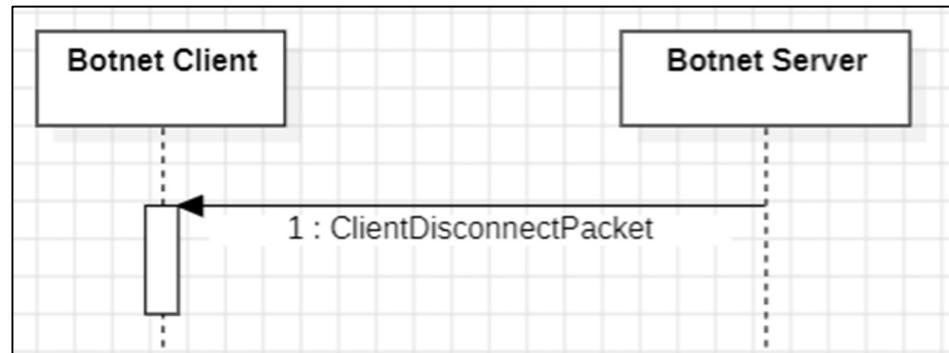


Hình1: Sơ đồ hoạt động ClientReconnectPacket

ClientReconnectPacket(Server=> Client)

Id	0x04
----	------

+ Gói tin 6 (ClientDisconnectPacket)

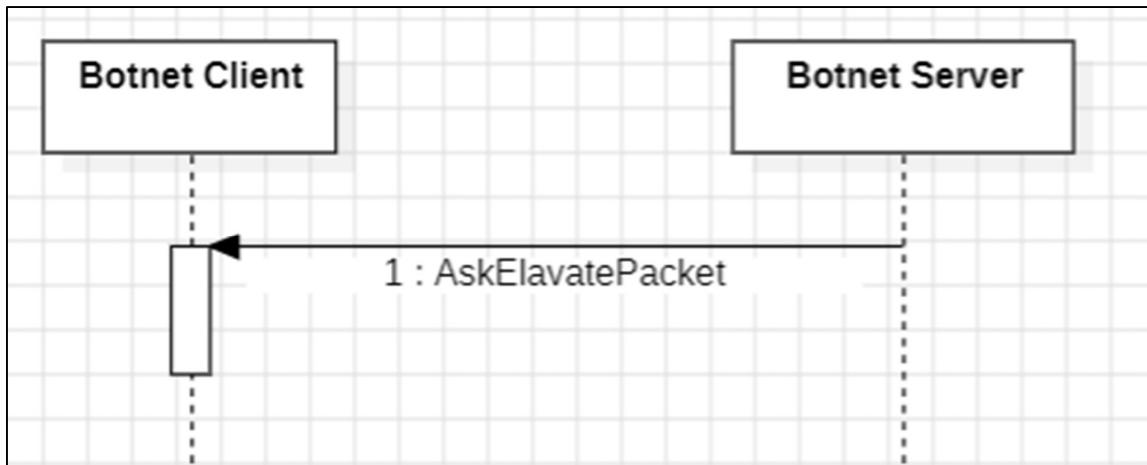


Hình 24: Sơ đồ hoạt động ClientReconnectPacket

ClientDisconnectPacket(Server=>Client)

Id	0x05
----	------

+ Gói tin 7(AskElavatePacket)

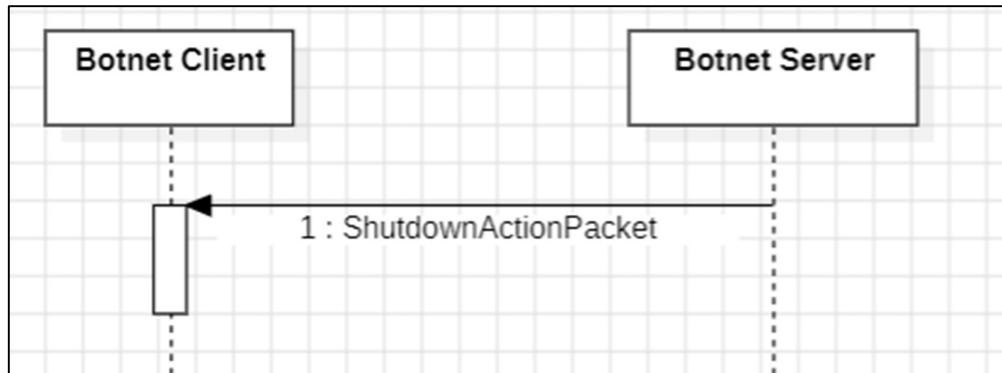


Hình 25: Sơ đồ hoạt động AskElavatePacket

AskElavatePacket(Server=> Client)

Id	0x06
----	------

+ Gói tin 8(ShutdownActionPacket)



Hình 26: Sơ đồ hoạt động ShutdownActionPacket

ShutdownActionPacket(Server=>Client)

Id	0x07
Action	ShutDownAction: [“ShutDown”, “Restart”, “StandBy”]

CHƯƠNG 3: DEMO ỦNG DỤNG VÀ ĐÁNH GIÁ KẾT QUẢ

3.1. Kết quả thực thi của chương trình

3.1.1. Giao diện quản lý chung

Giao diện quản lý chung của hệ thống đóng vai trò là màn hình trung tâm dùng để giám sát và quản lý các máy client đang kết nối đến máy chủ. Giao diện hiển thị danh sách các client theo dạng bảng, cung cấp thông tin tổng quan về trạng thái kết nối trong hệ thống.

