

BỘ THÔNG TIN VÀ TRUYỀN THÔNG  
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

\*\*\*



**NGUYỄN MINH VƯƠNG**

Đề tài: NGHIÊN CỨU, XÂY DỰNG VÀ THỬ NGHIỆM  
GIẢI PHÁP PHÁT HIỆN MÃ ĐỘC RANSOMWARE

Chuyên ngành: KHOA HỌC MÁY TÍNH  
Mã số: 60.48.01.01

**LUẬN VĂN THẠC SĨ KỸ THUẬT**

NGƯỜI HƯỚNG DẪN KHOA HỌC  
**PGS.TSKH. HOÀNG ĐĂNG HẢI**

**Hà Nội, tháng 6 năm 2017**

NGƯỜI HƯỚNG DẪN KHOA HỌC  
**PGS.TSKH. HOÀNG ĐĂNG HẢI**

## **LỜI CAM ĐOAN**

Tôi xin cam đoan: Luận văn tốt nghiệp với đề tài “Nghiên cứu, xây dựng và thử nghiệm giải pháp phát hiện mã độc Ransomware” là công trình nghiên cứu của cá nhân tôi, không sao chép của bất cứ ai.

Tôi xin chịu mọi trách nhiệm về công trình nghiên cứu của riêng mình!

Hà Nội, ngày 15 tháng 06 năm 2017

Người cam đoan

Nguyễn Minh Vương

## LỜI CẢM ƠN

Với lòng biết ơn sâu sắc của mình, em xin gửi lời cảm ơn đến PGS.TSKH Hoàng Đăng Hải đã tận tình hướng dẫn, giúp đỡ em trong quá trình học tập, nghiên cứu và hoàn thành khóa luận.

Em xin cảm ơn các thầy cô trong Khoa Quốc Tế & Đào Tạo Sau Đại Học – Học viện Công nghệ Bưu chính Viễn thông đã giúp đỡ em trong suốt quá trình học tập và nghiên cứu.

Trong suốt quá trình học tập và thực hiện đề tài tôi luôn nhận được sự động viên, giúp đỡ của bạn bè, đồng nghiệp và người thân trong gia đình. Tôi xin chân thành cảm ơn!

Hà Nội, tháng 6 - 2017

Tác giả khóa luận

Nguyễn Minh Vương

# MỤC LỤC

LỜI CAM ĐOAN .....	ii
LỜI CẢM ƠN .....	iii
MỤC LỤC.....	iv
DANH MỤC HÌNH .....	vi
DANH MỤC BẢNG BIÊU .....	vii
MỞ ĐẦU.....	1
1.    Tính cấp thiết của đề tài .....	1
2.    Mục tiêu của luận văn .....	2
3.    Nội dung thực hiện .....	2
4.    Đối tượng, phạm vi, phương pháp nghiên cứu .....	3
Chương 1: KHÁI QUÁT MÃ ĐỘC RANSOMWARE VÀ .....	4
CÁC PHƯƠNG PHÁP PHÂN TÍCH MÃ ĐỘC .....	4
1.1.    Tổng quan về mã độc Ransomware .....	4
1.1.1.    Khái niệm.....	4
1.1.2.    Lịch sử phát triển, các biến thể .....	4
1.1.3.    Mức độ nguy hiểm, nguy cơ, hậu quả .....	7
1.1.4.    Hiện trạng tại Việt Nam và Thế giới .....	8
1.1.5.    Nhu cầu phân tích phát hiện mã độc Ransomware .....	12
1.2.    Biện pháp phòng chống Ransomware .....	13
1.2.1.    Giải pháp lưu trữ (backup).....	14
1.2.2.    Giải pháp sử dụng lưu trữ đám mây .....	14
1.2.3.    Hướng nhận biết dẫn khắc phục hậu quả mã độc Ransomware .....	15
1.3.    Kết luận chương .....	19
Chương 2: PHƯƠNG PHÁP PHÂN TÍCH, PHÁT HIỆN MÃ ĐỘC RANSOMWARE ..	20
2.1.    Một số phương pháp phát hiện nhanh trong thực tiễn .....	20
2.1.1.    Thông qua danh sách đen (blacklist) .....	20
2.1.2.    Hashing, dấu vân tay của malware .....	20
2.1.3.    Kỹ thuật Fuzzy hashing .....	20
2.1.4.    Kỹ thuật Scan String .....	21
2.1.5.    Kỹ thuật Code Emulation .....	21
2.2.    Môi trường hỗ trợ phân tích, phát hiện mã độc.....	21
2.2.1.    Cơ sở lý thuyết.....	21
2.2.2.    Sử dụng môi trường ảo hóa.....	22

2.2.3. Công cụ trợ giúp .....	24
2.3. Phân tích đánh giá các phương pháp.....	29
2.3.1. Phương pháp phân tích tĩnh .....	30
2.3.2. Phương pháp phân tích động .....	42
2.4. Phân tích lựa chọn công cụ, phương pháp xây dựng giải pháp phân tích hành vi mã độc Ransomware .....	50
2.5. Kết luận chương .....	54
<b>Chương 3: XÂY DỰNG VÀ THỬ NGHIỆM GIẢI PHÁP PHÁT HIỆN RANSOMWARE .....</b>	<b>55</b>
3.1. Kiến trúc và các thành phần của giải pháp.....	55
3.1.1. Ý tưởng đề xuất .....	55
3.1.2. Kiến trúc và các thành phần chương trình.....	55
3.1.3. Các Module chương trình .....	57
3.2. Thử nghiệm giải pháp .....	61
3.2.1. Kịch bản thử nghiệm 1 .....	61
3.2.2. Kịch bản thử nghiệm 2.....	63
3.2.3. Đánh giá thử nghiệm và kết luận .....	65
<b>KẾT LUẬN .....</b>	<b>67</b>
1. Đạt được.....	67
2. Hạn chế .....	68
3. Hướng phát triển .....	68

## DANH MỤC HÌNH

Hình 1.1: Thông báo đòi tiền chuộc của TeslaCrypt.....	6
Hình 1.2 Sơ đồ tổng quan về mã độc Ransomware đến hết 2016.....	7
Hình 1.3: Thống kê số lượng người dùng bị tấn công phân loại theo nhóm mã độc tổng tiền mã hóa năm 2014-2015 .....	10
Hình 1.4: Thống kê số lượng người dùng bị tấn công phân loại theo nhóm mã độc tổng tiền mã hóa năm 2015-2016 .....	10
Hình 2.1: thuật toán Fuzzy Hashing.....	21
Hình 2.2: Process Explorer .....	25
Hình 2.3: Process Moniter .....	26
Hình 2.4: Process Moniter .....	27
Hình 2.5: Systracer.....	28
Hình 2.6: Tạo Snapshot sau khi chạy mã độc .....	28
Hình 2.7: Tổng quan về TeslaCrypt.....	33
Hình 2.8: Giả mạo chứng chỉ .....	34
Hình 2.9: Làm rối code (String Obfuscation) .....	35
Hình 2.10: Chống giám sát (anti-monitoring).....	36
Hình 2.11: các tập tin được mã hóa bằng thuật toán AES256 CBC) .....	37
Hình 2.12: Tạo thông tin về nạn nhân.....	38
Hình 2.13: Hành vi gửi dữ liệu về server .....	38
Hình 2.14: Dữ liệu POST .....	39
Hình 2.15: Phân tích mã độc bằng công cụ Process Moniter.....	44
Hình 2.16: Kiểm chứng bằng Process Hacker .....	44
Hình 2.17: Thông báo đòi tiền chuộc.....	45
Hình 2.18: Sử dụng công cụ Process Moniter.....	46
Hình 2.19: Sử dụng bộ lọc trong công cụ Process Moniter .....	46
Hình 2.20: Tạo bản Snapshot trạng thái hệ thống trước khi chạy .....	47
Hình 2.21: SysTracer Sau khi chạy mã độc .....	48
Hình 2.22: So sánh 2 trạng thái trước và sau để thấy sự thay đổi giá trị hệ thống.....	48
Hình 2.23: Công cụ Moniter các API.....	49
Hình 2.24: Mô hình hành vi .....	52
Hình 3.1: Kiến trúc chương trình .....	56
Hình 3.2: Xử lý dữ liệu .....	57
Hình 3.3: Module phát hiện mã độc.....	58
Hình 3.4: Chạy mã độc TeslaCrypt.....	62
Hình 3.5: Dữ liệu bị mã hóa và thông báo đòi tiền chuộc.....	62
Hình 3.6: Chương trình phát hiện mã độc.....	63
Hình 3.7: Liệt kê các hành vi nguy hiểm .....	63
Hình 3.8: Thủ nghiệm quét tệp tin trên virustotal.....	64
Hình 3.9: Kết quả chạy trên chương trình thử nghiệm.....	65
Hình 3.10: Hành vi của phần mềm thực thi .....	65

## **DANH MỤC BẢNG BIỂU**

Table 1: Danh sách các quốc gia bị tấn công Ransomware nhiều nhất trong năm 2014-2015 .....	11
Table 2: Danh sách các quốc gia bị tấn công Ransomware nhiều nhất trong năm 2015-2016 .....	11
Table 3: Tiêu chí đánh giá phần mềm độc hại .....	59
Table 4: Các ngưỡng xếp loại Payload .....	59
Table 5: Phân loại mức độ nguy hiểm theo điểm .....	60
Table 6: Tính mức ưu tiên (Priority) khi đánh giá các hành vi .....	60

## MỞ ĐẦU

### 1. Tính cấp thiết của đề tài

Trong năm 2015 và 2016 mã độc mã hóa dữ liệu (được gọi là Ransomware) quay trở lại với nhiều biến thể mới và nguy hiểm. Mã độc loại này được trang bị những thuật toán mã hóa mạnh mẽ, nhiều phương thức lây lan, nhiều biến thể khác nhau, dễ dàng tạo và sử dụng, thanh toán ẩn danh. Do vậy, tính chất nguy hiểm của Ransomware cao hơn rất nhiều cho với các trojan và virus thông thường... Một khi bị nhiễm loại mã độc này, tất cả dữ liệu gốc của nạn nhân sẽ bị mã hóa, các bản dữ liệu gốc sẽ bị xóa hoàn toàn và khả năng khôi phục dữ liệu gần như không có. Nạn nhân muốn lấy lại dữ liệu cần phải trả tiền cho kẻ tấn công để lấy key giải mã mà chúng nắm giữ. Lợi nhuận lớn từ việc phát triển mã độc để kiếm lời đã thúc đẩy sự nguy hiểm, tinh vi của mã độc lên những tầm cao mới, đặt ra nhiều thách thức đối với các biện pháp phòng vệ an ninh.

Phát hiện và xử lý ngăn chặn mã độc là một trong những biện pháp phòng vệ an ninh điển hình, trong đó chuyên gia kỹ thuật cần **phân tích, phát hiện mã độc** để có giải pháp **phòng chống, bảo vệ an ninh** cho thông tin và hệ thống thông tin, ngăn chặn và tránh bị mã độc xâm nhập.

Với sự tinh vi và đa dạng của Ransomware cách tiếp cận của những phần mềm diệt virus truyền thống dựa trên chữ ký đã không còn theo kịp sự phát triển của mã độc. Bên cạnh đó việc phân tích tinh đòi hỏi trình độ chuyên môn rất sâu, chi phí về thời gian, không kịp thời đáp ứng nhu cầu xử lý ngăn chặn, nhân lực vốn kén. Việc triển khai những hệ thống phòng vệ dạng như IDS/IPS hoặc các giải pháp cứng hóa của các hãng bảo mật với chi phí rất cao, và cần kinh nghiệm. Không những thế việc sử dụng những sản phẩm của các nước khác khiến chúng ta luôn rơi vào tình trạng bị động và phụ thuộc.

Với những yêu cầu thực tiễn như vậy, luận văn đặt vấn đề “**Nghiên cứu xây dựng và thử nghiệm giải pháp phát hiện mã độc Ransomware**” nhằm đưa ra

một giải pháp hiệu quả, thay thế một phần kiến thức chuyên gia, dễ sử dụng, có khả năng làm chủ công nghệ trong việc phát hiện mã độc Ransomware, từ đó đưa ra biện pháp xử lý, ngăn chặn mối đe dọa này.

## 2. Mục tiêu của luận văn

Mục tiêu của luận văn là Nghiên cứu phương pháp phân tích, phát hiện mã độc Ransomware và xây dựng một giải pháp thử nghiệm phát hiện mã độc Ransomware áp dụng được trong thực tiễn công việc tại Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT

## 3. Nội dung thực hiện

Luận văn sẽ thực hiện nghiên cứu theo các nội dung sau:

- Nghiên cứu khái quát về mã độc Ransomware, nguyên tắc nhận biết và phòng chống.
- Nghiên cứu một số phương pháp phát hiện nhanh trong thực tiễn, các kỹ thuật vượt qua phần mềm antivirus.
- Nghiên cứu thiết lập môi trường phân tích mã độc.
- Phân tích, đánh giá phương pháp phân tích mã độc tĩnh và động. Phân tích lựa chọn công cụ, phương pháp.
- Thu thập mẫu mã độc, nghiên cứu các hành vi, hoạt động của một số loại mã độc.
- Xây dựng một giải pháp phát hiện mã độc Ransomware dựa trên hành vi và phân tích heuristic.
- Thủ nghiệm giải pháp.
- Trong quá trình nghiên cứu, học viên đã viết và gửi bài báo khoa học có tiêu đề “Phương pháp kết hợp cho phân tích mã độc Ransomware” đến tạp chí an toàn thông tin ngày 21-5-2017.

## **4. Đối tượng, phạm vi, phương pháp nghiên cứu**

### **Đối tượng nghiên cứu**

- Hành vi phổ biến của một số họ mã độc Ransomware.
- Phương pháp phân tích phát hiện mã độc Ransomware.

### **Phạm vi nghiên cứu**

- Cơ sở lý thuyết cho phân tích, phát hiện mã độc Ransomware
- Thu thập mẫu, nghiên cứu hành vi, hoạt động của một số loại mã độc Ransomware.
- Giải pháp phát hiện mã độc Ransomware.

### **Phương pháp nghiên cứu**

- Nghiên cứu lý thuyết, khảo sát thực tiễn.
- Phương pháp phân tích mã độc, tính toán thống kê.
- Phương pháp phân tích thiết kế hệ thống.
- Thực nghiệm.

