HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN

NGHIÊN CỨU VÀ PHÁT TRIỂN MÃ ĐỘC NGỤY TRANG VÀ CHE GIẤU HÀNH VI

Giảng viên hướng dẫn	**:**	**TS. Đỗ Xuân Chợ**
Học phần	**:**	**Mật mã học cơ sở**
Sinh viên thực hiện	**:**	Nguyễn Ngọc Quân – B20DCAT002
		Đinh Việt Anh – B20DCAT005
		Phạm Khắc Phong – B20DCAT138
		My Phạm Trung Hiếu – B20DCAT058
		Phạm Vũ Minh Hiếu – B20DCAT061
Hệ đào tạo	**:**	**Đại học chính quy**

Hà Nội, tháng 11 năm 2022

MỤC LỤC

LỜI MỞ ĐẦU

Ngày nay, với sự phát triển nhanh chóng và mạnh mẽ của internet, an ninh mạng, an ninh thông tin cũng đang trở thành một chiến trường mới.

Để không bị tụt lại phía sau trong cuộc "chạy đua vũ trang" mới này, chúng ta cần phải học cách tạo ra vũ khí mới, bắt kịp xu thế. Mã độc là một vũ khí vô cùng mạnh, đa dạng về kĩ thuật, phương thức tấn công. Bài nghiên cứu này của chúng em tập trung nghiên cứu một số kỹ thuật tạo ra mã độc hiện nay và giới thiệu về kịch bản mã độc có thể sử dụng để lây lan vào máy nạn nhân, từ đó tiến hành một cuộc tấn công mã độc.

CHƯƠNG I. TỔNG QUAN VỀ MÃ ĐỘC

Chương I trình bày khái niệm về mã độc và các thông tin liên quan đến mã độc như: các dạng mã độc, phương thức hoạt động và lịch sử phát triển của mã độc.

1. GIỚI THIỆU VỀ MÃ ĐỘC

Mã độc (malware) là khái niệm chung cho những phần mềm nguy hiểm. Từ mã độc (malware) là sự kết hợp giữa Malicious và Software. Mã độc được thiết kế nhằm gây hại cho máy tính, máy chủ, người dùng và mạng máy tính.

Ngày nay mã độc đã phát triển rất đa dạng về chủng loại và môi trường phát tán. Ngoài việc hoạt động trên máy tính của người dùng, mã độc còn lây lan trên các thiết bị IOT.

Khi lây lan qua các thiết bị, mã độc có thể đánh cắp các thông tin nhạy cảm của người dùng như mật khẩu, tài khoản ngân hàng,… Tấn công tống tiền bằng cách mã hóa các tệp dữ liệu quan trọng.

Mã độc cũng được sử dụng như một phần mềm gián điệp cho các tổ chức, cơ quan,… với mục đích cạnh tranh, chính trị,…

2. LỊCH SỬ PHÁT TRIỂN MÃ ĐỘC

Mã độc đã là sự đe dọa từ khi kỉ nguyên của máy tính bắt đầu.

Với khả năng của người tấn công, mã độc ngày càng phát triển mạnh mẽ, bất kể thứ gì có bộ vi xử lý đều có nguy cơ bị lây nhiễm. Mã độc có thể được phát triển để xâm nhập thông qua các lỗ hổng của các phần mềm, vượt mặt các hàng rào an ninh của hệ thống, rồi từ đó lây nhiễm thông qua mạng máy tính.

Trong tương lai không xa, mã độc được dự đoán sẽ có các bước tiến mạnh mẽ, vượt bậc hơn. Mã độc sẽ được kết hợp với các kĩ thuật mới, những thủ đoạn tinh vi hơn. Chúng sẽ hoạt động đa dạng trên nhiều môi trường chứ không chỉ là Microsoft Windows như hiện nay.

Dựa trên những hiểu biết đã có, các lập trình viên mã độc sẽ còn cho ra đời những loại mã đọc tinh vi hơn, nhằm đạt hiệu quả cao hơn cho các cuộc tấn công với qui mô lớn.