Các thông tin chính được hiển thị bao gồm địa chỉ IP, tên người dùng và máy tính, hệ điều hành đang sử dụng, quốc gia trạng thái kết nối, trạng thái hoạt động của từng client. Thông qua các thông tin này, người quản trị có thể nhanh chóng nắm bắt tình trạng hiện tại của từng client đang hoạt động trong hệ thống.

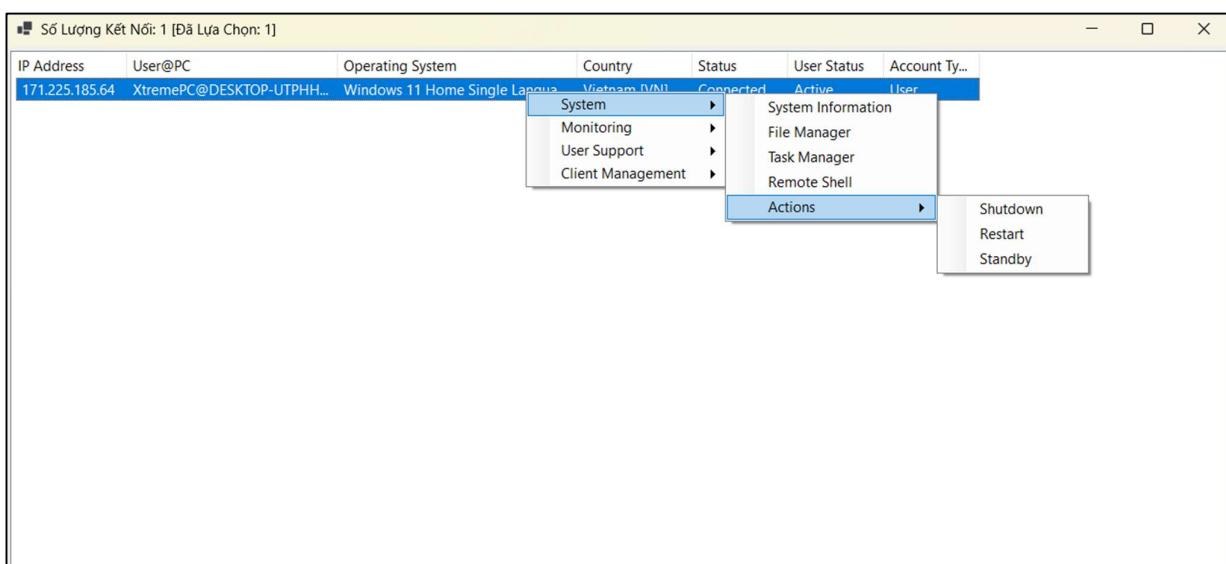
Số Lượng Kết Nối: 1							
IP Address	User@PC	Operating System	Country	Status	User Status	Account Ty...	
171.225.185.64	XtremePC@DESKTOP-UTPHH...	Windows 11 Home Single Langua...	Vietnam [VN]	Connected	Active	User	

Hình 27: Giao diện quản lý chung

3.1.2. Giao diện các chức năng hệ thống

Cho phép người quản trị truy cập và điều khiển các chức năng chính của chương trình thông qua menu thao tác. Giao diện này được kích hoạt sau khi lựa chọn một máy client trong danh sách quản lý chung.

Các chức năng được tổ chức theo từng nhóm logic, bao gồm quản lý hệ thống, theo dõi người dùng, quản lý client thực hiện các hành động điều khiển từ xa.

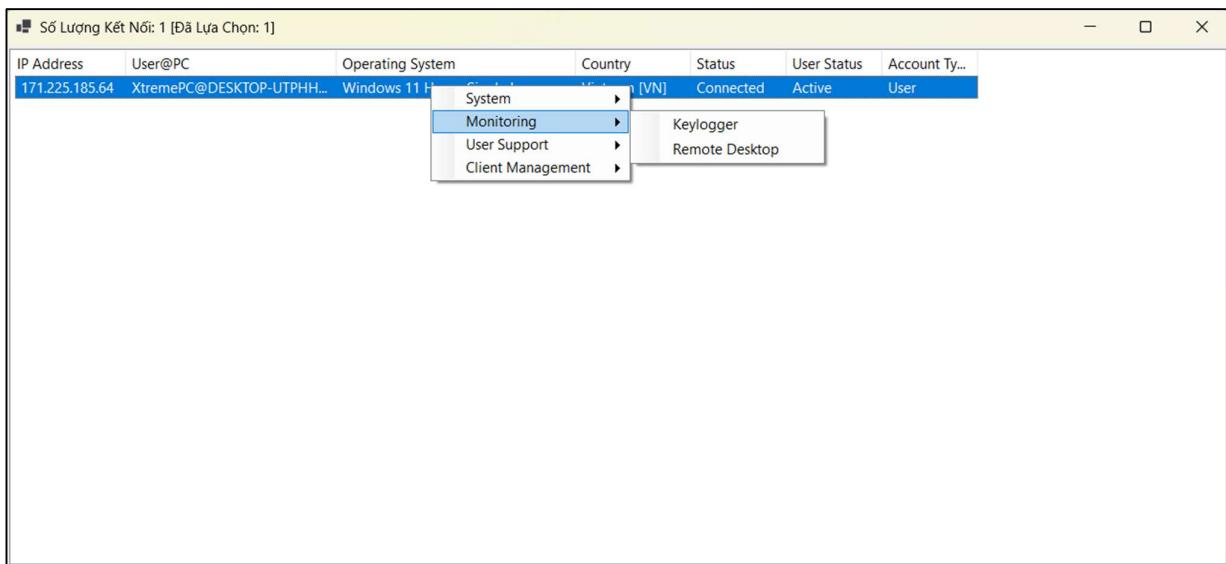


Hình 28: Giao diện các chức năng hệ thống

3.1.3. Giao diện các chức năng theo dõi hệ thống

Cho phép người quản trị truy cập và điều khiển các chức năng chính của chương trình thông qua menu theo dõi (Monitoring). Giao diện này được sử dụng sau khi lựa chọn một client đang kết nối trong danh sách quản lý.