# Chương 1: KHÁI QUÁT MÃ ĐỘC RANSOMWARE VÀ CÁC PHƯƠNG PHÁP PHÂN TÍCH MÃ ĐỘC

## 1.1. Tổng quan về mã độc Ransomware

### 1.1.1. Khái niệm

Ransomware là một loại malware (phần mềm máy tính độc hại) ngăn chặn hoặc giới hạn người dùng sử dụng thiết bị, hệ thống hoặc dữ liệu của mình. Một số loại mã hóa tệp tin khiến nạn nhân không thể mở được tài liệu quan trọng, một số khác dùng cơ chế khóa máy để không cho nạn nhân tiếp tục sử dụng. Để có thể tiếp tục sử dụng hệ thống hoặc đọc dữ liệu cá nhân nạn nhân cần phải trả một khoản tiền cho kẻ tấn công để nhận key giải mã dữ liệu đã bị mã hóa.

### 1.1.2. Lịch sử phát triển, các biến thể

Mã độc tống tiền Ransomware có lịch sử hơn 20 năm hình thành và phát triển. Ransomware có hai biến thể chính là: “blocker” khóa người dùng truy cập dữ liệu và “encryptor” mã hóa dữ liệu người dùng [1]. Cả hai đều yêu cầu nạn nhân tiền chuộc để lấy lại dữ liệu người dùng ban đầu hoặc tiếp tục sử dụng máy. Ransomware được phát hiện lần đầu tiên vào khoảng giữa năm 2005 - 2006 tại Nga [2]. Những bản báo cáo đầu tiên của hãng bảo mật TrendMicro là vào năm 2006, với biến thể TROJ\_CRYZIP.A – Một dạng Trojan sau khi xâm nhập vào máy tính của người dùng, sẽ lập tức mã hóa, nén các file hệ thống bằng mật khẩu, đồng thời tạo ra các file \*.txt với nội dung yêu cầu nạn nhân trả phí 300\$ để lấy lại dữ liệu cá nhân [3]. Phát triển theo thời gian, các Ransomware tấn công tiếp đến các file văn bản và hệ thống như \*.DOC, \*.XL, \*.DLL, \*.EXE...

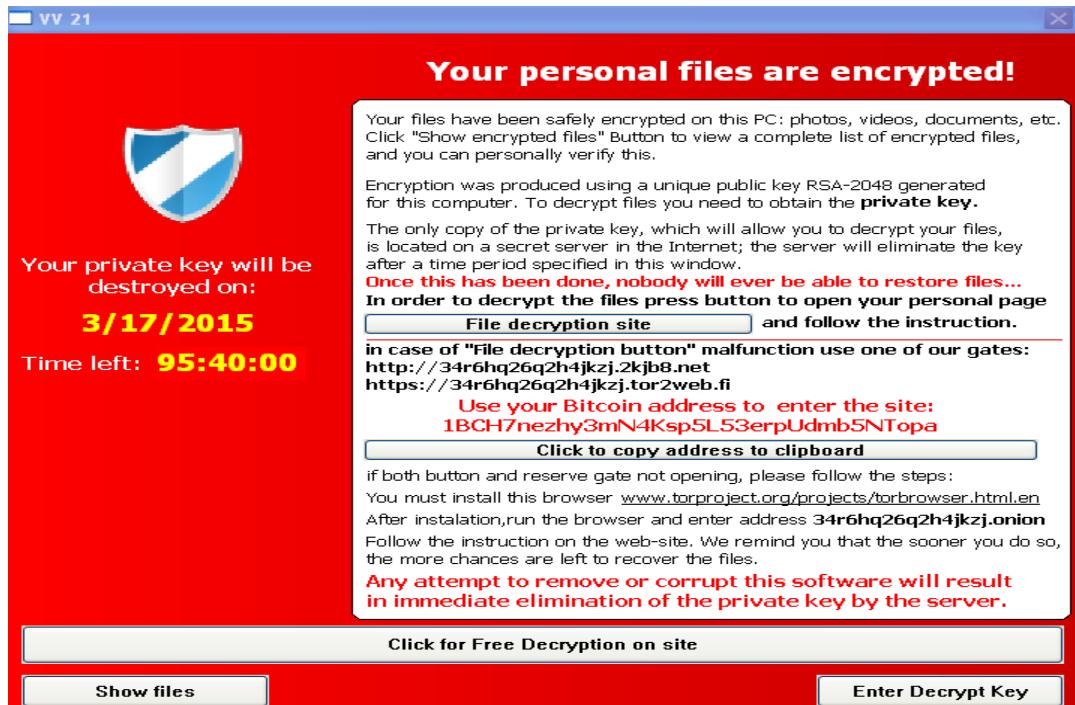
Năm 2011, một dạng khác của Ransomware là SMS Ransomware đã được phát hiện [4]. Cách thức của SMS Ransomware khác biệt hơn, đó là người dùng phải gửi tin nhắn hoặc gọi điện thoại đến số điện thoại của kẻ tấn công cho đến khi thực hiện xong thủ tục chuyển tiền cho kẻ tấn công. Biến thể này của Ransomware

được phát hiện dưới tên gọi TROJ\_RANSOM.QOWA sẽ liên tục hiển thị thông báo giả mạo trên màn hình máy tính. Bên cạnh đó, một biến thể khác của Ransomware nguy hiểm hơn nhiều, với mục tiêu của kẻ tấn công là tấn công vào Master Boot Record (MBR) của hệ điều hành nếu thành công hệ điều hành Windows sẽ không thể khởi động được. Các mã độc này sẽ sao chép phần MBR nguyên gốc của hệ thống và ghi đè bằng MBR giả mạo. Khi hoàn tất, quá trình này sẽ tự khởi động lại máy tính, và trong lần tiếp theo, các thông báo của kẻ tấn công sẽ hiển thị trên màn hình của nạn nhân.

Đến năm 2012, Ransomware Reventon sử dụng nhiều tài khoản, cách thức thanh toán khác nhau để nhận tiền của nạn nhân, thông thường là các hệ thống như UKash, PaySafeCard, hoặc MoneyPak [5]. Kẻ tấn công dùng những hình thức thanh toán này là vì hệ thống này thường làm ẩn đi thông tin người nhận tiền, do vậy kẻ tấn công sẽ yên tâm khi thực hiện giao dịch qua UKash, PaySafeCard, và MoneyPak.

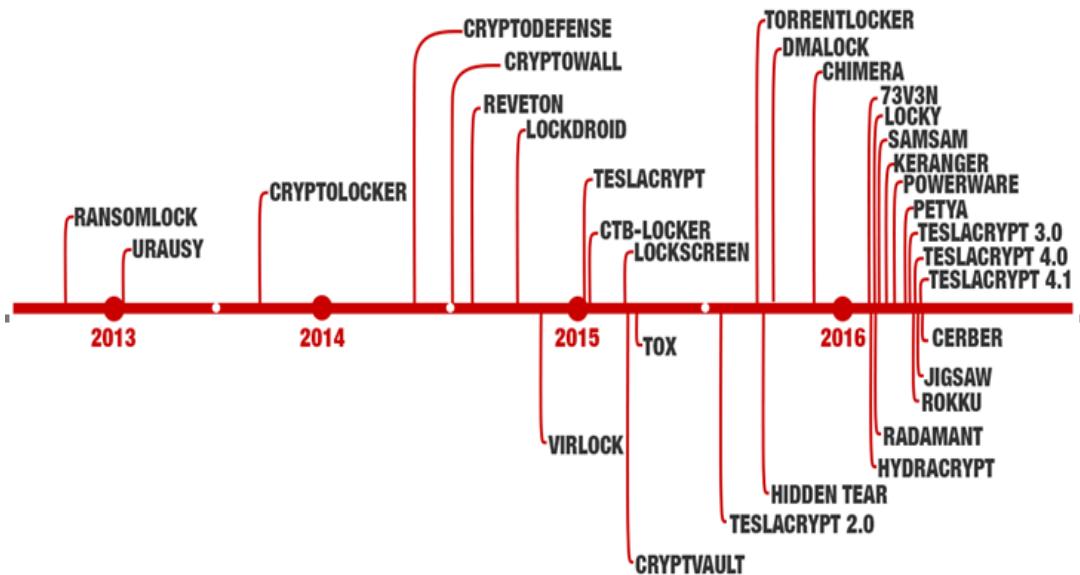
Năm 2014 một phiên bản mã độc mới có tên gọi là CryptoWall [6]. CryptoWall cho thấy sự tiến bộ trong phát triển phần mềm độc hại bởi vì nó có khả năng thay đổi và thiết lập thêm các khóa registry bổ sung và sao chép chính nó để khởi động các thư mục khác.

Tháng 3/2015, sự xuất hiện của mã độc Ransomware TeslaCrypt, biến thể này thường xuyên được sử dụng trong các cuộc tấn công lớn. Ransomware này thường nhắm đến người chơi game PC, một khi nhiễm loại mã độc này nó sẽ tiến hành khóa các tệp tin đến khi được trả tiền chuộc (thường là 500 USD và thanh toán dưới dạng Bitcoin). Nguồn lây nhiễm chủ yếu từ các website, quảng cáo độc hại và email lừa đảo. Cũng trong năm 2015 hàng loạt các mẫu malware mới thuộc họ Ransomware TeslaCrypt khác ra đời: LockerPin, LowLevel04 and Chimera.



**Hình 1.1: Thông báo đòi tiền chuộc của TeslaCrypt**

Trong năm 2016, có thể nói là một năm bùng nổ của mã độc Ransomware, rất nhiều cuộc tấn công lớn, sự kiện quan trọng liên quan đến Ransomware, các mẫu mới xuất hiện liên tục và tinh vi hơn rất nhiều. Trong số đó có thể kể đến những biến thể như: Ransom32 and 7ev3n, Locky, SamSam, KeRanger, Petya, Maktub, Jigsaw, CryptXXX, ZCryptor, TeslaCrypt...



**Hình 1.2 Sơ đồ tổng quan về mã độc Ransomware đến hết 2016**

### 1.1.3. Mức độ nguy hiểm, nguy cơ, hậu quả

Gửi email giả mạo hay có chứa tài liệu văn bản mà macro lập trình trong đó là hình thức phổ biến của nhiều loại Ransomware. Nội dung tài liệu có gắng lừa người dùng cho phép chạy macro. Và ngay sau khi người dùng kích hoạt macro, tất cả các tập tin thực thi yêu cầu của Locky được tải xuống và hệ thống được thỏa hiệp. Phiên bản mới nhất của Locky có thể ẩn mình trên hệ thống và có thể tự bảo vệ mình khi người dùng sử dụng các phương pháp truyền thống để kiểm tra hệ thống. Bên cạnh đó việc phát tán mã độc này được thực hiện một cách rất chuyên nghiệp, đã có cả một chiến dịch gửi thư spam nhằm lây lan mã độc được thuê từ bên thứ 3.

Cerber là có một gia đình trong họ Ransomware loại mã độc này khá mạnh và sở hữu nhiều kỹ thuật thông minh. Chúng sử dụng hai phương pháp lây nhiễm: Phương pháp đầu tiên cũng giống như Locky, Cerber cũng được gửi như một tệp tin đính kèm. Khi người dùng mở file này, nó sẽ tấn công máy tính và hệ thống người dùng. Phương pháp thứ hai là link để bỏ đăng ký từ danh sách lừa đảo, nhưng lại

“cung cấp” cho người dùng các tập tin đính kèm và cuối cùng là tấn công máy tính và hệ thống người dùng.

Tháng 5 năm 2017 mã độc mã hóa dữ liệu wannacry xuất hiện sau khi bộ công cụ khai thác lỗ hổng SMB của NSA bị lộ có tên ETERNALBLUE. Mã độc wannacry sử dụng một module có trong bộ khai thác gồm 7 công cụ bị rò rỉ. Chỉ sau hơn 2 ngày được phát hiện, WannaCry đã gây ảnh hưởng tới 10.000 tổ chức, 200.000 cá nhân trong khoảng 150 quốc gia trên thế giới, theo BBC. Đây cũng được coi là mã độc nguy hiểm nhất trên thế giới hiện nay. Nhiều bệnh viện, tổ chức y tế, từ thiện, tập đoàn ở các nước như Anh, Mỹ, Nga, Ấn Độ... bị mất dữ liệu gây ảnh hưởng nghiêm trọng không chỉ về kinh tế mà còn đến tính mạng, an ninh của người dân.

Đối với người dùng máy tính tại Việt Nam, với lượng người dùng sử dụng phần mềm crack và windows không có bản quyền và không được cập nhật thường xuyên thì tình trạng tồn tại các lỗ hổng bảo mật, bị cài backdoor là nguy cơ nghiêm trọng. Mã độc mã hóa ngày càng phát triển và nắm thế chủ động trong việc phát tán và lây nhiễm, đây là một thách thức rất lớn cho công tác đảm bảo an toàn an ninh thông tin.

#### **1.1.4. Hiện trạng tại Việt Nam và Thế giới**

Trong năm 2015 và 2016 mã độc Ransomware là vấn đề nghiêm trọng không chỉ ở Việt Nam mà cả trên phạm vi toàn thế giới. Với giá trị lớn từ đồng tiền ảo như bitcoin được phát triển đã mang đến một phương thức thanh toán an toàn cho tin tặc. Việt nam có thời điểm đã nằm trong mục tiêu của biến thể Ransomware có tên Locky. Ngoài việc phân chia theo địa lý quốc gia đối tượng tấn công của mã độc Ransomware còn theo các nhóm người sử dụng như:

##### **1.1.4.1. Nhóm người dùng thông thường**

Ransomware có lẽ hiệu quả nhất đối với cá nhân không thông thạo với máy tính hay không có nhận thức về Ransomware và cách thức nó hoạt động. Nhóm người dùng định là nạn nhân phổ biến của Ransomware do có ít kiến thức cơ

bản về bảo mật thông tin cũng như ít được tiếp cận với hỗ trợ kỹ thuật dẫn tới việc không có khả năng giải quyết cùng với việc gia tăng áp lực khi cần dùng dữ liệu sẽ dễ dàng trả tiền chuộc cho tội phạm.