3. PHÂN LOẠI MÃ ĐỘC

Các loại mã độc phổ biến

Một số loại mã độc thường gặp hiện nay có thể kể đến là:

- **Spyware:** Những phần mềm mã độc do thám máy tính. Spyware được cài đặt lặng lẽ và bí mật thông qua các phần mềm miễn phí. Spyware có thể gây chậm trễ internet, hoặc làm máy tính chậm đi do chiếm tài nguyên như RAM và chu kì làm việc của CPU.
- **Ransomware:** Mã độc chuyên mã hóa dữ liệu hoặc khóa quyền truy cập của người dùng. Để được trả lại quyền truy cập thiết bị hoặc dữ liệu bị mã hóa, người dùng phải trả cho hacker một khoản nhất định, gọi là tiền chuộc. Sau khi bị mất quyền truy cập hoặc mã hóa dữ liệu, hacker sẽ để lại một số thông tin để nạn nhân có trả tiền chuộc. Ransomware còn được biết đến với cái tên phần mềm tống tiền hay mã độc tống tiền.
- **Trojan horse:** Virus Trojan Horse là loại Virus phát tán bằng cách đánh lừa những người dùng cả tin để chạy nó. Ví dụ của Virus Trojan Horse sẽ yêu cầu người dùng mở thư Email đính kèm trong Microsoft Outlook. Nạn nhân đang chạy Virus Trojan thông thường sẽ cung cấp cho kẻ tấn công một vài mức độ để điều khiển lại máy tính

của nạn nhân. Điều khiển này có thể có phép kể tấn công truy cập từ xa tới máy tính nạn nhân, hoặc để ra lệnh tới những máy tính cũng là nạn nhân khác.

- **Remote Access Trojan (RAT):** Loại mã độc cho phép hacker giám sát và điều khiển máy tính hoặc mạng của bạn. RAT rất giống với các phần mềm truy cập từ xa hợp pháp, nhưng sự khác biệt chính là nó được cài đặt mà nạn nhân không hề biết. Hầu hết các chương trình truy cập từ xa hợp pháp được tạo ra cho việc hỗ trợ công nghệ và chia sẻ tệp, trong khi RAT được tạo ra để theo dõi, chiếm quyền điều khiển hoặc phá hủy máy tính.
- **Backdoor:** một loại phần mềm độc hại cung cấp thêm "lối vào" bí mật của hệ thống cho những kẻ tấn công. Nếu chỉ sử dụng mình nó, nó không gây ra bất kỳ tác hại nào nhưng cung cấp cho kẻ tấn công một công cụ tấn công lợi hại hơn. Bởi vì điều này, backdoors không bao giờ được sử dụng độc lập. Thông thường, chúng được sử dụng kết hợp với các phần mềm độc hại khác.
- **Keylogger:** Mã độc ghi lại tất cả các phím người dùng đã bấm và các cửa sổ bấm phím đó. Kết quả của việc thu thập này, hacker có thể lấy được thông tin về tài khoản ngân hàng, tài khoản mail, mọi loại mật khẩu của người dùng. Thông thường keylogger sẽ được tích hợp vào trong các loại mã độc khác để tang hiệu quả tấn công.
- **Virus:** Virus máy tính là chương trình có khả năng tự nhân rộng chính nó bằng cách chỉnh sửa chương trình khác và chèn mã riêng của nó. Nó có thể làm hỏng dữ liệu, thay đổi dữ liệu hoặc làm giảm hiệu suất của hệ thống máy tính bằng cách chiếm dụng tài nguyên của hệ thống như: bộ nhớ hoặc khoảng trống trên đĩa. Có một số loại virus chính thường gặp là Virus Macro, Virus Boot Sector, Worm.
- **Adware:** mã độc được thiết kế để hiển thị quảng cáo trên màn hình của bạn, thường xuyên nhất trong trình duyệt web. Adware có thể làm châm máy tính do chiếm bộ nhớ RAM và các chu kì làm việc của CPU. Adware cũng làm giảm hiệu quả truy cập internet vì nó chiếm dụng băng thông cho việc quảng cáo. Thêm vào đó, Adware làm tăng độ bất ổn định cho hệ thống vì số lượng quả cáo nó tạo ra. Adware gây khó chịu cho người dùng vì mất thời gian đóng những PopUp do nó tạo ra.

- **Rootkit:** Rootkit là một chương trình máy tính bí mật được thiết kế để cung cấp quyền truy cập liên tục vào máy tính đồng thời chủ động che giấu sự hiện diện của nó. Thuật ngữ rootkit là sự kết nối của hai từ "root" và "kit". Rootket thường gắn liền với phần mềm độc hại chẳng hạn như Trojan, sâu, vi rút - che giấu sự tồn tại và hành động của chúng khỏi người dùng và các quy trình hệ thống khác. Chúng cũng có khả năng leo quyền trên hệ thống nạn nhân.