Các chức năng theo dõi hệ thống bao gồm Keylogger và Remote Desktop, giúp ghi nhận hành vi nhập liệu và quan sát trực tiếp màn hình của máy client trong quá trình hoạt động.

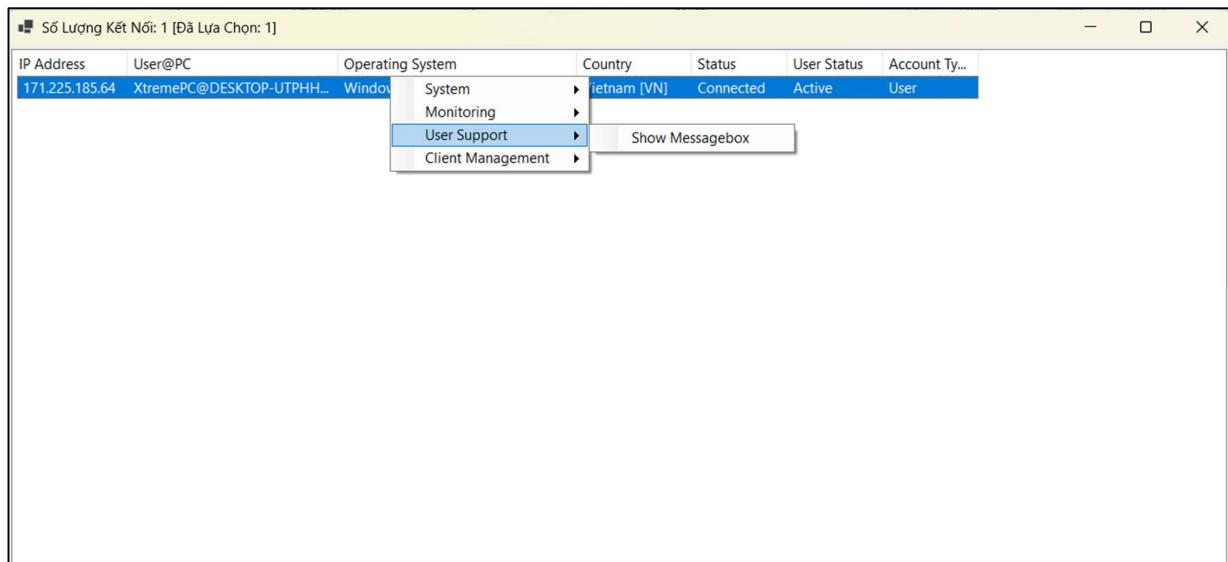


Hình 29: Giao diện các chức năng theo dõi hệ thống

3.1.4. Giao diện các chức năng người dùng

Giao diện này cho phép người quản trị tương tác trực tiếp với người dùng đang làm việc trên máy client thông qua các thao tác hỗ trợ từ xa.

Chức năng chính trong nhóm này là hiển thị thông báo (Show Messagebox) trên máy client, cho phép gửi các thông điệp cảnh báo, hướng dẫn hoặc thông tin cần thiết đến người dùng. Các thông báo được hiển thị trực tiếp trên màn hình máy client nhằm đảm bảo người dùng có thể nhận được nội dung một cách kịp thời.

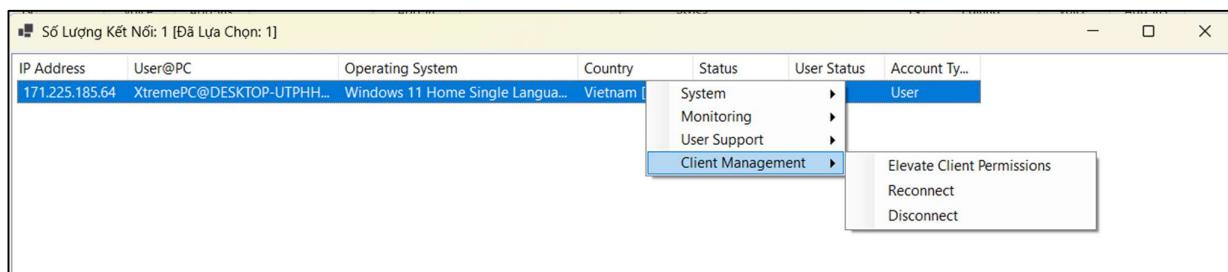


Hình 30: Giao diện các chức năng người dùng

3.1.5. Giao diện các chức năng client

Giao diện này cho phép người quản trị thực hiện các thao tác quản lý trực tiếp đối với từng máy client đang kết nối thông qua menu điều khiển trong ứng.

Các chức năng quản lý client bao gồm nâng quyền thực thi cho client (Elevate Client Permissions), ngắt kết nối và kết nối lại client với máy chủ. Những thao tác này hỗ trợ việc duy trì trạng thái kết nối ổn định, xử lý các tình huống gián đoạn mạng, cũng như kiểm soát quyền thực thi trong quá trình vận hành hệ thống.