#### 1.1.4.2. Khối doanh nghiệp

Thông tin và loại hình công nghệ sử dụng đã trở thành thứ quyết định sống còn của doanh nghiệp. Giả định rằng một doanh nghiệp có hàng tỷ lượt giao dịch trên hệ thống và bị Ransomware tấn công. Toàn bộ dữ liệu giao dịch, thông tin khách hàng trên hệ thống bị mã hóa dẫn tới ngưng trệ hoặc tạm dừng hoạt động sẽ khiến cho doanh nghiệp thiệt hại nghiêm trọng. Nhóm người dùng doanh nghiệp cũng có những dữ liệu quan trọng như tài liệu mật, tài sản trí tuệ, kế hoạch, số liệu tài chính...

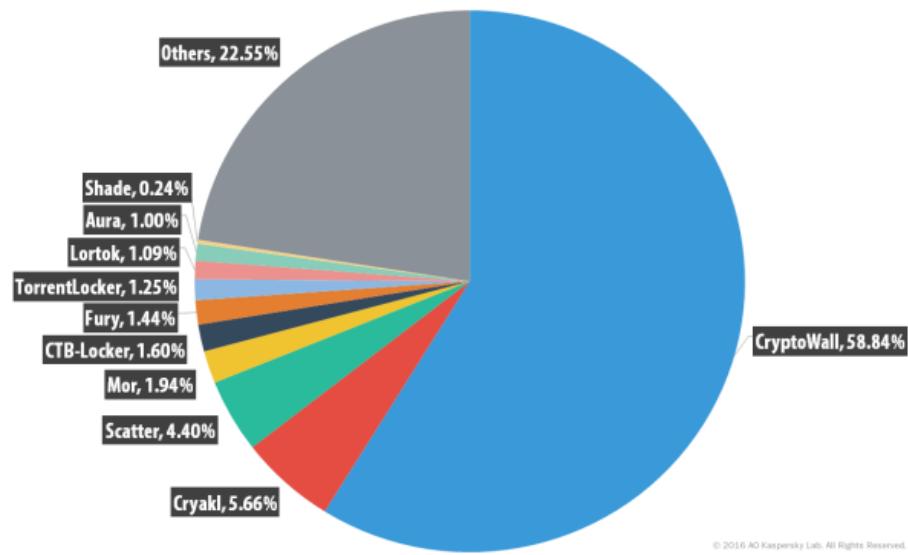
#### 1.1.4.3. Người dùng công cộng

Các cơ quan công cộng như tổ chức giáo dục, chăm sóc sức khỏe, tổ chức thực thi pháp luật cũng không ngoại trừ khả năng bị tấn công của Ransomware. Trong quá khứ đã có một vài trường hợp cơ quan thực thi pháp luật bị tấn công bởi Ransomware. Cũng như nhóm doanh nghiệp, khả năng trả tiền chuộc của đối tượng này cũng không cao như nhóm hộ gia đình do có các kế hoạch lưu trữ định kỳ và bộ phận CNTT để đảm bảo an toàn của hệ thống.

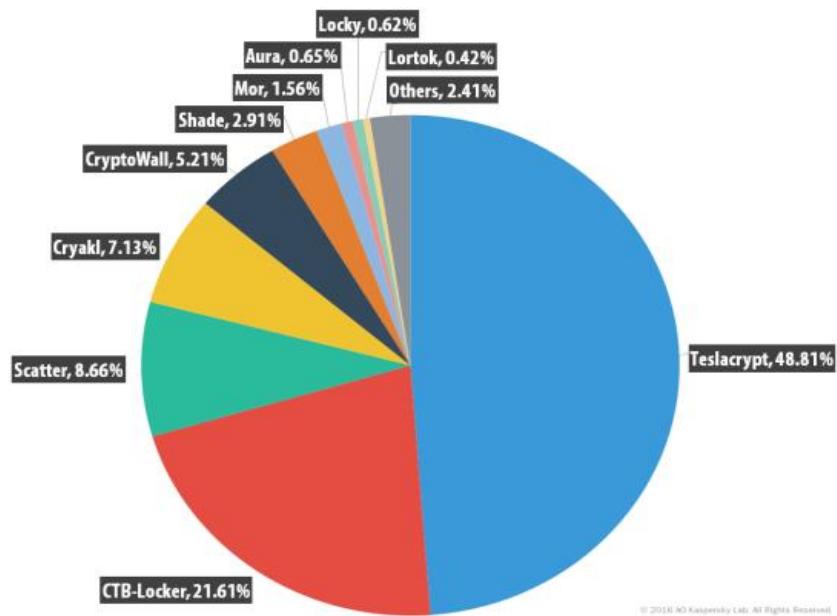
Theo số liệu thống kê của hãng bảo mật uy tín Kaspersky [20] tính đến quý III năm 2016, thay đổi lớn nhất khiến Ransomware trở nên báo động là sự phát triển của mã độc tống tiền dạng mã hóa. Số kiểu Ransomware đã tăng lên 17,7% trong vòng hai năm. Và số biến thể encryptor tăng lên 5.5 lần (từ 131,111 biến thể vào năm 2014-2015 lên tới 718,536 biến thể vào năm 2015-2016) .Cùng thời điểm đó, biến thể blocker giảm 13% từ 1,836,673 xuống còn 1,597,395 biến thể.

Tại thời điểm 2014-2015, mã độc CryptoWall chiếm khoảng 59% các vụ tấn công. Năm 2015-2016, TeslaCrypt đã thay thế vị trí dẫn đầu của CryptoWall với 49% các vụ tấn công.

Dưới đây là số liệu thống kê từ trang chủ của hãng Kaspersky [20].



**Hình 1.3: Thống kê số lượng người dùng bị tấn công phân loại theo nhóm mã độc tổng tiền mã hóa năm 2014-2015**



**Hình 1.4: Thống kê số lượng người dùng bị tấn công phân loại theo nhóm mã độc tổng tiền mã hóa năm 2015-2016**

### Phân bố địa lý mã độc Ransomware

Số lượng người dùng bị tấn công phân loại theo địa lý được thống kê bởi khách hàng sử dụng sản phẩm bảo mật của Kaspersky trên toàn cầu năm 2014-2015 như sau:

Table 1: Danh sách các quốc gia bị tấn công Ransomware nhiều nhất trong năm 2014-2015

Quốc gia	% người dùng bị tấn công Ransomware trong tổng số tất cả các mã độc
Kazakhstan	6.99%
Algeria	6.23%
Ukraine	5.87%
Italy	4.69%
Nga	4.63%
<b>Việt Nam</b>	<b>3.86%</b>
Ấn Độ	3.77%
Đức	3.00%
Brazil	2.60%
Hoa Kỳ	2.07%

#### 1.1.4.4. Theo kiểu người dùng bị tấn công Ransomware

Hầu hết mã độc tống tiền đều tấn công trực tiếp người dùng. Trong đó tin tặc có xu hướng chuyển nhanh từ người dùng hộ gia đình sang người dùng doanh nghiệp do cơ hội được thanh toán tiền chuộc lớn hơn.

Table 2: Danh sách các quốc gia bị tấn công Ransomware nhiều nhất trong năm 2015-2016

Quốc gia	2014-2015	2015-2016
Liên Bang Nga	562190	867651
Ấn Độ	143973	325638
Hoa Kỳ	107755	55679
Đức	102289	138750
Việt Nam	96092	89247
Ukraine	69220	39246
Kazakhstan	62719	39179
Algeria	61623	38530
Italy	49400	59130
Brazil	43674	70078

### ***1.1.5. Nhu cầu phân tích phát hiện mã độc Ransomware***

Nguồn gốc thành công của Ransomware nằm trong mô hình kinh doanh có lợi nhuận cao của nó. Khoảng 3% các công ty của Mỹ trả khoản tiền chuộc. Điều này có vẻ thấp nhưng vẫn làm cho Ransomware tống tiền một cách hiệu quả. Bên cạnh lợi cao, Ransomware là một con đường hấp dẫn cho kẻ tấn công mạng thực hiện và thu về lợi nhuận. Những kẻ tấn Ransomware có ít khả năng bị bắt vì sử dụng mạng thanh toán ẩn danh và đồng tiền ảo bitcoin, công việc phát triển Ransomware và thực hiện tống tiền là tương đối dễ dàng.

Trên phương diện kỹ thuật, các yếu tố dẫn đến thành công của Ransomware có thể được liệt kê như:

- Hệ thống thanh toán vô danh và liền mạch: Các loại tiền tệ cung cấp khả năng lưu động nhanh bất cứ nơi nào trên thế giới với các địa chỉ được ẩn danh. Điều này rất có lợi Cho kẻ tấn công Ransomware, có thể hoạt động trên quy mô toàn cầu trong khi vẫn có thể thu được tiền chuộc dễ dàng từ nạn nhân.
- Công sức phát triển thấp: Các gia đình Ransomware mới và các biến thể được phát hiện hàng ngày. Điều này một phần là vì Ransomware tương đối dễ phát triển. mặt khác với sự sẵn có của các thư viện mật mã tiêu chuẩn các chương trình mã hóa mã hóa sử dụng RSA và AES một cách dễ dàng. Hơn nữa, với xu hướng phát triển của Ransomware-as-a-Service (RaaS), ngay cả những kẻ tấn công không kỹ thuật cũng có thể nhanh chóng tạo ra Ransomware tùy biến. Với RaaS, các nhà phát triển Ransomware tạo ra một bộ dụng cụ phát triển Ransomware dễ sử dụng, mà khách hàng có thể mua và sử dụng để tạo ra Ransomware và địa chỉ để thanh toán tiền chuộc. Ngoài ra một số dự án Ransomware nguồn mở như EDA23 và Hidden Tear4 ban đầu được dự định cho các mục đích giáo dục nhưng được sử dụng như một khuôn mẫu để tạo ra hàng trăm biến thể Ransomware khác nhau.
- Chi phí phân phối hiệu quả: Kẻ tấn công Ransomware sử dụng phân phối độc hại có trả tiền dịch vụ để phân phối Ransomware một cách dễ dàng trên quy mô

toàn cầu. Những dịch vụ phân phối này sử dụng một loạt các nền tảng như spam, drive-by-downloads, malvertising và bộ dụng cụ khai thác...

- **Tống tiền:** Việc xác nhận thanh toán tiền chuộc và cấp chìa khóa giải mã (nếu có) thường tự động sử dụng email phản hồi tự động. Điều này trái ngược với mục tiêu các cuộc tấn công mà những kẻ tấn công phải lọc dữ liệu ra và hiểu giá trị của dữ liệu đã bị đánh cắp, hoặc hiểu được tổ chức cụ thể và tìm ra cách đánh cắp tiền.

Sự thành công liên tục của Ransomware tạo ra một mối đe dọa an ninh mạng nghiêm trọng. Theo thống kê của các hãng bảo mật uy tín, Việt Nam đang là một trong nhiều nạn nhân của các cuộc tấn công mã hóa dữ liệu đòi tiền chuộc. Mã độc này có rất nhiều hình thức lây lan nguy hiểm thông qua các chiến dịch phát tán các thư điện tử, thông qua việc khai thác các lỗ hổng bảo mật, thông qua các trình downloader và được sử dụng các kỹ thuật tinh vi nhằm tránh bị phát hiện bởi các phần mềm antivirus, chính vì vậy nhu cầu phân tích mã độc này là cao và thiết thực. Mặt khác số lượng nhân lực có trình độ chuyên môn sâu trong ngành còn hạn chế, trong khi kỹ thuật phát triển mã độc ngày càng tinh vi, công tác phân tích đòi hỏi trình độ chuyên gia và chuyên môn sâu. Bên cạnh đó sự phụ thuộc vào các sản phẩm nước ngoài khiến cho chúng ta luôn lệ thuộc vào các sản phẩm của nước ngoài. Chính vì vậy việc nghiên cứu các quy trình phân tích, thông tin phương thức hoạt động, và đặc biệt là giải pháp phát hiện mã độc sẽ giúp nhiều người dùng nâng cao nhận thức, phòng ngừa cũng như hiểu biết về mã độc để làm cơ sở phát triển các công cụ phát hiện và ngăn chặn mã độc trong tương lai.

## 1.2. Biện pháp phòng chống Ransomware

Để phòng chống mã độc Ransomware có thể sử dụng một số các giải pháp tạm thời như lưu trữ dữ liệu vật lý, sử dụng giải pháp lưu trữ đám mây, sử dụng phần mềm antivirus mạnh để phát hiện những loại đã biết. Tuy nhiên về mặt lâu dài và hiệu quả cao chúng ta cần phát triển những công cụ nhằm phát hiện sớm các

cuộc tấn công dạng này và đặc biệt là nâng cao nhận thức của người sử dụng máy tính.

### **1.2.1. Giải pháp lưu trữ (backup)**

Backup dữ liệu là một hoạt động quan trọng của người dùng, việc này cần được thực hiện thường xuyên, nếu máy tính hoặc máy chủ của người dùng bị tấn công và dữ liệu bị mã hóa, người dùng có thể khôi phục lại dữ liệu mà không phải trả tiền chuộc cho kẻ tấn công.

Back-up dữ liệu có nghĩa là người dùng sao chép các dữ liệu trong máy tính (hoặc tablet, smartphone...) của người dùng và lưu trữ nó ở một nơi khác, phòng khi máy tính của người dùng bị mã hóa dữ liệu hoặc gặp vấn đề như hỏng ổ cứng, bị nhiễm virus nặng, bị mất máy... Người dùng sẽ không lo bị mất dữ liệu trên máy nữa vì người dùng có thể backup dữ liệu của mình về từ nơi lưu trữ dự bị. Cách nhanh nhất để back-up dữ liệu là sử dụng các ổ đĩa rời, ổ cứng di động, USB hay thậm chí là đĩa DVD, VCD. Tùy theo yêu cầu cụ thể của bài toán đặt ra mà lựa chọn công nghệ và thiết bị cho phù hợp. Theo cơ chế lưu trữ, hiện nay có một số loại hình lưu trữ dữ liệu cơ bản như:

**DAS (Direct Attached Storage):** Lưu trữ dữ liệu qua các thiết bị gắn trực tiếp.

**NAS (Network Attached Storage):** Lưu trữ dữ liệu vào thiết bị lưu trữ thông qua mạng IP

**SAN (Storage Area Network):** Lưu trữ dữ liệu qua mạng lưu trữ chuyên dụng riêng. Mỗi loại hình lưu trữ dữ liệu có những ưu nhược điểm riêng và được dùng cho những mục đích nhất định.