4. KẾT CHƯƠNG

Như vậy chương 1 đã cho chúng ta cái nhìn tổng quát về mã độc, khái niệm, lịch sử và phân loại mã độc.

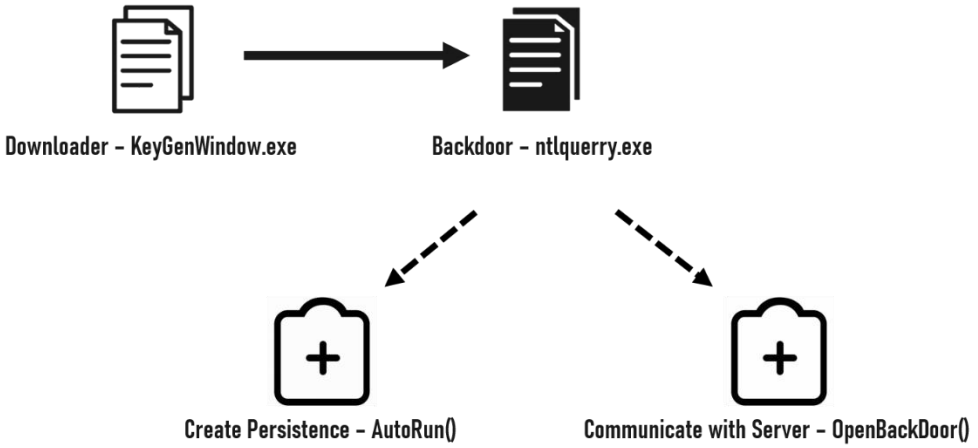
CHƯƠNG II. XÂY DỰNG MÃ ĐỘC VÀ NGỤY TRANG CHE GIẤU HÀNH VI ĐỘC HẠI

Chương II trình bày về cách xây dựng mã độc và giải thích chức năng từng module, qua đó giới thiệu về cách mã độc ngụy trang, che giấu hành vi độc hại.

1. MÔ HÌNH TỔNG QUAN

Mẫu mã độc gồm 2 file chính:

- **Keygen.exe**: Mã độc ngụy trang thành phần mềm sinh khóa để lây nhiễm vào máy nạn nhân. Sau khi được thực thi, mã độc kết nối vào Internet và truy cập đến máy chủ điều khiển C&C và thực hiện chức năng tự cập nhật.
- **ntlquerry.exe**: Sau khi được cài vào máy nạn nhân, mã độc ngay lập tức được thực thi và tạo một backdoor để giao tiếp với máy chủ điều khiển. Mã độc gồm 2 module chính với các chức năng lần lượt như sau:
  - ***AutoRun()***: Module có nhiệm vụ tạo persistence trên máy victim. Sau khi tạo persistence, mã độc sẽ tự thực thi mỗi khi máy được khởi động.
  - ***OpenBackDoor()***: Module khi được chạy sẽ tạo một kênh liên lạc (backdoor) mã hóa giữa máy victim và server, từ đó attacker có quyền điều khiển máy victim và thực thi hành vi độc hại.