Hình 31: Giao diện các chức năng client

3.1.6. Giao diện thông tin hệ thống

Chức năng này cho phép thu thập và hiển thị các thông tin tổng quan về phần cứng, hệ điều hành và trạng thái mạng của máy client đang kết nối đến máy chủ.

Các thông tin được hiển thị bao gồm bộ xử lý (CPU), dung lượng bộ nhớ (RAM), card đồ họa (GPU), tên người dùng, tên máy, ổ đĩa hệ thống, thư mục hệ thống, thời gian hoạt động (uptime), địa chỉ MAC, địa chỉ IP nội bộ (LAN), địa chỉ IP công cộng (WAN) ...

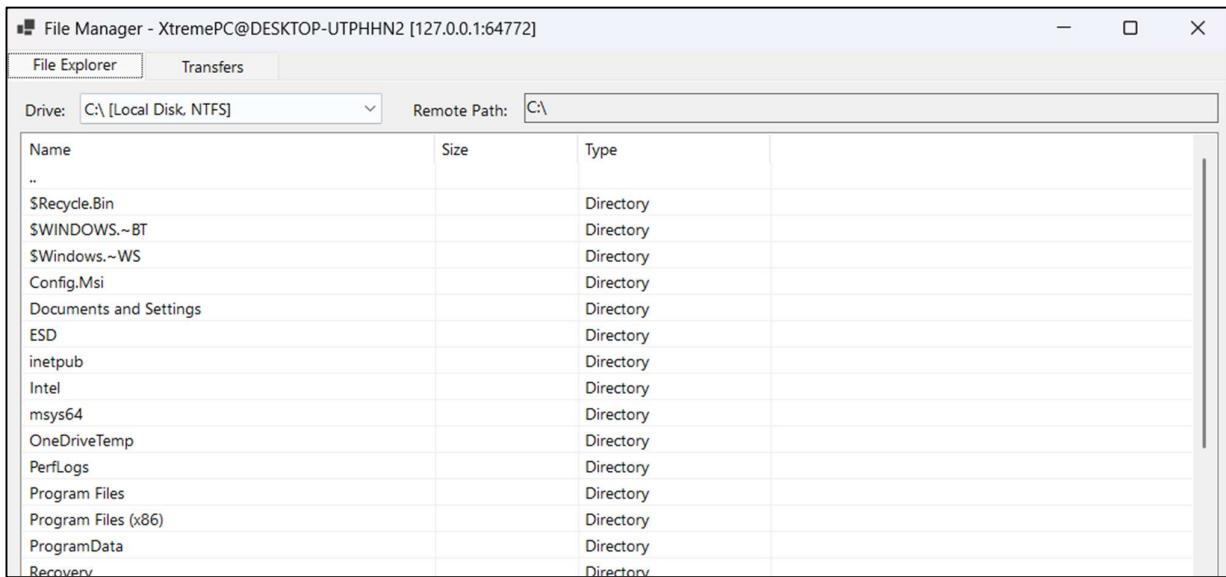
System Information - XtremePC@DESKTOP-UTPHHN2 [127.0.0.1:50219]	
Component	Value
Processor (CPU)	11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz
Memory (RAM)	16106 MB
Video Card (GPU)	NVIDIA GeForce RTX 3050 Ti Laptop GPU
Username	XtremePC
PC Name	DESKTOP-UTPHHN2
Domain Name	-
Host Name	DESKTOP-UTPHHN2
System Drive	C:\
System Directory	C:\WINDOWS\system32
Uptime	8d : 11h : 38m : 37s
MAC Address	F8:54:F6:3C:30:37
LAN IP Address	192.168.1.11
WAN IP Address	171.225.185.64
ASN	7552
ISP	Viettel Group
Antivirus	Windows Defender
Firewall	N/A
Time Zone	+07:00

Hình 32: Giao diện thông tin hệ thống

3.1.7. Giao diện quản lý tệp tin

Giao diện này cho phép người quản trị duyệt và quản lý cấu trúc thư mục trên máy client thông qua kết nối từ xa, tương tự như trình quản lý tệp tin trên hệ điều hành cục bộ.

Qua giao diện, người quản trị có thể truy cập các ổ đĩa, duyệt danh sách thư mục và tệp tin, đồng thời xem các thông tin cơ bản như tên, loại và kích thước của tệp. Giao diện hỗ trợ chuyển đổi nhanh đường dẫn làm việc, giúp việc điều hướng trong hệ thống tệp của client trở nên thuận tiện.



Hình 33: Giao diện quản lý tệp tin

3.1.8. Giao diện các tác vụ

Giao diện này cho phép người quản trị theo dõi danh sách các tiến trình đang chạy trên máy client thông qua kết nối từ xa.

Danh sách tác vụ được hiển thị dưới dạng bảng, bao gồm các thông tin như tên tiến trình, mã định danh tiến trình (PID) và tiêu đề cửa sổ tương ứng. Thông qua giao diện này, người quản trị có thể thực hiện các thao tác cơ bản như làm mới danh sách tiến trình, khởi chạy tiến trình mới hoặc kết thúc các tiến trình đang hoạt động.