### **1.2.2. Giải pháp sử dụng lưu trữ đám mây**

Khi người dùng sử dụng các dịch vụ lưu trữ đám mây, người dùng có thể lưu trữ và tải dữ liệu về từ nguồn trực tuyến trên Internet. Giống như việc người dùng lưu giữ hình ảnh, video trên các trang mạng xã hội: Google Driver, One Driver,

Facebook, YouTube... Có rất nhiều giải pháp lưu trữ dữ liệu đám mây, đây là hình thức lưu trữ rất tiện dụng, nhanh chóng và có độ an toàn dữ liệu tương đối. Tuy nhiên về tính bí mật dữ liệu là điều cần phải xem xét, sử dụng giải pháp lưu trữ đám mây này vẫn có nguy cơ bị tin tặc hoặc người có quyền quản trị xem hoặc lấy cắp dữ liệu, chính vì vậy phương án này chỉ phù hợp cho người dùng cá nhân hoặc tổ chức nhưng những dữ liệu này không phải là những tài liệu bí mật. Nếu các cơ quan tổ chức sử dụng dịch vụ lưu trữ đám mây của một số hãng uy tín, có trả phí cũng cần lưu ý cân nhắc việc giữ tính bí mật của dữ liệu bằng cách mã hóa dữ liệu cá nhân quan trọng trước khi đưa lên đám mây để lưu trữ.

### **1.2.3. Hướng nhận biết dấu khắc phục hậu quả mã độc Ransomware**

#### **1.2.3.1. Hướng dẫn nhận biết**

Khi bị nhiễm Ransomware các tài liệu, văn bản sẽ bị thay đổi nội dung, đổi tên tệp tin và đổi tên phần mở rộng như .locky, virus cerber, kimcilware..., phổ biến là các tệp tin có định dạng: .doc, .docx, .pdf, .xls, .xlsx, .jpg, .txt, .ppt, .pptx,.. một số loại còn khóa máy tính không cho sử dụng và đòi tiền chuộc. Đối với mỗi hệ điều hành và mỗi loại Ransomware đều có những dấu hiệu nhận biết khác nhau, tuy nhiên dấu hiệu nhận biết chung bao gồm những triệu chứng sau đây:

- Máy tính bị treo, tự khởi động lại vào chế độ Safe Mode (phổ biến trên Windows).
- Máy tính tự động bị khoá, không thể sử dụng được chuột và bàn phím hoặc không thể khởi động được và yêu cầu phải có password để đăng nhập.
- Trên màn hình Desktop của nạn nhân liên tục mở các file có nội dung thông báo lạ hoặc trình duyệt web tự động truy cập vào các trang web không rõ nguồn yêu cầu nạn nhân nạp tiền vào một tài khoản nào đó.
- Ngoài ra để xác định chính xác loại Ransomware mà mình đã nhiễm người dùng có thể sử dụng tiện ích “ID Ransomware”. ID Ransomware là một tiện ích trực tuyến giúp người dùng kiểm tra và xác định xem đã bị Ransomware nào tấn

công và từ đó sẽ đưa ra giải pháp để người dùng cách khôi phục dữ liệu. Đầu tiên người dùng truy cập vào ID Ransomware tại địa chỉ: [https://idransomware.malwarehunterteam\[.\]com-/index.php](https://idransomware.malwarehunterteam[.]com-/index.php). Sau đó bạn tiến hành tải lên một tập tin mẫu có thể là tập tin chứa thông tin về tiền chuộc và thanh toán mà Ransomware yêu cầu hoặc một tập tin đã bị Ransomware mã hóa. Sau khi tải lên người dùng chờ trong giây lát để trang web phân tích dữ liệu và sẽ hiển thị thông tin của loại Ransomware đồng thời sẽ đưa ra hướng giải quyết.

#### 1.2.3.2. Khắc phục và hạn chế rủi do

Khi gặp sự cố về Ransomware người quản trị viên cần:

- Nhanh chóng xác định phạm vi bị nhiễm Ransomware, cài đặt máy bị nhiễm và phạm vi bị nhiễm thông thường là File Server, các thư mục dùng chung, máy tính nhân viên...
- Thông báo cho toàn thể tổ chức về tình hình sơ lược của Ransomware và dấu hiệu nhận dạng sơ lược của Ransomware từ máy bị nhiễm. Các bước và biện pháp phòng tránh nhiễm, lây nhiễm cơ bản.
- Cách ly hoạt động của phòng người dùng, đối tượng bị nhiễm như tắt chia sẻ file trên máy chủ (Stop Sharing), cách ly máy chủ, phòng người dùng bị nhiễm mã độc (Cách ly vật lý hoàn toàn máy tính bị nhiễm) ...
- Xem lại các file backup dữ liệu trước đó và xác định lượng dữ liệu có thể phục hồi, dữ liệu bị mất cho phòng người dùng liên quan để chuẩn bị cho công tác khôi phục lại dữ liệu.
- Lấy mẫu và gửi mẫu phân tích lên cho hãng cung cấp dịch vụ Antivirus/Endpoint của tổ chức. Nếu là mẫu cũ thì kiểm tra có các công cụ giải mã có sẵn (tham khảo trang <https://www.nomoreransom.org/>).
- Xác định nguyên nhân lây nhiễm. Do tải, cài đặt phần mềm, do email phishing có mã độc, do truy cập trang web, do USB..., để có thông tin bổ sung thông báo người dùng khác cách phòng tránh. Tăng cường chính sách ngăn chặn hạn chế các trường hợp xảy ra sau.

- Giữ lại Ổ cứng (Chứa dữ liệu) của máy tính lấy nhiễm để kiểm tra khả năng phục hồi dữ liệu (nếu có thể hoặc khi có key giải mã).
- Tiến hành các phương pháp ngăn chặn dấu hiệu cơ bản theo dấu hiệu của Ransomware.
  - Chặn trên các hash MD5, tên file, đường dẫn và sử dụng Endpoint để chặn các dạng file này.
  - Kiểm tra dấu hiệu nghi ngờ trên các email gửi vào hệ thống (nếu có) là dấu hiệu chung, cập nhật tạm thời cho Mail Gateway (nếu có) hoặc trên Mail Server để cách ly.
  - Rà soát lại log của Web Gateway, Proxy trong thời điểm bị mã hóa và ngăn chặn kết nối đến C&C bên ngoài.
  - Tổng hợp kết quả, gửi lại toàn bộ người dùng cảnh báo, dấu hiệu nhận biết, biện pháp phòng tránh, biện pháp thực hiện khi phát hiện.
  - Thông báo về tình trạng dữ liệu có thể khôi phục lại (backup hoặc tool giải mã), thời gian dự kiến cho việc thực hiện này.
  - Email cho người đứng đầu của bộ phận (Data Owner) để xác nhận cho việc thực hiện công tác phục hồi được thực hiện.
  - Thực hiện công tác rà soát lần cuối cùng khả năng Ransomware còn tồn tại trên Server sau đó thực hiện phục hồi.
  - Thông báo việc phục hồi hoàn tất và để người đứng đầu bộ phận xác nhận lại tình trạng của dữ liệu.
  - Thông báo cho bộ phận bị nhiễm về việc dữ liệu được khôi phục lại và có thể làm việc (vẫn truy cập trong tình trạng cách ly cho đến khi hệ thống an toàn).
  - Nhận lại kết quả của việc quét trên hệ thống và số lượng máy còn nhiễm, chưa quét, số lượng máy đã ẩn và quét lại lần nữa hoặc nhờ hỗ trợ thêm từ bộ phận hỗ trợ.
  - Chuẩn bị cho việc mở truy cập lại bình thường cho các bộ phận, phòng người dùng bị nhiễm khi xác định máy tính là sạch.

### 1.2.3.3. Khuyến nghị người dùng

Thường xuyên cập nhật bản vá, phiên bản mới nhất cho hệ điều hành và phần mềm chống mã độc (Kaspersky, Synmatec, Avast, AVG, MSE, CMC, v.v...). Khuyến khích các cơ quan, tổ chức sử dụng các phiên bản phần mềm phòng chống mã độc có chức năng đảm bảo an toàn khi truy cập mạng Internet và phát hiện mã độc trực tuyến.

Thường xuyên sử dụng phần mềm diệt mã độc, virus kiểm tra máy tính, ổ lưu trữ để phát hiện sớm nếu xuất hiện mã độc trên thiết bị.

Cần chú ý cảnh giác với các tệp tin đính kèm, các đường dẫn được gửi đến qua thư điện tử hoặc tin nhắn, hạn chế tối đa việc truy cập vào các đường dẫn này vì tin tặc có thể đánh cắp hoặc giả mạo hòm thư điện tử người gửi phát tán các kết nối chứa mã độc.

Sử dụng phần mềm diệt virus kiểm tra các tệp tin được gửi qua thư điện tử, tải từ trên mạng về trước khi kích hoạt. Nếu không cần thiết hoặc không rõ nguồn gốc thì không kích hoạt các tệp tin này.

Tắt chế độ tự động mở, chạy các tệp tin đính kèm theo thư điện tử.

Thực hiện sao lưu định kỳ dữ liệu: Cần tiến hành sao lưu định kỳ dữ liệu thường xuyên để có thể khôi phục dữ liệu khi máy tính bị Ransomware gây hại, các cơ quan, tổ chức có thể tham khảo một số biện pháp sau:

Sử dụng các ổ lưu trữ USB, ổ đĩa cắm ngoài, ổ chia sẻ mạng v.v... Cần chú ý dữ liệu trong các ổ lưu trữ này hoàn toàn có thể bị ảnh hưởng nếu kết nối vào máy tính đã bị nhiễm mã độc Ransomware. Do vậy phải đảm bảo máy chưa bị nhiễm mã độc trước khi sao lưu hoặc khởi động máy tính từ ổ đĩa khởi động ngoài khi thực hiện sao lưu để đảm bảo an toàn.

Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu như: các máy chủ quản lý tệp tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi của tập tin mà khi xảy ra sự cố có thể khôi phục lại từ thời điểm trước đó.

### **1.3. Kết luận chương**

Chương 1 luận văn đã trình bày cơ bản về thực trạng của mã độc Ransomware bao gồm các nội dung: lịch sử phát triển, mức độ nguy hiểm, thực trạng tại Việt Nam và thế giới, cách nhận biết, một số biện pháp phòng tránh tạm thời và khuyến nghị, quy trình xử lý khi nhiễm mã độc. Các nội dung trên nhằm giúp người sử dụng có một cái nhìn tổng quát và nhận thức rõ ràng về mối nguy hại mã hóa dữ liệu. Trong chương 2 luận văn tập trung thử nghiệm các phương pháp phân tích mã độc, môi trường phân tích mã độc và những công cụ hỗ trợ để tiến hành phân tích các mẫu mã độc Ransomware để tìm những hành vi đặc trưng nhất, dấu hiệu nhận biết những hành vi này làm tiền đề cho ý tưởng xây dựng giải pháp phát hiện mã độc Ransomware dựa trên hành vi đặc trưng.

## Chương 2: PHƯƠNG PHÁP PHÂN TÍCH, PHÁT HIỆN MÃ ĐỘC RANSOMWARE

### 2.1. Một số phương pháp phát hiện nhanh trong thực tiễn

#### 2.1.1. Thông qua danh sách đen (blacklist)

Phương pháp phát hiện dựa trên dấu hiệu kết nối mạng đến các danh sách địa chỉ IP, máy chủ điều khiển C&C thuộc danh sách đen đã biết. Trong luận văn sử dụng cơ sở dữ liệu các máy chủ điều khiển C&C, địa chỉ TOR thuộc danh sách đen để phát hiện loại mã độc này. Danh sách được cập nhật từ nguồn được chia sẻ miễn phí trên trang web <https://ransomwaretracker.abuse.ch/blocklist/>.

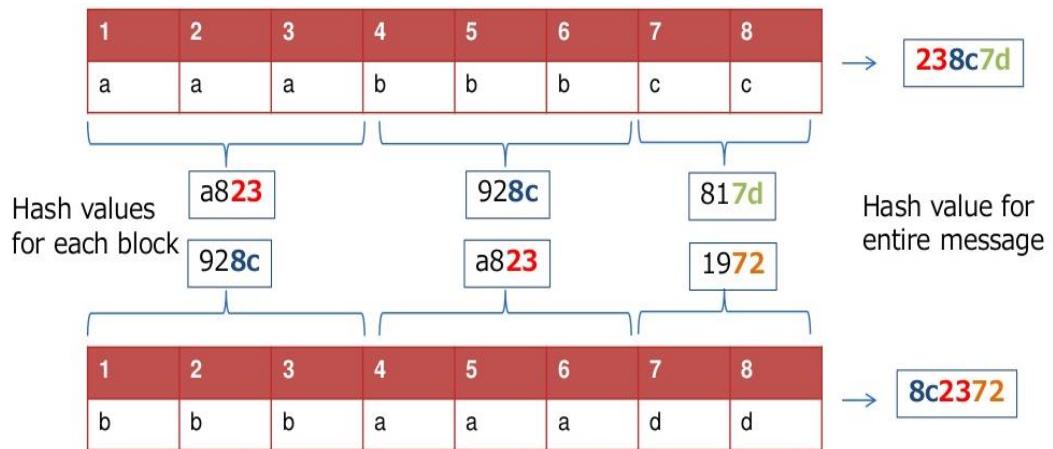
#### 2.1.2. Hashing, dấu vân tay của malware

Hashing là một phương pháp phổ biến được sử dụng để định danh malware. Dựa file malware qua một chương trình hashing sẽ tạo ra một giá trị hash duy nhất. Với đặc tính của thuật toán hash, chỉ cần dữ liệu đầu vào sai khác 1 bit, thì giá trị hash đầu ra sẽ có những sai khác rất lớn và không thể dự đoán được nên giá trị hash đó là định danh của malware, không thể có 2 file khác nhau mà có giá trị hash giống nhau. Thuật toán Message Digest Algorithm 5 (MD5) thường được sử dụng nhiều nhất, tiếp sau là Secure Hash Algorithm 1 (SHA-1) cũng khá phổ biến. Hiện nay chuyên trang virutotal.com đang được sử dụng rất nhiều với hàng chục các hãng Antivirus uy tín.