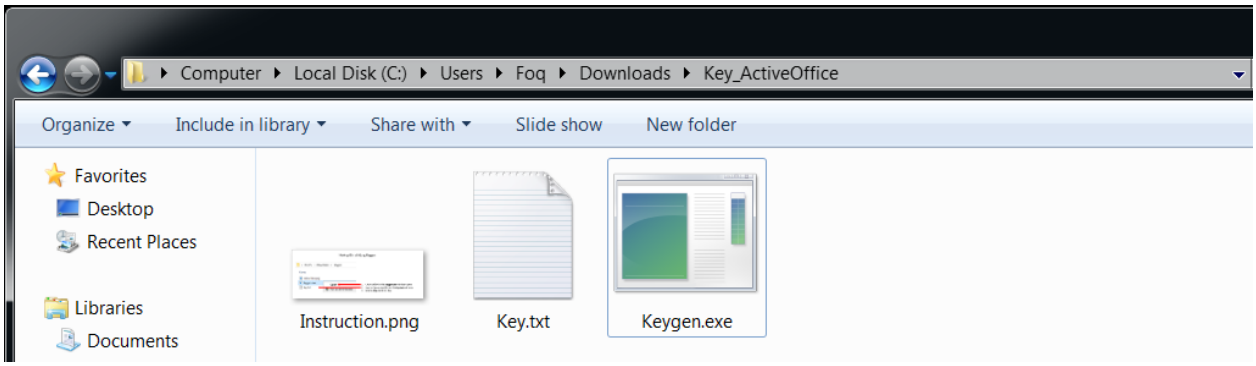


Sơ đồ mô hình tổng quan mã độc trên máy nạn nhân

2. QUÁ TRÌNH LÂY NHIỄM VÀ LUỒNG THỰC THI CỦA MÃ ĐỘC

2.1. Hành vi ngụy trang phần mềm sinh khóa (Masquerading)

Dưới góc nhìn của nạn nhân là người dùng thông thường, mã độc sau khi được thực thi sẽ tạo file *Key.txt* chứa khóa vừa được sinh.

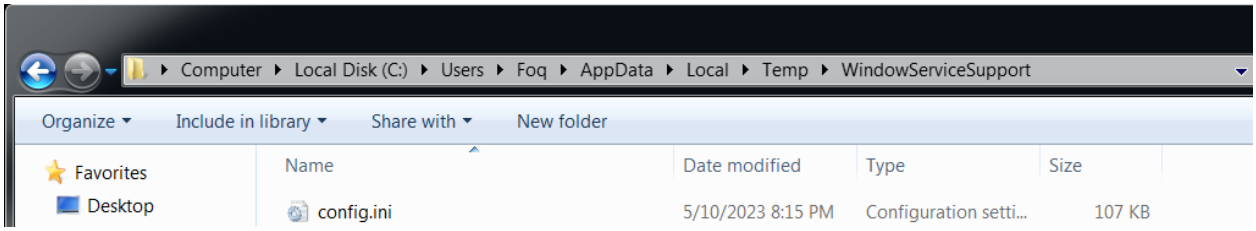


Kết quả thực thi mã độc từ góc nhìn của victim

Trong đó, file *Instruction.png* được ngụy trang là file ảnh chứa hướng dẫn sử dụng phần mềm sinh khóa.

2.2 Phân tích quá trình lây nhiễm và luồng thực thi của mã độc

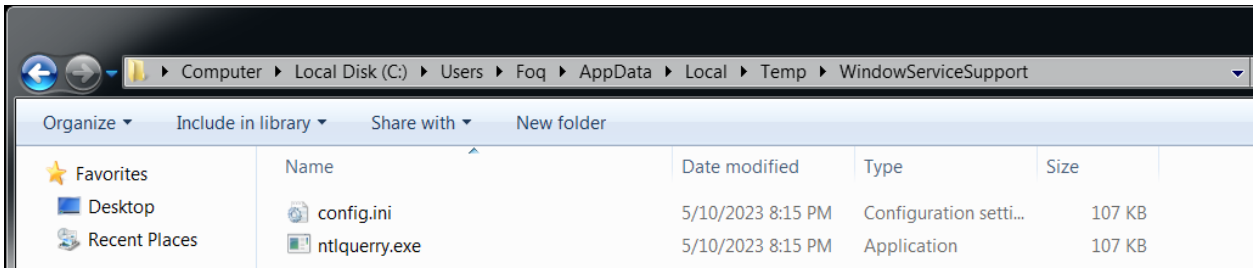
Khi được thực thi, *Keygen.exe* kết nối đến máy chủ và tải xuống file *config.ini* tại *%TEMP%/WindowServiceSupport*.



*File dữ liệu **config.ini** được mã độc tải xuống vào máy victim*

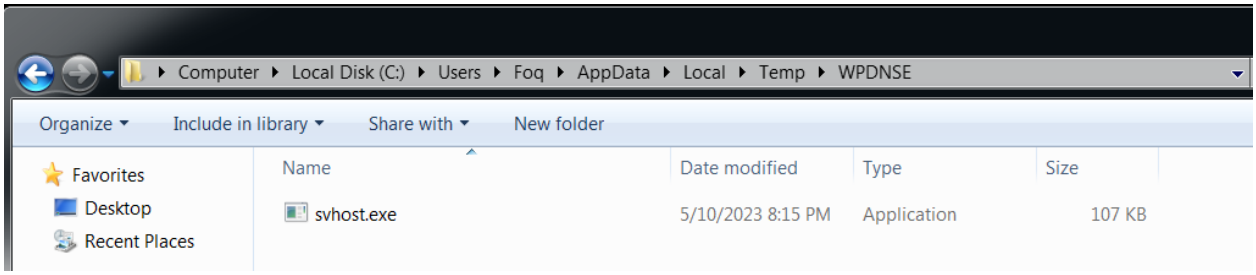
Với file *config.ini* thực chất là một backdoor đã được encode để bypass các firewall, AV,.. để có thể lây nhiễm vào máy victim.