The screenshot shows a Windows-style task manager window titled "Task Manager - XtremePC@DESKTOP-UTPHHN2 [127.0.0.1:53098]". The table lists the following processes:

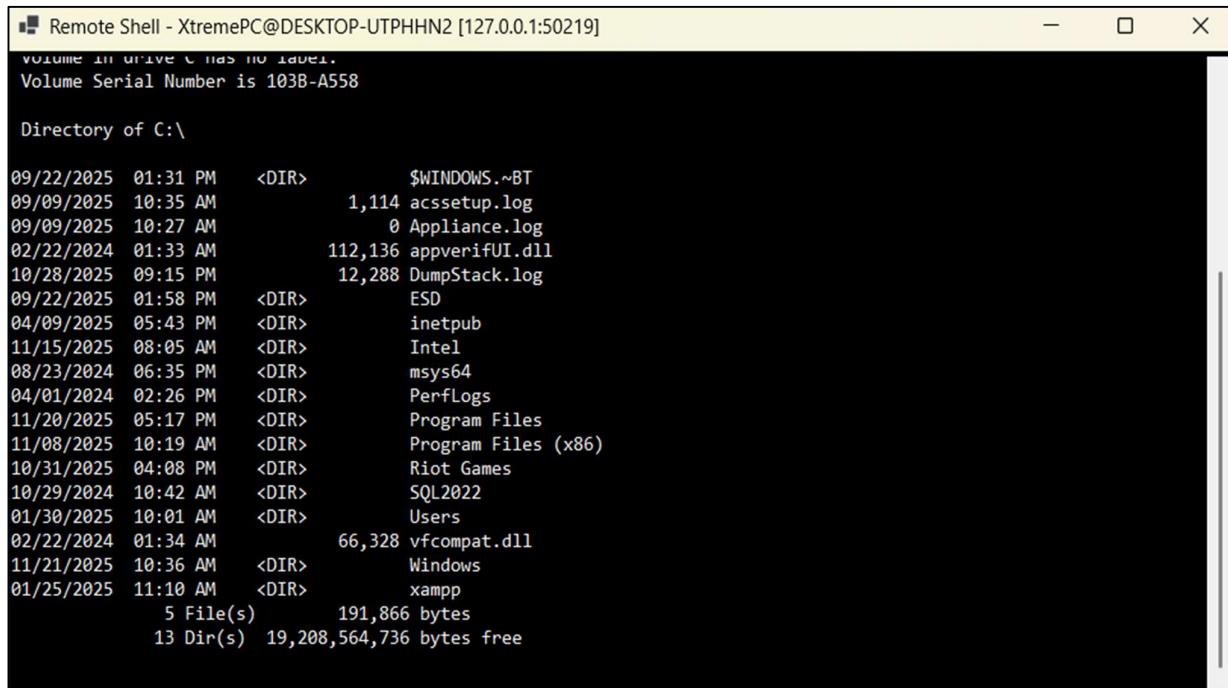
Process Name	PID	Title
Idle.exe	0	
System.exe	4	
Secure System.exe	236	
Registry.exe	280	
smss.exe	872	
csrss.exe	1448	
wininit.exe	1552	
services.exe	1624	
lalso.exe	1668	
lsass.exe	1676	
svchost.exe	1816	
fontdrvhost.exe	1836	
svchost.exe	1904	

Hình 34: Giao diện các tác vụ

3.1.9. Giao diện shell từ xa

Chức năng này cho phép người quản trị gửi và thực thi các dòng lệnh trực tiếp trên máy client thông qua kết nối mạng, đồng thời nhận lại kết quả thực thi theo thời gian thực.

Giao diện hiển thị tương tự như cửa sổ Command Prompt trên hệ điều hành Windows, giúp người sử dụng dễ dàng thao tác và theo dõi kết quả. Các lệnh này đều được thực hiện từ xa mà không cần truy cập trực tiếp vào máy client.