#### 2.1.3. Kỹ thuật Fuzzy hashing

Vẫn sử dụng kỹ thuật nhận dạng mã độc thông qua mã hash tuy nhiên đã được bổ sung thêm các phân tích và tính toán để từ một mã hash của mã độc, có thể nhận dạng ra các hash họ hàng của mã độc từ đó nâng cao khả năng phát hiện mã độc. Ưu điểm của kỹ thuật này là nó cao cấp hơn kỹ thuật checksum vì được cải tiến kỹ thuật phát hiện họ hàng của mã độc. Tuy nhiên nhược điểm của nó nằm ở

chỗ xây dựng các thuật toán và lựa chọn độ dài ký tự phù hợp là khó khăn dẫn đến có khả năng cảnh báo giả và cảnh báo sai.



Hình 2.1: thuật toán Fuzzy Hashing

#### 2.1.4. Kỹ thuật Scan String

Kỹ thuật này sử dụng một chuỗi trích ngang (chuỗi byte) là đặc trưng của tập tin mã độc và không tồn tại trong các tập tin sạch để làm cơ sở dữ liệu mẫu dùng để nhận dạng mã độc. Với ưu điểm nhận dạng chính xác, tốc độ nhận dạng nhanh hơn so với kỹ thuật checksum, tuy nhiên quá trình xây dựng và cập nhật cơ sở dữ liệu phức tạp, nhận dạng bị động và không phát hiện được mã chương trình bị thay đổi.

#### 2.1.5. Kỹ thuật Code Emulation

Là một kỹ thuật phát hiện mã độc dựa trên việc mô phỏng lại hệ thống CPU, hệ thống quản lý bộ nhớ, các mã máy ở cấp thấp. Ưu điểm mã độc hoạt động độc lập không ảnh hưởng đến hệ thống máy thật. Nhược điểm quá trình mô phỏng đòi hỏi kỹ thuật cao.

### 2.2. Môi trường hỗ trợ phân tích, phát hiện mã độc

#### 2.2.1. Cơ sở lý thuyết

Để phân tích mẫu mã độc, trước hết người phân tích phải chắc chắn có một môi trường chuẩn để tiến hành phân tích, đây là điều rất quan trọng ảnh hưởng trực tiếp đến kết quả phân tích. Môi trường cần phải đầy đủ các phần mềm, bộ công cụ

cần thiết. Có hai cách xây dựng môi trường phân tích là xây dựng trực tiếp trên phần cứng hoặc xây dựng hệ thống phân tích trên phần mềm. Khi xây dựng môi trường phân tích trên phần cứng sẽ có lợi thế đối với một số mã độc tinh vi có cơ chế chống gỡ lỗi (debug) khi nhận thấy môi trường phân tích là máy ảo. Nhưng bất lợi là khi xây dựng môi trường trên phần cứng chi phí đầu tư, vận hành rất cao. Trái với xây dựng môi trường phân tích trên phần cứng, xây dựng môi trường phân tích trên phần mềm đang là lựa chọn đáp ứng tốt việc phân tích mã độc hiện nay. Môi trường phân tích sẽ được xây dựng dựa trên phần mềm có nhiều ưu điểm, được sử dụng các thiết bị phần cứng ảo hóa với số lượng lớn mà chi phí thấp. Chức năng chụp trạng thái (Snapshot) của phần mềm ảo hóa cho phép người phân tích ghi lại một trạng thái của máy ảo với thời gian rất nhanh, ngoài ra có thể trả máy ảo về thời điểm trước khi thực hiện một thao tác nào đó.

### **2.2.2. Sử dụng môi trường ảo hóa**

Công nghệ máy ảo VMware Workstation là một phần mềm ảo hóa mạnh mẽ dành cho các nhà phát triển, kiểm tra phần mềm và các chuyên gia công nghệ cần chạy nhiều hệ điều hành (HĐH) cùng lúc trên một máy vật lý. Người dùng có thể chạy các HĐH Windows, Linux, Netware hay Solaris trên các máy ảo mà không cần phải khởi động lại hay phân vùng ổ cứng. Khi sử dụng phần mềm VMware Workstation người sử dụng có thể tạo nhiều máy ảo bên trong và các máy ảo này chia sẻ CPU, RAM, Card mạng với máy tính thật. Điều này cho phép xây dựng nên một hệ thống với một vài máy tính được nối với nhau theo một mô hình nhất định, người sử dụng có thể tạo nên hệ thống của riêng mình đảm bảo môi trường cho mã độc hoạt động hết hành vi của mình. Snapshot là một tính năng rất hay của Vmware, ý nghĩa của nó như sau:

- Giúp lưu lại tình trạng của máy tính tại một thời điểm bất kỳ.
- Hỗ trợ khôi phục máy tính về một thời điểm đã được tạo snapshot trước đó.
- Chức năng snapshot giúp cho việc khôi phục hệ thống trở nên đơn giản hơn mà không cần phải cài lại HĐH hay xóa đi các dịch vụ, ứng dụng đã cài đặt trước đó.

Đặc biệt trong trường hợp người dùng triển khai thành công một hệ thống phức tạp và muốn cài đặt thêm một chức năng nào đó thử nghiệm mà sau đó muốn loại bỏ nó khỏi hệ thống, hoặc lo ngại một thời gian sau sẽ không chạy được nữa, người dùng có thể tạo snapshot của hệ thống tại thời điểm đó và nếu xảy ra bất cứ trục trặc gì, chỉ cần restore lại trạng thái đã tạo snapshot.

#### 2.2.2.1. Lựa chọn hệ điều hành

Lựa chọn một hệ điều hành để làm môi trường hoạt động của mã độc, thông thường người phân tích thường chọn phiên bản HĐH Windows XP SP3. Thứ nhất Windows là hệ điều hành phổ biến của tất cả mọi loại mã độc (trừ mã độc dành cho mobile) có thể hoạt động được. Thứ hai, hệ điều hành này gọn nhẹ và đơn giản, chỉ cần 512MB RAM là đủ cho việc phân tích các mẫu malware nhỏ đến vừa. Các dịch vụ trên XP cũng ít và đơn giản, không rắc rối và nhiều như các phiên bản sau của họ Windows. Và SP3 là phiên bản ổn định nhất của hệ điều hành này. So với SP2, SP3 được phép cài đặt nhiều gói phần mềm từ Microsoft hơn. Người phân tích cần chú ý tắt các dịch vụ ảnh hưởng đến mạng của Windows như Windows Update, Firewall... để tránh cản trở mã độc hoặc các gói tin bị lẩn vào dữ liệu mạng giám sát.

#### 2.2.2.2. Chuẩn bị kết nối mạng

Nên sử dụng một hệ thống mạng riêng (vlan riêng đã được cấu hình không ảnh hưởng đến vlan khác) để phân tích cho phép mã độc kết nối ra mạng thật qua chức năng chọn kết nối mạng NAT hoặc Bridge. Việc này giúp cho việc giám sát không bị lẩn các gói tin của mạng khác, ứng dụng khác. Nếu cho phép mã độc kết nối ra hệ thống mạng thật, mã độc sẽ lấy về những dữ liệu thật và thực hiện những thao tác phá hoại thật giúp người phân tích thu thập được nhiều thông tin quan trọng.

### 2.2.2.3. Cài đặt các gói phần mềm hỗ trợ cần thiết

Với sự đa dạng của mã độc chỉ có hệ điều hành là chưa đủ để thực thi mã độc, một số loại mã độc được viết bằng .Net, Java, ... nên người phân tích cần phải cài đặt các gói nền tảng Net Framework (tất cả các bản từ 2.0 đến mới nhất) và Java Runtime Environment các bản cũ 32 bit vì tính tương thích với hệ điều hành, Adobe Flash Player, Office 2003...

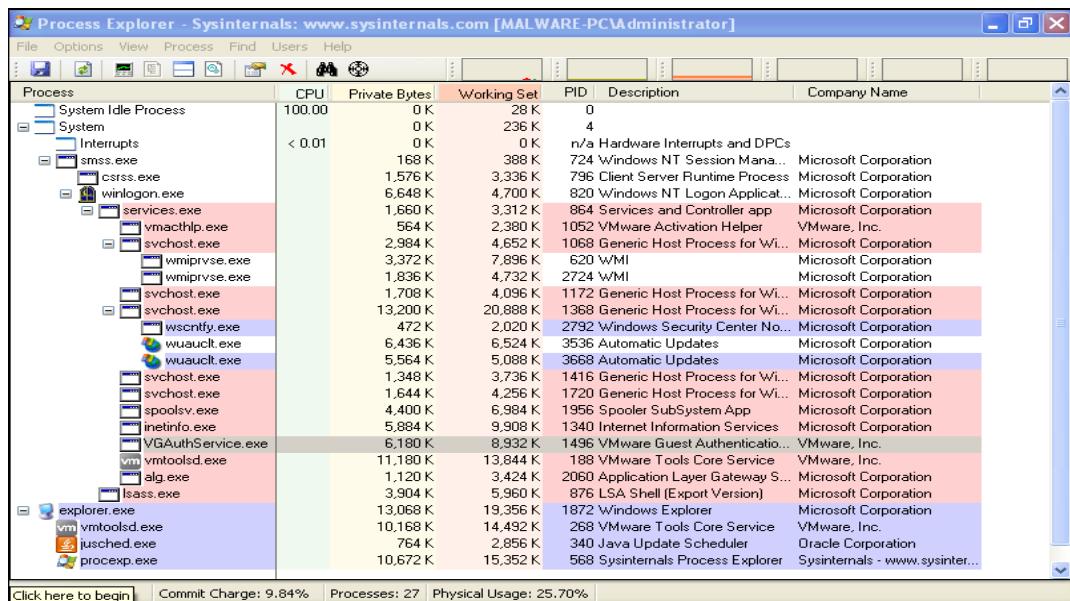
### 2.2.3. *Công cụ trợ giúp*

Việc lựa chọn các công cụ phân tích giúp người phân tích giảm tài công việc cũng nhưng làm cho quá trình phân tích diễn ra nhanh hơn, mang lại kết quả chính xác hơn.

Bộ công cụ phân tích do chính Microsoft cung cấp có tên “Sysinternals Suite”. Bộ này bao gồm đầy đủ các công cụ để giám sát những gì đang diễn ra trong hệ điều hành Windows. Người phân tích có thể giám sát mọi tác động lên một máy tính thông thường. Các công cụ theo dõi mọi tiến trình trong hệ thống thường dùng : Process Explorer (procexp.exe), Process Monitor (procmon.exe), Strings...

#### 2.2.3.1. Process Explorer

Cho phép xem danh sách các tiến trình dưới dạng cây của từng tiến trình và dịch vụ đang chạy dưới tiến trình nào.



Hình 2.2: Process Explorer

### 2.2.3.2. Process Monitor

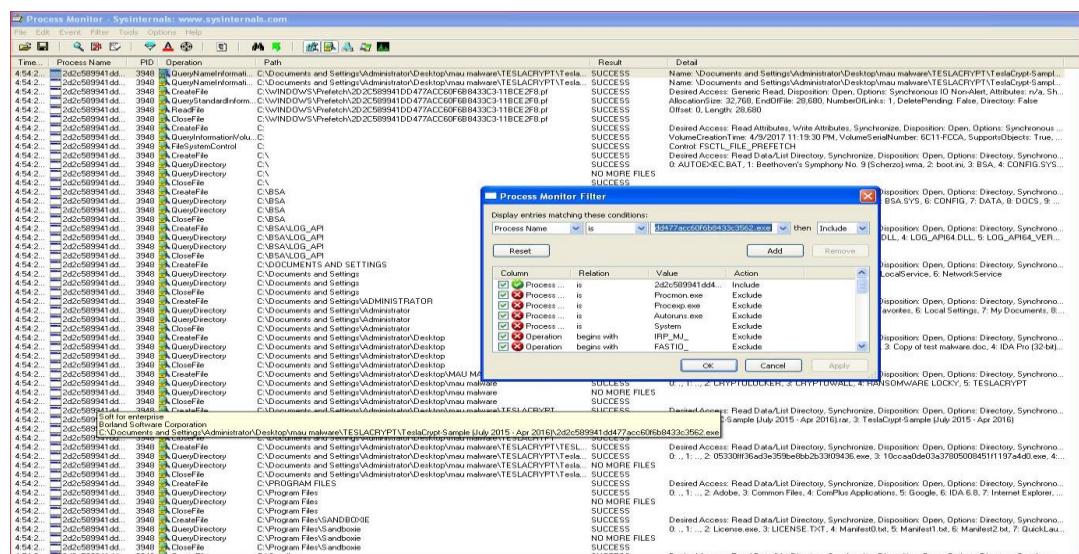
Process Monitor hay procmon là một công cụ giám sát nâng cao cho Windows, cung cấp một phương pháp để giám sát những hoạt động nhất định của registry, hệ thống file, mạng, process và thread. Mặc dù procmon thu thập một lượng lớn dữ liệu, nhưng không phải tất cả. Nó có thể không bắt được hoạt động của các trình điều khiển thiết bị (device driver) của thành phần user-mode đang giao tiếp với rootkit qua điều khiển I/O, cũng như là lệnh gọi GUI như SetWindowsHookEx. Cột Operation sẽ nhanh chóng cho ta biết những hoạt động mà process thực hiện trên hệ thống, ở đây bao gồm các hoạt động trên file, và registry.

Sử dụng bộ lọc để xem các lời gọi hệ thống khác như RegSetValue, CreateFile, WriteFile, Process Name (biet ten file ma doc dang chay), Operation (Làm gì vào đâu), và Detail (chi tiết hơn). Cuối cùng là lựa chọn hiển thị "Include" hay không hiển thị "Exclude" trên giao diện chính của procmon. Ngoài ra procmon cung cấp 5 nút lọc nhanh trên giao diện để sử dụng lần lượt là:

- Show Registry Activity: hiển thị các sự kiện liên quan đến registry
- Show File System Activity: hiển thị các sự kiện liên quan đến file

- Show Network Activity: hiển thị các sự kiện liên quan đến mạng
- Show Process and Thread Activity: hiển thị các sự kiện liên quan đến process và thread.
- Show Profilling Events: hiển thị những sự kiện liên quan đến thời gian sử dụng bộ xử lý của process.