Mã độc sau đó tiến hành decode file *config.ini* và tạo file backdoor dưới tên *ntlquerry.exe* tại cùng thư mục với file mã hóa.



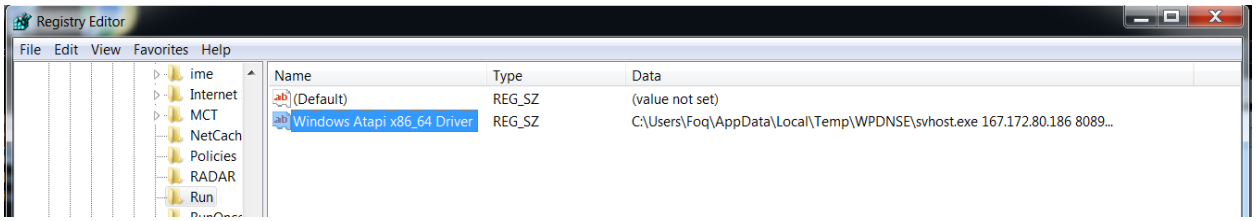
Mã độc lây nhiễm backdoor trên máy victim

Mã độc nhân bản backdoor *ntlquerry.exe* vào thư mục *%TEMP%\WPDNSE* dưới tên *svhost.exe*.



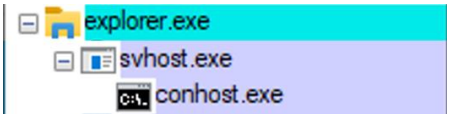
Bản sao của backdoor

Sau khi lây nhiễm thành công, mã độc tạo persistence cho backdoor bằng cách tạo ra entry mới trong registry ***HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run***:



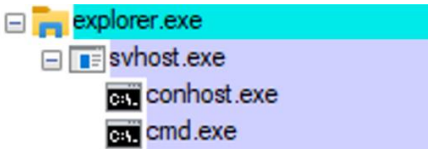
Mã độc tạo persistence bằng registry

Mã độc sau đó thực thi file backdoor để tạo kênh liên lạc đến server.