The screenshot shows a terminal window titled "Remote Shell - XtremePC@DESKTOP-UTPHHN2 [127.0.0.1:50219]". It displays a directory listing for the C:\ drive. The output is as follows:

```
VOLUME IN DRIVE C HAS NO LABEL.
Volume Serial Number is 103B-A558

Directory of C:\

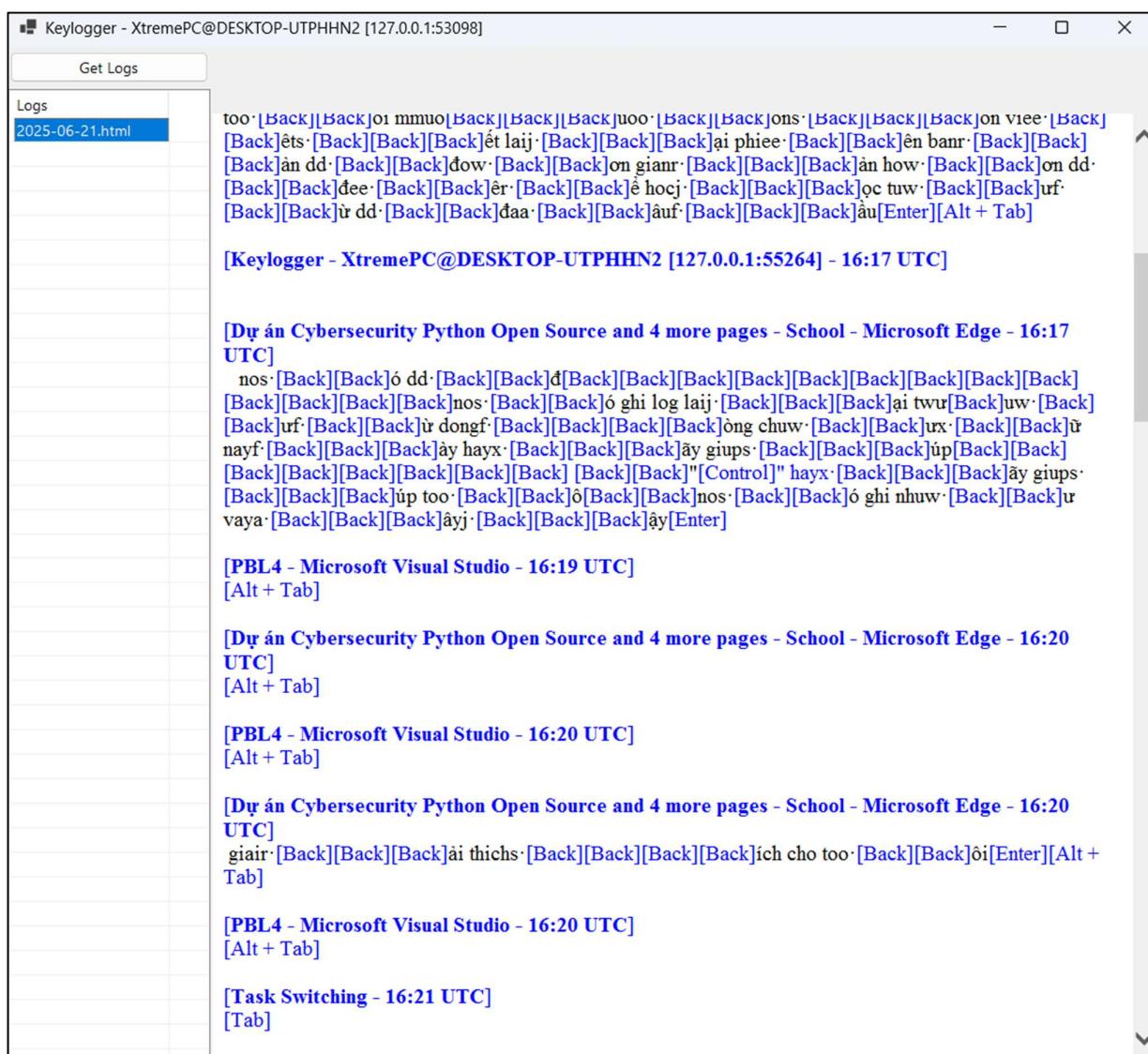
09/22/2025  01:31 PM    <DIR>      $WINDOWS.~BT
09/09/2025  10:35 AM        1,114 acssetup.log
09/09/2025  10:27 AM          0 Appliance.log
02/22/2024  01:33 AM       112,136 appverifUI.dll
10/28/2025  09:15 PM       12,288 DumpStack.log
09/22/2025  01:58 PM    <DIR>      ESD
04/09/2025  05:43 PM    <DIR>      inetpub
11/15/2025  08:05 AM    <DIR>      Intel
08/23/2024  06:35 PM    <DIR>      msys64
04/01/2024  02:26 PM    <DIR>      PerfLogs
11/20/2025  05:17 PM    <DIR>      Program Files
11/08/2025  10:19 AM    <DIR>      Program Files (x86)
10/31/2025  04:08 PM    <DIR>      Riot Games
10/29/2024  10:42 AM    <DIR>      SQL2022
01/30/2025  10:01 AM    <DIR>      Users
02/22/2024  01:34 AM        66,328 vfccompat.dll
11/21/2025  10:36 AM    <DIR>      Windows
01/25/2025  11:10 AM    <DIR>     xampp
      5 File(s)      191,866 bytes
     13 Dir(s)  19,208,564,736 bytes free
```

Hình 35: Giao diện Shell từ xa

3.1.10.Giao diện Keylogger

Giao diện cho phép người quản trị theo dõi và truy xuất các dữ liệu nhập phím đã được thu thập từ phía máy client trong quá trình hoạt động. Danh sách các tệp log được hiển thị theo mốc thời gian, giúp dễ dàng quản lý và tra cứu dữ liệu theo từng phiên làm việc cụ thể.

Nội dung log bao gồm các ký tự được nhập từ bàn phím, kèm theo thông tin ngữ cảnh như thời gian ghi nhận và ứng dụng đang được sử dụng tại thời điểm nhập liệu. Điều này giúp phản ánh chính xác hành vi nhập liệu của người dùng trong môi trường thử nghiệm.