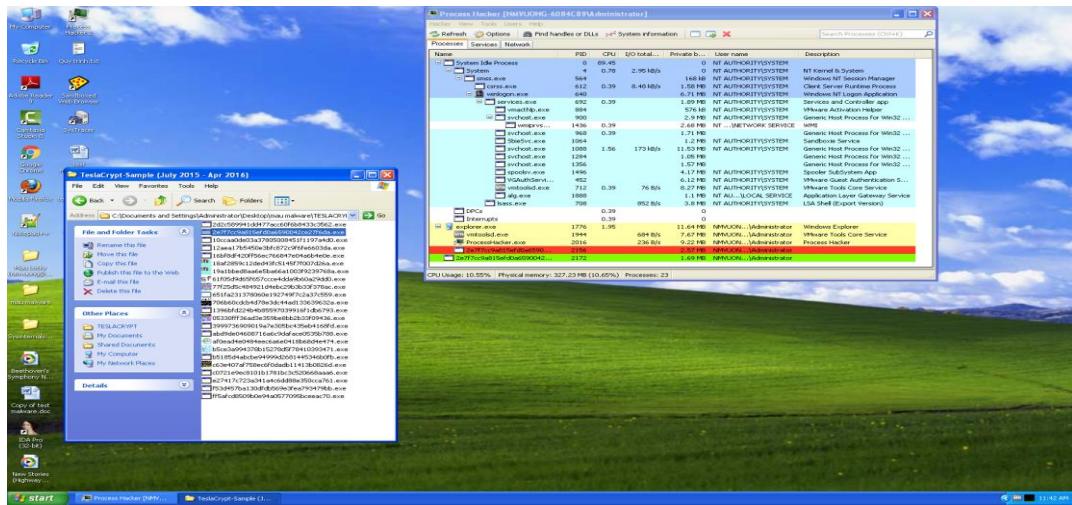
Nếu malware khởi chạy cùng hệ thống lúc khởi động, sử dụng Options chọn Enable Boot Logging để cài đặt procmon như là một startup driver để bắt những sự kiện startup. Phân tích những sự kiện được ghi lại bởi procmon cần sự kiên nhẫn, có rất nhiều sự kiện thuộc về hoạt động khởi động bình thường của file thực thi. Nhưng đây vẫn là cách dễ nhất để quan sát và đánh giá hoạt động của malware.



Hình 2.3: Process Moniter

### 2.2.3.3. ProcessHacker

Là một tiện ích miễn phí, có thể chỉ ra tất cả những thông tin liên quan đến tất cả các tiến trình đang hoạt động trên một giao diện cũng tương tự như Task Manager.

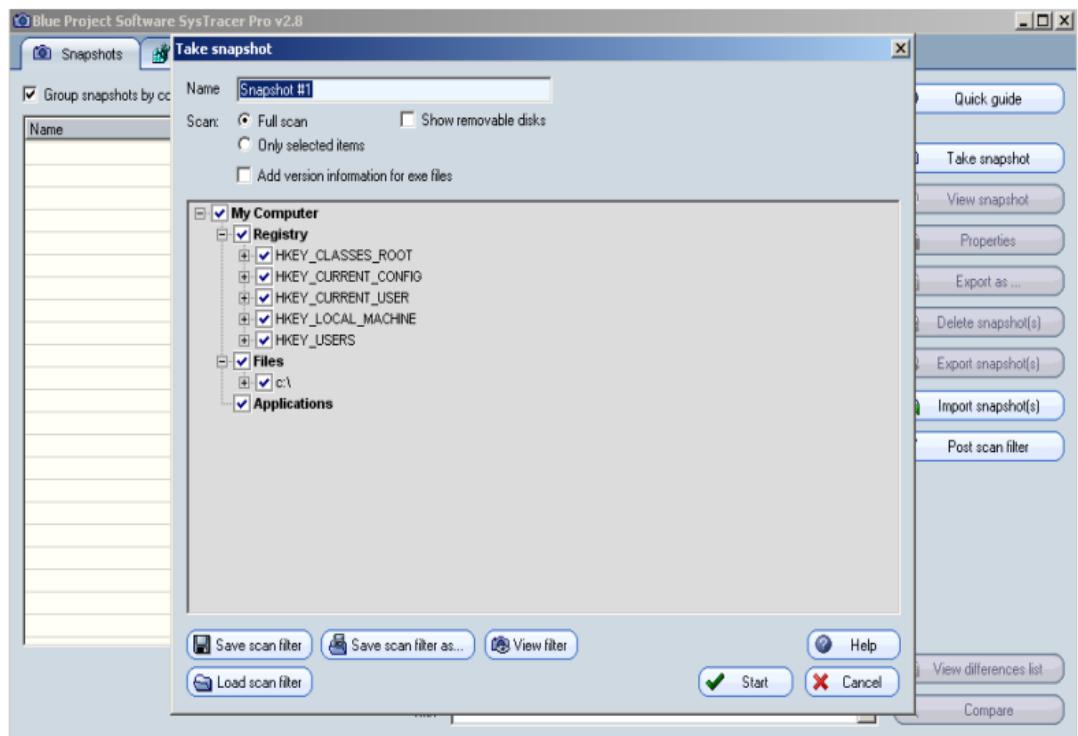


Hình 2.4: Process Monitor

### 2.2.3.4. SysTracer (Blue Project)

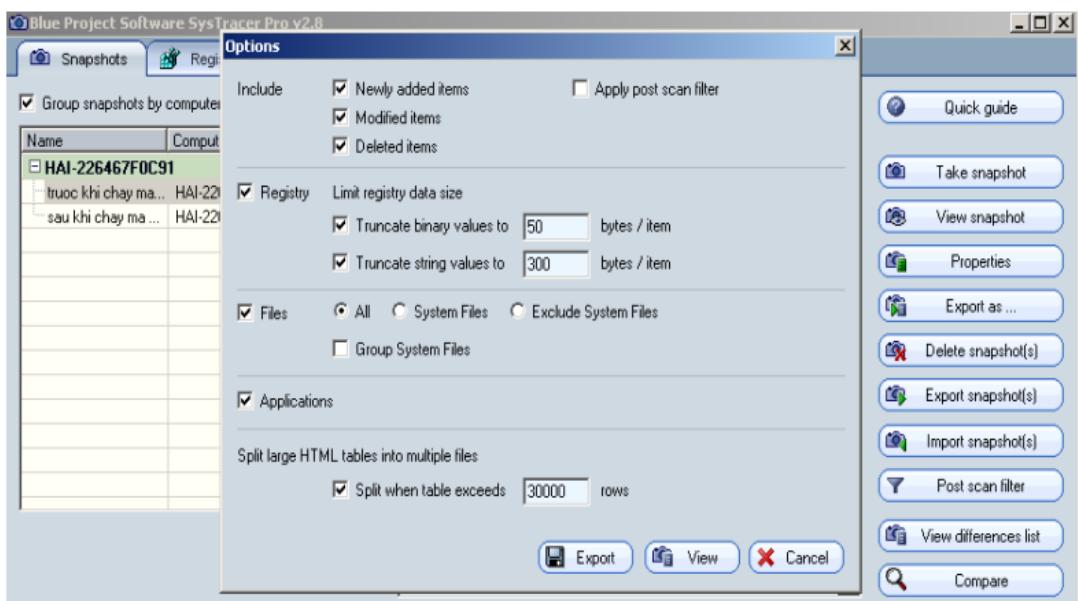
Chức năng chính của SysTracer là tạo snapshot và so sánh hai snapshot với nhau để hiển thị những sự thay đổi. Chúng ta sẽ tạo một snapshot tại thời điểm trước khi chạy malware và một snapshot sau khi chạy malware để xem malware có thêm, sửa, xóa tệp tin và registry hay không. Virus và Ransomware là hai dòng mã độc tác động rất nhiều vào hệ thống tệp tin. Do đặc tính của mình, virus sẽ thực hiện tìm kiếm những tệp tin đối tượng thích hợp và đính kèm chính nó vào những tệp tin đó. Ransomware thì sẽ mã hóa, làm thay đổi toàn bộ tệp tin, nhưng Ransomware sẽ dễ phát hiện hơn bởi sau khi thực hiện xong nó sẽ thông báo cho người dùng.

Bước 1: Tạo một bản snapshot ở trạng thái sạch trước khi chạy mã độc



Hình 2.5: Systracer

Bước 2: So sánh với trạng thái sau khi chạy mã độc để quan sát sự thay đổi của hệ thống regedit, file...



Hình 2.6: Tạo Snapshot sau khi chạy mã độc

### 2.2.3.5. Các công cụ khác

**PEview:** Công cụ phân tích header của file PE. Cho phép ta xem mọi thông tin có trong file PE như ngày giờ biến dịch, các section, các Import và Export Function.

**Regshot:** Theo dõi sự thay đổi của Registry. Chỉ cần trước khi kích hoạt malware công cụ này sẽ capture lại Registry và capture lại Registry lần nữa sau khi đã kích hoạt mẫu thì người dùng sẽ có được thông tin về các giá trị bị thay đổi dưới dạng text dễ nhìn.

**PEiD:** Công cụ phân tích PE signature mạnh mẽ, cho phép người dùng biết được file PE được tạo ra bằng ngôn ngữ gì, công cụ gì, version, và thông tin về packer đã được sử dụng. Dùng những thông tin này, người dùng sẽ dễ dàng hơn trong việc phân tích file PE dựa vào các đặc trưng của từng ngôn ngữ lập trình. Ngoài ra PEiD còn hỗ trợ các plugin cho phép người dùng thực hiện một số tính năng đặc biệt ngay trong cửa sổ chương trình như tìm OEP, view strings, calculate checksum, hoặc thậm chí là unpack.

**OllyDBG, IDA:** Các công cụ dịch ngược mã nhị phân file PE.

**Wireshark:** Công cụ không thể thiếu trong việc phân tích mạng thông qua các gói tin nó bắt được hoặc từ các tệp tin PCAP xuất ra từ hệ thống giám sát, nó thay thế được cho gần như mọi công cụ phân tích mạng khác.

**Sandbox:** Công cụ phân tích hành vi của các tệp tin thực thi như: dll, exe, bin... Vd: Norman SandBox, GFI Sandbox, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis, Cuckoo Sandbox, Malwr...

## 2.3. Phân tích đánh giá các phương pháp

Thông thường khi tiến hành phân tích mã độc chúng ta chỉ có mẫu mã độc dưới dạng tệp tin thực thi, và không thể đọc trực tiếp tệp tin này để tìm kiếm hành vi của mã độc. Để có thể hiểu được mã độc người phân tích sẽ sử dụng những công cụ khác nhau, mỗi công cụ sẽ tiết lộ một chút thông tin về mã độc. Từ những mảnh

nhỏ thông tin đó người phân tích sẽ có được một bức tranh đầy đủ chi tiết về mã độc.

Có hai cách tiếp cận để phát hiện mã độc

- Phát hiện mã độc dựa vào dấu hiệu đặc trưng
- Phát hiện mã độc dựa vào đặc điểm bất thường

Có hai cách tiếp cận để phân tích mã độc

- Phương pháp phân tích tĩnh (code (static) analysis)
- Phương pháp phân tích động (behavioral (dynamic) analysis)

Cả 2 phương pháp cùng có mục đích “giải thích” cách hoạt động của mã độc, công cụ, tuy nhiên thời gian làm việc và kỹ năng cần có thì lại rất khác nhau. Phân tích tĩnh thường đòi hỏi người phân tích xem xét kỹ mã của virus (đã được chuyển sang dạng có thể hiểu được như assembly hay C), hiểu được luồng thực thi và các hành vi của nó thông qua mã đã dịch ngược. Phân tích động là phân tích cách hoạt động của mã độc khi nó được thực thi, nó kết nối đến đâu, lây lan như thế nào, cài đặt những gì vào hệ thống, thay đổi thành phần nào, hoạt động ra sao. Mỗi phương pháp đều có điểm mạnh, yếu riêng. Trong phần tiếp theo tôi sẽ làm rõ hơn về hai phương pháp này.

### **2.3.1. Phương pháp phân tích tĩnh**

#### **2.3.1.1. Phương pháp phân tích tĩnh mức cơ bản**

Bao gồm việc kiểm tra các tập tin thực thi. Phân tích tĩnh cơ bản có thể xác định một tập tin là độc hại, cung cấp các thông tin chức năng của tập tin độc hại đó, và đôi khi cung cấp thông tin mà sẽ cho phép người dùng tạo ra các chữ ký mạng đơn giản. Phân tích tĩnh cơ bản thì đơn giản và nhanh chóng, tuy nhiên nó sẽ không hiệu quả hoặc bỏ sót những hành vi quan trọng khi gặp phải các phần mềm độc hại sử dụng các kỹ thuật chống dịch ngược mã tinh vi.

### 2.3.1.2. Phương pháp phân tích tĩnh mức nâng cao

Với những loại mã độc phức tạp để đọc hiểu được hết mã thực thi của nó là một việc rất khó cần phải thực hiện phân tích tĩnh nâng cao. Phương pháp này cung cấp cho người phân tích cái nhìn hết sức chính xác về những gì mà mã độc tác động lên hệ thống. Để làm được việc này cần thực hiện kỹ thuật dịch ngược (Reverse Engineering) nội dung bên trong của mã độc bằng cách đọc tập tin thực thi vào một bộ phân tích và xem xét các chỉ thị của chương trình để phát hiện các chương trình nghi ngờ. Các chỉ thị được thực thi bởi CPU, phân tích tĩnh nâng cao sẽ cho biết tiến trình nào là đáng ngờ. Tuy nhiên, phân tích tĩnh nâng cao đòi hỏi kiến thức chuyên môn về lập trình, cấu trúc mã lệnh, và các khái niệm về hệ điều hành với thời gian phân tích lâu và tốn rất nhiều công sức.