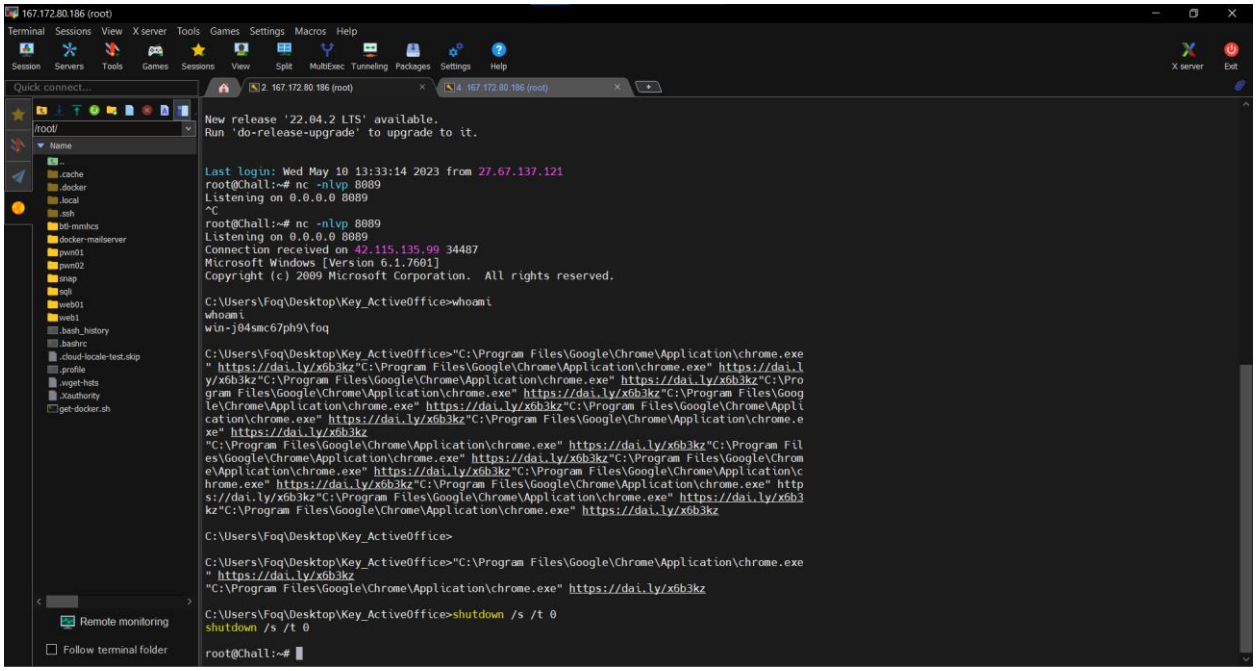


Trong đó *svhost.exe* là backdoor tạo ra process *conhost.exe* để connect đến máy chủ điều khiển.

Nếu server trong trạng thái LISTENING, backdoor nhận phản hồi từ server và tạo process *cmd.exe* để thực hiện lệnh nhận được từ server. Nếu server không phản hồi, mã độc tiếp tục gửi connect request đến server mỗi 4953ms.