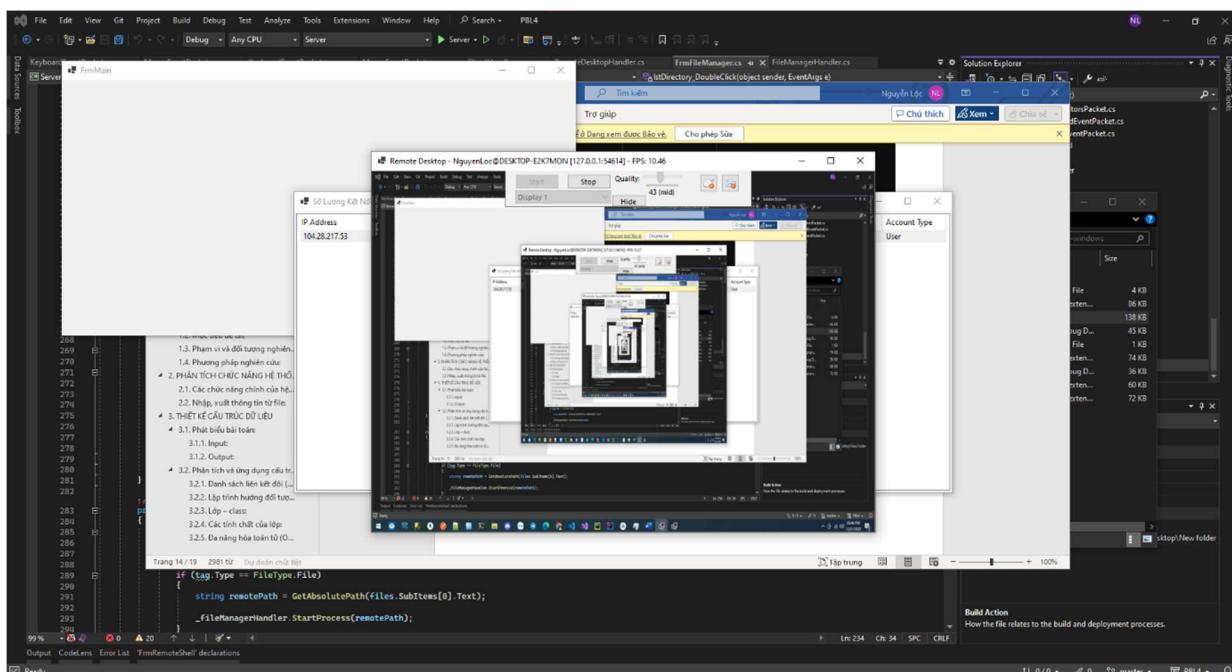


Hình 36: Giao diện Keylogger

3.1.11.Giao diện Remote Desktop

Chức năng này cho phép người quản trị quan sát trực tiếp màn hình máy client thông qua kết nối mạng, đồng thời phản ánh trạng thái làm việc của máy từ xa theo thời gian thực.

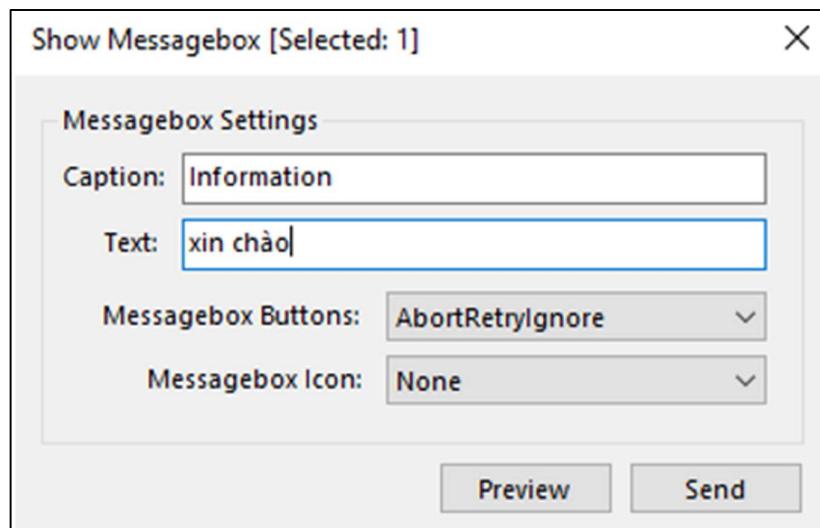
Giao diện hiển thị nội dung màn hình của client dưới dạng luồng hình ảnh liên tục. Hiện tượng lặp khung hình là kết quả của việc máy client đang chia sẻ chính màn hình đang hiển thị phiên Remote Desktop. Bên cạnh việc quan sát, còn hỗ trợ tương tác từ xa như điều khiển chuột và bàn phím.



Hình 37: Giao diện remote desktop

3.1.12.Giao diện hiển thị thông báo

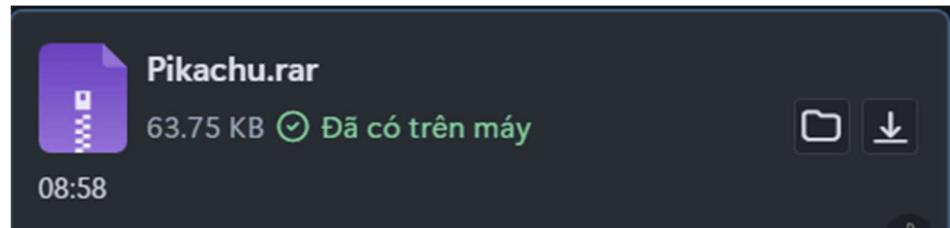
Chức năng này cho phép người quản trị soạn và gửi các thông báo trực tiếp đến máy client đang được lựa chọn. Cung cấp các tùy chọn cấu hình nội dung thông báo như tiêu đề (Caption), nội dung văn bản (Text), kiểu nút bấm và biểu tượng hiển thị. Trước khi gửi, người dùng có thể xem trước thông báo nhằm đảm bảo nội dung được hiển thị đúng như mong muốn trên máy client.