### 2.3.1.3. Một số hàm thư viện quan trọng

Phân tích tĩnh được thực hiện dưới sự hỗ trợ của các công cụ debugger, disassembler, decompiler (như OllyDbg, IDA, WinDbg...). Trong khi phân tích động dựa vào các công cụ monitor hệ thống, mạng (như ProcessMon, network monitor, TcpView, Autoruns...). Để thực hiện trích xuất những thông tin quan trọng từ tập tin chứa mã độc

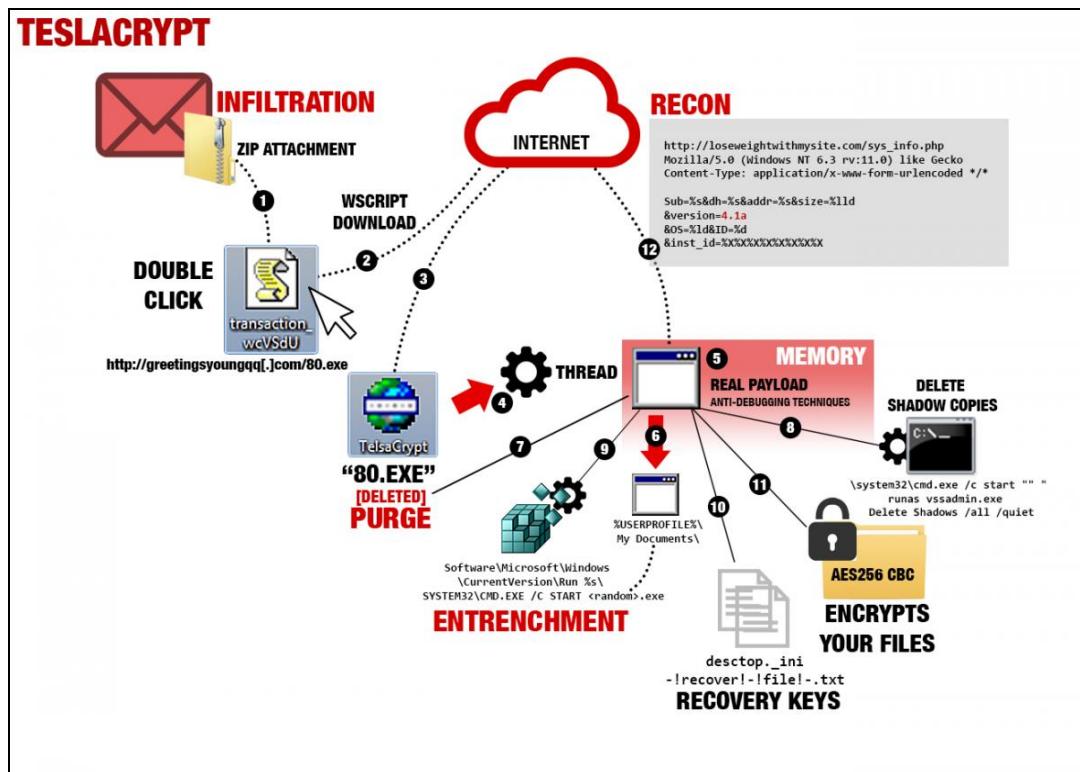
Ý nghĩa một số hàm, thư viện:

- Hàm **LoadLibrary** và **GetProcAddress** cho phép một chương trình truy cập vào bất cứ hàm nào trong bất kỳ thư viện nào trên hệ thống.
- Hàm **CreateProcessA**, **CreateMutexA**, **OpenMutexA** liên quan đến việc tạo process, tạo và mở mutex, có thể malware sẽ tạo thêm process mới, đồng bộ bằng mutex.
- Thư viện **WS2\_32.dll**: Đây là một thư viện chứa các hàm sử dụng để giao tiếp mạng, có thể malware sẽ kết nối ra ngoài internet.
- Thư viện **Kernel32.dll**: Đây là một DLL rất phổ biến và có chức năng cốt lõi quan trọng, cho phép truy cập thao tác trên bộ nhớ, tập tin, và hệ thống phần cứng.

- Thư viện **Advapi32.dll**: Đây là DLL cung cấp việc truy cập tới các thành phần cốt lõi cao cấp của Windows như là Service Manager và Registry.
- Thư viện **User32.dll**: Đây là DLL chứa tất cả các thành phần giao diện người dùng, như là các nút (buttons), các thanh cuộn (scroll bars), và các thành phần cho việc kiểm soát và hồi đáp các hành động tác vụ của người dùng.
- Thư viện **Gdi32.dll**: Đây là DLL chứa các chức năng hiển thị và các thao tác đồ họa.
- Thư viện **Ntdll.dll**: DLL này là giao diện tương tác với nhân của Windows (Windows Kernel). Các tác vụ thực thi thường không thêm trực tiếp tập tin này khi chạy, mà nó luôn được thêm gián tiếp thông qua tập tin Kernel32.dll. Nếu một tiến trình thực thi thêm tập tin này vào, nó có nghĩa là tác giả có ý định sử dụng chức năng ẩn đối với các chương trình Windows. Một vài nhiệm vụ như ẩn các chức năng hay các tiến trình hoạt động sẽ sử dụng giao diện tương tác này.
- Thư viện **WSock32.dll** và **Ws2\_32.dll**: Đây là các DLLs về hệ thống mạng. Một chương trình có thể truy cập một là bằng các kiểu kết nối thông dụng nhất tới hệ thống mạng hoặc thực hiện các tác vụ liên quan tới hệ thống mạng.
- **Wininet.dll**: Đây là DLL chứa các chức năng mạng cao cấp hơn như triển khai thực hiện các giao thức như FTP, HTTP, và NTP.

#### 2.3.1.4. Minh họa quá trình thực hiện phân tích tĩnh mẫu mã độc TeslaCrypt

Đây là mẫu mã độc Ransomware khá phổ biến và nhiều biến thể nguy hiểm, chúng đã có cả một chiến dịch thuê bén thứ 3 để phát tán thư rác có chứa mã độc đến người dùng. Hình dưới đây mô tả về quá trình từ khi phát tán mã độc đến khi mã hóa thông tin của nạn nhân và cảnh báo đòi tiền chuộc.



Hình 2.7: Tổng quan về TeslaCrypt

### a. Quá trình phát tán

Phát tán phần mềm trình downloader đến người dùng: TeslaCrypt được phân phối sử dụng một tập tin đính kèm được nén trong email chứa một downloader JavaScript. Theo thông tin từ các tổ chức nghiên cứu bảo mật uy tín như Kapersky TeslaCrypt Ransomware có cả một chiến dịch phát tán mail bằng cách thuê một bên thứ 3 chuyên nghiệp.

### b. Quá trình cài đặt lây nhiễm

Sau khi người dùng click vào link file zip đính kèm sẽ được tải chia sẻ một file có tên **transaction\_wcVsdU.js**. Khi người dùng giải nén gói tin này và file JavaScript được thực thi, Windows Script Host (Microsoft Windows Script Host (WSH) là một công nghệ tự động của hệ điều hành Microsoft Windows cung cấp các kịch bản thực thi các tệp tin batch, nhưng với nhiều tính năng được hỗ trợ) sẽ chạy và thực thi JavaScript. Trình “downloader” khởi tạo một yêu cầu HTTP GET đến URI sau đây để tải về mã độc TeslaCryp

t: [http://greetingsyoungqq\[.\]com/80.exe](http://greetingsyoungqq[.]com/80.exe). Nếu yêu cầu thành công, mã nhị phân sẽ được ghi vào đĩa trong thư mục %TEMP% của người dùng hiện tại.

Phiên bản thông tin chứa trong metadata của nó sẽ giúp việc cấy ghép và giả mạo chính nó như là một hệ thống DLL chính thức của Windows.

English (United States) (1033/1200)	
File Version	5.1.2600.5512 (xpsp.080413-2105)
Company name	Microsoft Corporation
Internal name	MSUTB
Copyright	© Microsoft Corporation. All rights reserved.
Original filename	MSUTB.DLL
Product name	Microsoft® Windows® Operating System
Product version	5.1.2600.5512
File description	MSUTB Server DLL

**Hình 2.8: Giả mạo chứng chỉ**

Khi thực hiện, nó sẽ giải nén và ghi vào một tệp tin PE sạch nằm trong bộ nhớ heap (heap memory - Khi người dùng chạy chương trình Java, JVM sẽ yêu cầu hệ điều hành cấp cho một không gian bộ nhớ trong RAM để dùng cho việc chạy chương trình. JVM sẽ chia bộ nhớ được cấp phát này thành 2 phần: Heap và Stack cho việc quản lý). Tệp tin PE sạch này chứa các lời gọi hàm, thư viện mà nó đã cấy ghép để thực hiện chức năng độc hại.

### c. Các kỹ thuật chống phân tích

Làm rối code (String Obfuscation) để tránh bị phát hiện và ẩn đi những chuỗi gốc của nó, những mã nhị phân được sử dụng khen liên lạc giữa các tiến trình (COM objects). Bằng cách sử dụng các API CoInitialize và CoCreateInstance của Windows. Những cấy ghép đó có thể được DirectShow điều khiển thông qua Software\Microsoft\DirectShow\PushClock sử dụng một khen bí mật với thư viện quartz.

```

mov    [esp+350h+var_200], esi
call   ds:CoInitializeEx
mov    edi, ds:LoadLibraryW
push   offset aCoCreateInstan ; "CoCreateInstance"
push   offset aOle32_dll_0 ; "Ole32.dll"
call   edi, LoadLibraryW
mov    ebx, ds:GetProcAddress
push   eax,          ; hModule
call   ebx, GetProcAddress
lea    edx, [esp+348h+var_334]
push   edx

```

**Hình 2.9: Làm rối code (String Obfuscation)**

Chống gỡ lỗi (anti-debugging): TeslaCrypt gọi chức năng chống gỡ lỗi (anti-debugging) nhiều lần để ngăn chặn gỡ lỗi tự động hoặc theo dõi API. Bằng cách sử dụng các kỹ thuật né tránh QueryPerformance/GetTickCount, lưu trữ bộ đếm thời gian đầu vào của một tiến trình và sau đó ghi lại nó ở cuối của tiến trình.

Chống giám sát (anti-monitoring): Biến thể TeslaCrypt được thiết kế để vô hiệu hóa 5 ứng dụng giám sát tiêu chuẩn của Windows. Các mã nhị phân liệt kê tắt cả các tiến trình hoạt động và sử dụng GetProcessImageFileName để lấy tên tập tin thực thi trong mỗi tiến trình. Một tiến trình sẽ được chấm dứt nếu tên tập tin của nó có chứa bất kỳ của các chuỗi sau đây:

- taskmgr (Task Manager)
- regedi (Registry Editor)
- proce (SysInternals Process Explorer)
- msconfig (System Configuration)
- cmd (Command Shell)

004067E0	68 00100000	PUSH 1000	Arg2 = 1000
004067E5	50	PUSH EAX	Arg1
004067E6	E8 14DE0000	CALL 004145FF	Binary.004145FF
004067EB	8B00 40624700	MOV ECX,DWORD PTR DS:[476240]	ASCII "p4,"
004067F1	8B41 60	MOU EAX,DWORD PTR DS:[ECX+60]	
004067F4	50	PUSH EAX	
004067F5	8D95 FCDFFFFF	LEA EDX,[EBP-2004]	
004067FB	52	PUSH EDX	
00406801	E8 AAE70000	CALL 00414FAB	Arg2 = UNICODE "taskmg"
00406804	83C4 10	ADD ESP,10	Arg1
00406805	-75 72	TEST EAX,EAX	Binary.00414FAB, _Wcsstr
00406808	A1 40624700	JNZ SHORT 0040687A	
0040680D	8B40 64	MOV EAX,DWORD PTR DS:[476240]	
00406810	50	MOU EAX,DWORD PTR DS:[EAX+64]	
00406811	8D80 FCDFFFFF	PUSH EAX	
00406817	51	LEA ECX,[EBP-2004]	
00406818	E8 8EE70000	PUSH ECX	
0040681D	83C4 08	CALL 00414FAB	Arg2
00406820	85C0	ADD ESP,8	Arg1
00406822	-75 56	TEST EAX,EAX	Binary.00414FAB, _Wcsstr
00406824	8B15 40624700	JNZ SHORT 0040687A	
0040682A	8B42 68	MOV EDX,DWORD PTR DS:[476240]	
0040682D	50	MOU EAX,DWORD PTR DS:[EDX+68]	
0040682E	8D85 FCDFFFFF	PUSH EAX	
00406834	50	LEA EAX,[EBP-2004]	
00406835	E8 71E70000	PUSH ECX	
0040683A	83C4 08	CALL 00414FAB	Arg2
0040683D	85C0	ADD ESP,8	Arg1
0040683F	-75 39	TEST EAX,EAX	Binary.00414FAB, _Wcsstr
00406841	8B00 40624700	JNZ SHORT 0040687A	
00406847	8B41 6C	MOV ECX,DWORD PTR DS:[476240]	
0040684A	50	MOU EAX,DWORD PTR DS:[ECX+6C]	
0040684B	8D95 FCDFFFFF	PUSH EAX	
00406851	52	LEA EDX,[EBP-2004]	
00406852	E8 54E70000	PUSH EDX	
00406857	83C4 08	CALL 00414FAB	Arg2
0040685A	85C0	ADD ESP,8	Arg1
0040685C	-75 1C	TEST EAX,EAX	Binary.00414FAB, _Wcsstr
0040685E	A1 40624700	JNZ SHORT 0040687A	
00406863	8B40 70	MOV EAX,DWORD PTR DS:[476240]	
00406866	50	MOU EAX,DWORD PTR DS:[EAX+70]	
00406867	8D80 FCDFFFFF	PUSH EAX	
0040686D	51	LEA ECX,[EBP-2004]	
0040686E	E8 38E70000	PUSH ECX	
00406873	83C4 08	CALL 00414FAB	Arg2
00406875	85C0	ADD ESP,8	Arg1
00406878	-74 09	TEST EAX,EAX	Binary.00414FAB, _Wcsstr
0040687A	> 6A 00	JZ SHORT 00406883	
0040687C	> 56	PUSH 0	
0040687D	> FF15 E8454800	PUSH ESI	
00406883	> 56	CALL DWORD PTR DS:[4845E8]	
00406884	> FF15 EC454800	PUSH ESI	
0040688A	> 47	CALL DWORD PTR DS:[4845FC]	
		INC EDI	

**Hình 2.10: Chống giám sát (anti-monitoring)**

d. Cơ chế trốn tránh

Mã độc thực hiện cấy ghép chính nó vào ô đĩa.