Backdoor thành công kết nối đến máy chủ điều khiển



Server thực thi mã từ xa trên máy victim

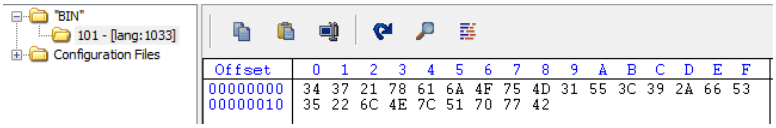
```
C:\Users\Foq\Desktop\Key_ActiveOffice>shutdown /s /t 0
shutdown /s /t 0

root@Chall:~# nc -nlvp 8089
Listening on 0.0.0.0 8089
Connection received on 42.115.135.99 64006
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Sau khi máy tính nhiễm mã độc được bật, mã độc sẽ tự động chạy và connect về server đã tạo trước đó.

3. CÁC KỸ THUẬT MÃ HÓA ĐƯỢC SỬ DỤNG

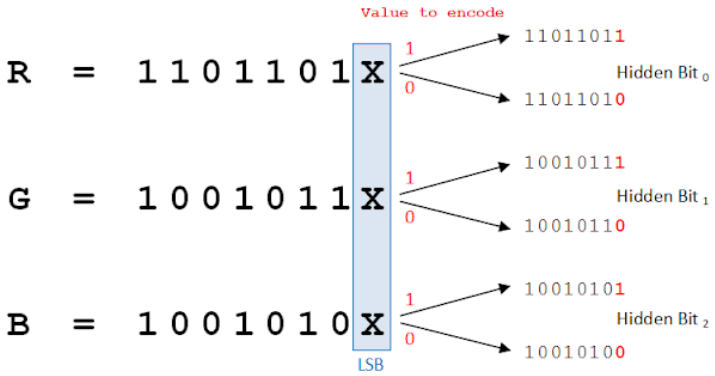
3.1 Base91

Base91 là phương pháp encode dữ liệu ở dạng ASCII sử dụng bảng chữ cái gồm 91 ký tự có thể hiển thị (printable characters). Được sử dụng để mã hóa địa chỉ máy chủ điều khiển và lưu trong resource của file *Keygen.exe*



3.2 Mật mã LSB (Least Significant Bit cipher)

Least Significant Bit (bit ít quan trọng nhất - LSB) là vị trí bit trong một số nguyên nhị phân đại diện cho 1 bit nhị phân của số nguyên. LSB đôi khi được gọi là bit ngoài cùng bên phải vì thường dữ liệu được quy ước viết các bit ít quan trọng hơn ở bên phải.

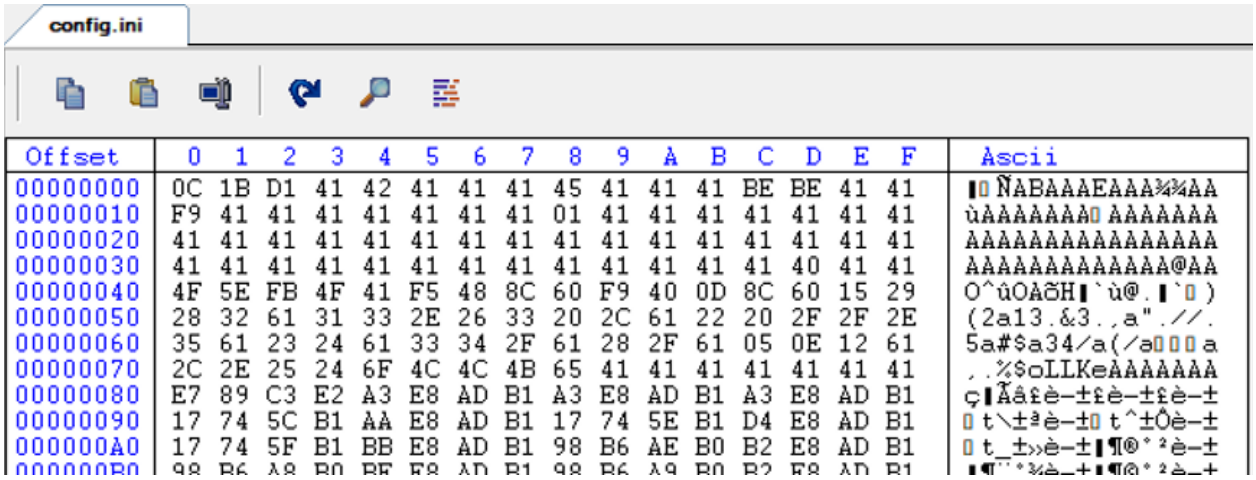


Mã hóa LSB là mã hóa với ý tưởng giấu data trong các LSB của một file ảnh vì sự thay đổi giá trị của LSB chỉ dẫn đến sự thay đổi rất ít trên file ảnh nếu nhìn bằng mắt thường.

Mã hóa LSB được sử dụng để giấu URL của backdoor trong file *Instruction.png*.

3.3 Mã hóa XOR (XOR cipher)

Mã hóa dữ liệu sử dụng phép XOR với một key cụ thể. Trong phạm vi mẫu mã độc này, XOR được sử dụng để mã hóa file backdoor và đảm bảo backdoor không bị phát hiện là file độc hại trong quá trình lây nhiễm đến máy victim.



File backdoor sau khi mã hóa XOR

4. TỔNG KẾT

Phần 1 trình bày về mô hình mã độc được sử dụng, cách xây dựng và một số kỹ thuật bypass các AV, firewall,… từ đó giới thiệu một số kỹ thuật ngụy trang phổ biến của mã độc.

CHƯƠNG III. CÀI ĐẶT VÀ THỰC NGHIỆM MÃ ĐỘC

1. CÀI ĐẶT MÃ ĐỘC

Để tạo máy chủ điều khiển, ta cần thực hiện các tác vụ sau:

- Cấu hình máy chủ cho phép tải file backdoor để mã độc thực hiện chức năng tự cập nhật trên máy victim
- Cấu hình máy chủ điều khiển đợi kết nối từ các máy nạn nhân để thực hiện điều khiển máy nạn nhân

Mẫu mã độc được phát triển trong bài viết này có các tính năng chính như sau:

- Là sự kết hợp của nhiều loại mã độc khác nhau (Backdoor, downloader, trojan)
- Tất cả thông tin gửi và nhận đều được mã hóa trên đường truyền
- Mã độc được thực thi dưới hình thức multi-stage, sử dụng một số kỹ thuật đặc biệt để vượt qua và gây rối các hệ thống phát hiện mã độc và phân tích mã độc.
- Mã độc tạo persistence để tự động kết nối mỗi khi hệ điều hành khởi động.
- Sau khi được cài đặt, mã độc kết nối đến máy chủ và đợi lệnh điều khiển từ máy chủ.

Mọi tác vụ cài đặt cấu hình nhắc đến trên đều được thực hiện thông qua script file *automate.py*.

2. THỰC NGHIỆM MÃ ĐỘC

2.1. Mục tiêu tấn công

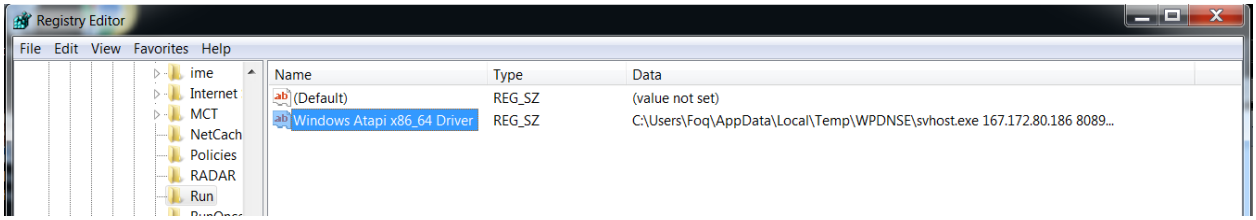
Mục tiêu được chọn để tấn công là máy tính sử dụng hệ điều hành Windows 10 đã đáp ứng đầy đủ các yếu tố về môi trường và công cụ.

2.2. Kịch bản lây nhiễm

Mã độc ngụy trang phần mềm sinh khóa để lây nhiễm vào máy người dùng. Nạn nhân tải về phần mềm và thực thi trên máy. Mã độc được thực thi.

2.3. Kết quả

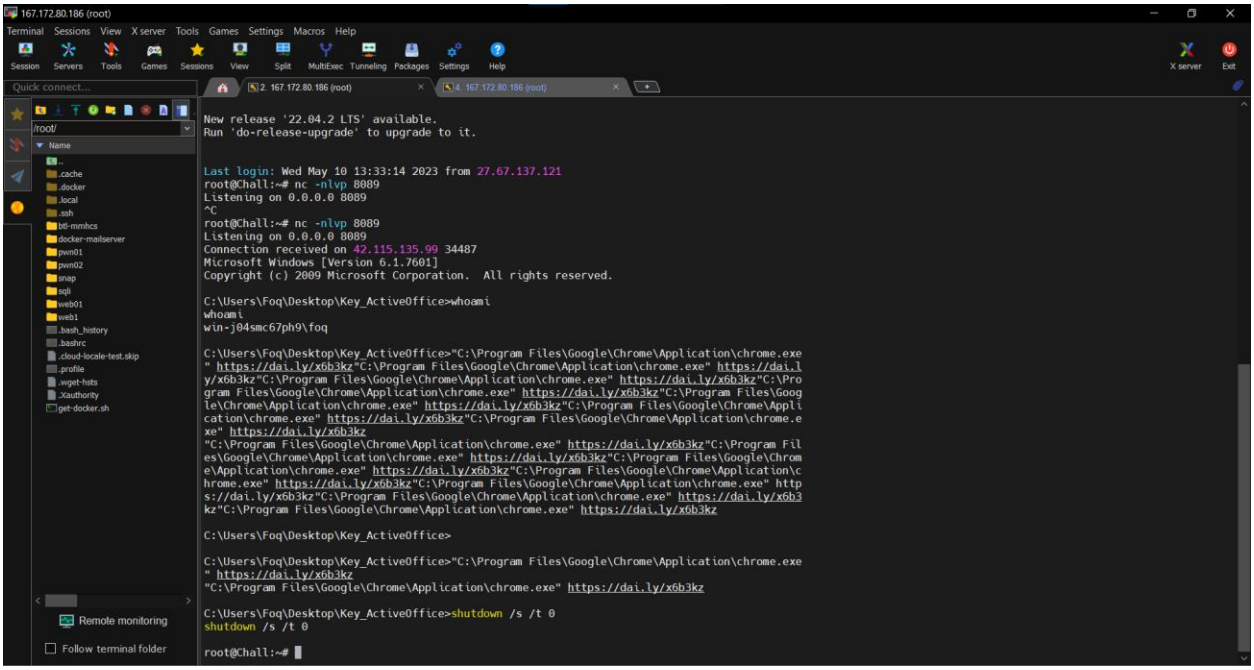
Mã độc thành công tạo Persistence để đảm bảo mã độc luôn được thực thi mỗi khi hệ điều hành khởi động.



Mã độc lây nhiễm vào máy victim và giao tiếp với máy chủ điều khiển. Trong phạm vi thử nghiệm, kết nối giữa máy chủ điều khiển và máy nạn nhân là ổn định, máy nạn nhân đảm bảo nhận lệnh từ máy chủ và phản hồi kết quả về máy chủ.

Sau khi kết nối, một backdoor được tạo để nhận lệnh và máy chủ có thể tự do tương tác với máy nạn nhân qua cmd.exe.

Cửa sổ tiến trình cmd.exe hoàn toàn bị ẩn khỏi màn hình của máy nạn nhân.



3. KẾT CHƯƠNG

Như vậy, chương III đã giới thiệu về kịch bản lây nhiễm và cách cài đặt của mã độc, ngoài ra trình bày sơ bộ về quá trình giao tiếp giữa máy chủ và máy victim.