Hình 38: Giao diện hiển thị thông báo

3.2. Kết quả của việc vượt qua sự kiểm tra của Window Defender

Mô phỏng tình huống: Giả sử nạn nhân đang tải phần mềm trò chơi Pikachu từ một nguồn nào đó không đáng tin cậy:



Hình 39: File trò chơi Pikachu đính kèm mã độc

Sau khi nạn nhân tải về và mở lên để chơi trò chơi, khi đó file mã độc đã chạy ngầm mà nạn nhân không hề hay biết:



Hình 40: Giao diện trò chơi

Apps (1)					
> Client		0%	22.1 MB	0 MB/s	0 Mbps

Hình 41: Mã độc đang chạy ngầm

3.3. Đánh giá kết quả

Qua quá trình triển khai và thực nghiệm, hệ thống đã hoạt động đúng theo mục tiêu và định hướng ban đầu của đề tài. Các chức năng chính được xây dựng đầy đủ và vận hành ổn định trong môi trường thử nghiệm, đáp ứng yêu cầu quản lý, giám sát và tương tác từ xa giữa máy chủ và máy client. Cơ chế giao tiếp dựa trên TCP/IP cho thấy tính đồng bộ và độ tin cậy trong quá trình truyền nhận dữ liệu. Bên cạnh đó, nhóm đã thực hiện được chạy ẩn mã độc và vượt qua Window Defender. Tuy nhiên, hệ thống vẫn còn một số hạn chế về hiệu năng và khả năng xử lý ngoại lệ trong các điều kiện mạng không ổn định, cần tiếp tục được cải thiện trong các hướng phát triển tiếp theo.

CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

4.1. Kết luận

Nhóm đã thành công đáp ứng được các mục tiêu đã đề ra, thành công xây dựng, cài đặt chương trình Keylogger/ Botnet để thu thập dữ liệu, đánh cắp thông tin nhạy cảm của người dùng, điều khiển và theo dõi người dùng từ xa và vượt qua window defender.

Nhóm đã tìm hiểu và nắm được các cơ chế, truyền gói tin TCP/IP, bao gồm cách thức thiết lập kết nối, đóng gói – truyền – nhận dữ liệu giữa máy khách và máy chủ. Các kiến thức này được vận dụng trực tiếp vào việc thiết kế kiến trúc hệ thống, xây dựng các gói tin và triển khai xây dựng được một con Botnet.

Kết quả thực nghiệm cho thấy các chức năng chính của chương trình như thu thập dữ liệu nhập phím, quản lý tiến trình, truyền tệp và điều khiển màn hình từ xa hoạt động đúng theo thiết kế. Tuy nhiên, trong một số trường hợp, hệ thống vẫn tồn tại những hạn chế về tính ổn định và khả năng xử lý ngoại lệ, đặc biệt khi hoạt động trong môi trường mạng không ổn định.

Nhìn chung, đề tài đã đạt được mục tiêu học tập và nghiên cứu, góp phần giúp nhóm hiểu rõ hơn về cơ chế hoạt động của mối đe dọa mạng phổ biến, từ đó nâng cao nhận thức về an toàn thông tin và các biện pháp phòng vệ trong thực tế.

4.2. Hướng phát triển

Xây dựng hệ thống hoàn chỉnh hơn, tối ưu tốc độ truyền tải gói tin, nâng cấp thêm chức năng để có thể khai thác nhiều thông tin từ người dùng hơn.

Thêm khả năng ngụy tạo trên cho Botnet (chạy ngầm, ẩn khỏi Task Manager ...). Nghiên cứu bổ sung cơ chế tăng tính ổn định và khả năng tự bảo vệ của chương trình, đồng thời cải thiện khả năng xử lý lỗi và các tình huống ngoại lệ phát sinh trong quá trình vận hành.

Cải thiện giao diện người dùng theo hướng trực quan và thân thiện hơn, giúp việc quản lý, theo dõi và thao tác hệ thống trở nên thuận tiện và hiệu quả.

TÀI LIỆU THAM KHẢO

- [1] M. Hạnh, “TCP/IP là gì? Kiến thức về giao thức mạng TCP/IP,” Quantrimang, 30 Tháng 8 2018. [Trực tuyến]. Nguồn: <https://quanzimang.com/cong-nghe/kien-thuc-ve-giao-thuc-mang-tcp-ip-48>. [Đã truy cập 12 Tháng 10 2025].
- [2] A. Duy, “Keylogger là phần mềm gì? Giải thích chi tiết và cách ngăn chặn hiệu quả” FPT Shop, 15 Tháng 12 2025. [Trực tuyến]. Nguồn: <https://fptshop.com.vn/tin-tuc/for-gamers/keylogger-la-phan-mem-gi-195608>. [Đã truy cập 20 Tháng 12 2025].
- [3] T. Nguyễn, “Keylogger là gì? Cách thức hoạt động và phòng tránh,” CryptoViet, 13 Tháng 1 2023. [Trực tuyến]. Nguồn: <https://cryptoviet.com/keylogger-la-gi/>. [Đã truy cập 1 Tháng 12 2025].
- [4] “Botnet là gì? Cách phòng chống DDoS Botnet hiệu quả,” viettel idc, 2 Tháng 10 2024. [Trực tuyến]. Nguồn: <https://viettelidc.com.vn/tin-tuc/botnet-la-gi-cung-viettel-idc-tim-hieu-chi-tiet-ve-7-loai-tan-cong-botnet-3002>. [Đã truy cập 8 Tháng 10 2025].
- [5] “Windows Defender là gì? Hướng dẫn bật/tắt nhanh trên win 10/11,” LAPTOPS.VN, [Trực tuyến]. Nguồn: <https://laptops.vn/entity/windows-defender-la-gi/>. [Đã truy cập 12 Tháng 10 2025].
- [6] “quasar/Quasar: Remote Administration Tool for Windows,” Github, 17 Tháng 3 2024. [Trực tuyến]. Nguồn: <https://github.com/quasar/Quasar>. [Đã truy cập 10 Tháng 4 2025].
- [7] “Botnet,” Wikipedia, [Trực tuyến]. Nguồn: <https://vi.wikipedia.org/wiki/Botnet>. [Đã truy cập 1 Tháng 7 2025].