`">%UserProfile%\Documents\[12 random a-z characters].exe`".

Để duy trì thiết lập này lâu dài, mã độc còn thực hiện thay đổi một giá trị trong registry:

*HKCU\Software\Microsoft\Windows\CurrentVersion\Run\%s|*

**SYSTEM32\cmd.exe /c start %USERPROFILE%\Documents\[12 random  
a-z characters].exe**

Đăng ký giá trị registry:

**“HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections”**

Bằng cách đăng ký giá trị này chúng đều có thể lợi dụng cả người dùng thông thường và quản trị viên cho quyền kết nối thiết bị với mạng, điều này cho phép việc cấy ghép dễ dàng truy cập vào các tập tin trên kết nối mạng chia sẻ bên ngoài để mã hóa các tệp tin trên ổ cứng cục bộ. Trong môi trường mạng có kết nối sẽ làm tăng đáng kể nguy cơ lây lan và thiệt hại.

Mã hóa:

```

add    esp, 4
lea    edx, [ebp-60h]
push  edx, [ebp-60h] ; int
lea    eax, [ebp-148h]
push  eax, [ebp-148h] ; void *
mov   ecx, edi
call  secp256k1_ec_pubkey_create
lea    ecx, [ebp-148h]
push  ecx
push  edi
lea    esi, [ebp-14Ch]
mov   edi, offset unk_476360
call  secp256k1_ec_pubkey_serialize
mov   esi, [ebp-150h]
lea    edx, [ebp-40h]
push  edx, [ebp-40h] ; int
lea    eax, [ebp-148h]
push  eax, [ebp-148h] ; void *
mov   ecx, esi
call  secp256k1_ec_pubkey_create
lea    ecx, [ebp-148h]
push  ecx
push  esi
lea    esi, [ebp-14Ch]
lea    edi, [ebp-0F0h]
call  secp256k1_ec_pubkey_serialize
lea    edx, [ebp-40h]
push  edx
mov   ecx, offset unk_427E18

```

Hình 2.11: các tập tin được mã hóa bằng thuật toán AES256 CBC)

Color Mappings	Color Mappings
Victim ID: 76 34 E3 E3 06 CD FE F4	Victim ID: 76 34 E3 E3 06 CD FE F4
Generated PublicKey 1	Generated PublicKey 1
Master PrivateKey AES	Master PrivateKey AES
Master Sha256 PublicKey	Master Sha256 PublicKey
Generated PublicKey 2	Generated PublicKey 2
PrivateKey AES File	PrivateKey AES File
AES IV	AES IV

Hình 2.12: Tạo thông tin về nạn nhân

Thường xuyên gọi lại các yêu cầu HTTP POST: Sau khi mã hóa thành công dữ liệu của nạn nhân, malware khởi tạo một tiến trình khác và cố gắng yêu cầu http post đến các địa chỉ URI:

```

loseweightwithmysite[.]com/sys_info.php
helcel[.]com/sys_init.php
thinktrimbebeautiful[.]com[.]au/sys_init.php
lorangeriedelareine[.]fr/sys_init.php
bluedreambd[.]com/inifile.php
onguso[.]com/inifile.phploseweightwithmysite[.]com/sys_info.php
UserAgent: Mozilla/5.0 (Windows NT 6.3 rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
*/

```

Hình 2.13: Hành vi gửi dữ liệu về server

Dữ liệu POST được sử dụng để truyền tải các dữ liệu theo dõi nạn nhân. Bao gồm các thông tin như: cấu hình máy, thông tin phiên bản, địa chỉ hướng dẫn thanh toán Bitcoin...

Sub=[Ping: hardcoded callback mode]&dh=[combination of public and private key data]&addr=[bitcoin address generated at runtime]&size=0&version=[4.1a: hardcoded TeslaCrypt version number]&OS=[OS build number derived from VersionInformation.dwBuildNumber]&ID=[821: appears to be a hardcoded value possibly used to further identify a particular variant]&inst\_id=[user ID generated at runtime]

**Hình 2.14: Dữ liệu POST**

### Tổng hợp hành vi

**Bước 1:** Phát tán tập tin JavaScript đã nén và chứa phần mềm downloader.

**Bước 2:** Tập tin JavaScript là một downloader sử dụng môi trường hỗ trợ của Windows Script Host (WSH) hoặc Wscript để download mã. Khi tập tin JavaScript được giải nén và thực hiện, WSH sẽ được gọi để thực thi mã bên trong.

**Bước 3:** Chương trình downloader tải TeslaCrypt về cây ghép thông qua một yêu cầu HTTP đến “greetingsyoungqq[.]com/80.exe”. Sau đó mã nhị phân này sẽ được chạy bởi trình downloader.

**Bước 4:** Để trốn tránh gỡ lỗi, đoạn mã này sử dụng kỹ thuật trốn tránh QueryPerformance/GetTickCount để kiểm soát thời gian chạy.

**Bước 5:** Lưu các hàm vào bộ nhớ heap vào một file PE sạch.

Nó sẽ thiết lập một kênh truyền thông liên tiến trình với hàm CoInitialize(), CoCreateInstance(), APIs để giao tiếp thông qua DirectShow để thiết lập các chuỗi khác nhau trong bộ nhớ.

- Sử dụng hàm QueryPerformance/GetTickCount (hàm đo thời gian thực thi mã lệnh) để trốn tránh việc debugging.
- Sử dụng Wow64DisableWow64FsRedirection để tắt chuyển hướng tệp tin cho luồng gọi.
- Xóa Zone.Identifier ADS sau khi thực hiện thành công.
- Kiểm tra xác thực quyền hệ thống.

**Bước 6:** Tiếp theo, tệp tin PE thêm một bản sao chính nó vào đường dẫn: %UserProfile%\Documents\[12 random a-z characters].exe và tạo một tiến trình con và thêm quyền cho tệp tin mới riêng biệt này.

**Bước 7:** Xóa các đoạn mã cũ bằng %COMSPEC% /C DEL %S

**Bước 8:** Tạo "\_\_wretw\_w4523\_345" cho nhiều luồng hoạt động hơn và chạy một lệnh shell để xóa giá trị tệp tin ẩn copy.

**Bước 9:** Thêm giá trị vào registry

**Bước 10:** Trong quá trình mã hóa, nó sẽ tạo ra các khóa công khai dựa trên khóa riêng đã được mã hóa.

**Bước 11:** Mã hóa tất cả các tệp tin thư mục dự trên giá trị đuôi mở rộng của tệp tin.

**Bước 12:** Cuối cùng nó sẽ hiển thị chú ý đòi tiền chuộc thông qua: văn bản, hình ảnh, các trang web. Chương trình sẽ thông báo cho máy chủ C&C về nạn nhân mới.

Qua quá trình phân tích tinh tham khảo ta thấy mã độc thực hiện rất nhiều hành vi tinh vi nhằm thực hiện mục đích mã hóa các tệp tin của nạn nhân. Các kỹ thuật này cho thấy mã độc được thiết kế bởi những người am hiểu và có trình độ rất cao về công nghệ thông tin chính vì vậy nếu người phân tích không đủ kinh nghiệm và có những trình độ nhất định sẽ hoàn toàn bị người viết mã độc đánh lừa.

### 2.3.1.5. Đánh giá phương pháp phân tích tinh

#### a. Ưu điểm

Bằng cách phân tích các mẫu malware dựa trên các kỹ thuật phân tích dịch ngược và đọc chức năng hàm, chuyên viên phân tích sẽ xác định chính xác những gì đã xảy ra trên hệ thống, đảm bảo xác định được những máy, những loại tệp tin bị lây nhiễm. Khi phân tích mẫu mã độc nghi ngờ, xác định được mẫu nghi ngờ đó được viết bằng ngôn ngữ gì, chức năng các hàm làm gì từ đó tìm phương pháp để

xác định nó trên hệ thống. Kết quả phân tích mã độc từ các nguồn này được cập nhật những dấu hiệu (signature) vào phần mềm, hệ thống quét mã độc, IDS/IPS. Đây cũng chính là cách chủ yếu mà một số phần mềm antivirut đang thực hiện để xác định và lấy chữ ký mã độc.

### **b. Nhược điểm**

Phân tích tĩnh giúp hiểu rõ về hoạt động của mã độc tuy nhiên thời gian phân tích lâu và đòi hỏi người phân tích có trình độ chuyên gia. Sau khi phân tích và xác nhận mã độc, mã độc này sẽ được gán một chữ ký để phát hiện trong những lần gây hại khác. Lỗi hỏng cơ bản của phát hiện dựa trên chữ ký là không có khả năng phát hiện phần mềm độc hại chưa biết chưa có chữ ký. Một mã thực thi độc hại chỉ có thể được phát hiện khi nó đã được báo cáo là độc hại và được thêm vào kho lưu trữ chữ ký độc hại.

Để bỏ qua việc phát hiện dựa trên chữ ký, các nhà phát triển phần mềm độc hại Sử dụng kỹ thuật obfuscation mã để lặp lại các phần mềm độc hại để mỗi phiên bản xuất hiện khác nhau. Sự ngụy trang mã này không ảnh hưởng đến hành vi nguy hiểm được thiết kế, chỉ ảnh hưởng đến cách nó bị phát hiện bởi một hệ thống phát hiện do con người hoặc dựa trên chữ ký. Đối với các cuộc tấn công Ransomware, kỹ thuật obfuscation mã thường được sử dụng khi tạo ra tải trọng ở phía máy chủ. Một ví dụ về cuộc tấn công của phần mềm độc hại đã được nhìn thấy trong Cerber Ransomware, nơi mà máy chủ tấn công đã có thể tạo ra các mẫu tìm kiếm độc đáo mới mỗi 15 giây. Các hình thức khác của obfuscation mã xảy ra ở phía nạn nhân của nơi mà các phần mềm độc hại giải nén một biến thể duy nhất của payload thực thi mỗi khi nó thực thi. Loại phần mềm độc hại này có thể nhân bản các phiên bản của chính nó hay còn gọi thông thường là biến hình và đa hình.

Không hiệu quả với các cuộc tấn công được nhắm mục tiêu. Điều này đặc biệt liên quan đến trường hợp Ransomware, Ransomware tấn công nhắm mục tiêu xảy ra thường xuyên hơn. Thay vì phân phối phát triển Ransomware mới, các nhà

phát triển có thể chọn để lần đầu tiên giải phóng Ransomware mới nó sẽ tự biến đổi trên máy nạn nhân.

Để giải quyết bão toán này luận văn giới thiệu phương pháp phân tích động dựa trên công nghệ Sandbox, một cách tiếp cận hiện đại nhằm để đánh giá một tệp tin thực thi không phải thông qua phân tích hàm chức năng mà theo hành vi của nó.

### 2.3.2. Phương pháp phân tích động

Phân tích động là kiểm tra bất kỳ quá trình nào chạy khi thực thi mã độc. Phân tích động thường được tiến hành sau khi phân tích tĩnh đã không khả năng phân tích được mã độc, khi mà mã độc được sử dụng kỹ thuật làm rối obfuscation, pack hoặc khi đã sử dụng hết các kỹ thuật phân tích tĩnh sẵn có. Phân tích động còn có thể liên quan đến việc giám sát hoặc kiểm tra hệ thống sau khi mã độc được thực thi. Không giống phân tích tĩnh, phân tích động cho phép quan sát được chức năng của mã độc. Ví dụ nếu mã độc là một keylogger, phân tích động cho phép bạn xác định được log file trên hệ thống, tìm được nơi sẽ gửi thông tin đến... Những thông tin rõ ràng như vậy rất khó để thu được nếu chỉ sử dụng các kỹ thuật phân tích tĩnh.

#### 2.3.2.1. Phương pháp phân tích động mức cơ bản

Chạy mã độc và quan sát hành vi trên hệ thống để gỡ bỏ những tệp tin bị lây nhiễm. Tuy nhiên trước khi có thể chạy mã độc một cách an toàn cần phải xây dựng một môi trường sẽ cho phép chạy mã độc đó mà không làm ảnh hưởng đến hệ thống cũng như hạ tầng mạng (đã trình bày trong phần 3b). Giống như các kỹ thuật phân tích tĩnh cơ bản, các kỹ thuật phân tích động cơ bản có thể được tiến hành bởi hầu hết mọi người mà không cần hiểu biết sâu về lập trình.

#### 2.3.2.2. Phương pháp phân tích động mức nâng cao

Sử dụng một chương trình debugger để kiểm tra trạng thái của một mã độc đang thực thi. Phân tích động nâng cao cung cấp một cách khác để trích xuất thông tin chi tiết từ tệp tin thực thi. Những kỹ thuật phân tích này rất hữu dụng khi muốn

thu nhận những thông tin mà rất khó có thể lấy được bằng những kỹ thuật khác. Điển hình là các giải pháp phân tích trên Sandbox.

### 2.3.2.3. Công cụ hỗ trợ

**Process Explorer:** Công cụ cho phép xem danh sách các tiến trình dưới dạng cây của từng tiến trình và dịch vụ đang chạy dưới tiến trình nào. Hoặc các tiến trình được sinh ra từ tiến trình gốc.

**Process Moniter:** Chương trình này cho phép theo dõi các tiến trình sinh ra sẽ hoạt động như thế nào và có những tác động gì với hệ thống. Đây là công cụ rất mạnh với bộ lọc cơ động giúp chuyên viên phân tích dễ dàng xem xét việc thêm sửa xóa các tệp tin trên hệ thống.

**SysTracer:** Đây là công cụ cho phép chuyên viên phân tích có thể theo dõi hiện trạng của hệ thống, từ các tệp tin cho đến các giá trị trong regedit trước và sau khi khởi chạy mã độc.

**Các Sandbox:** Norman SandBox, GFI Sandbox, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis, Cuckoo Sandbox, Malwr... Sandbox có cơ chế bảo vệ để chạy những chương trình không tin cậy trên môi trường an toàn mà không cần lo sợ ảnh hưởng tới hệ thống thật. Những sandbox gồm có môi trường ảo thường mô phỏng những dịch vụ mạng thông thường để đảm bảo rằng phần mềm hoặc mã động được kiểm tra sẽ có hoạt động bình thường.

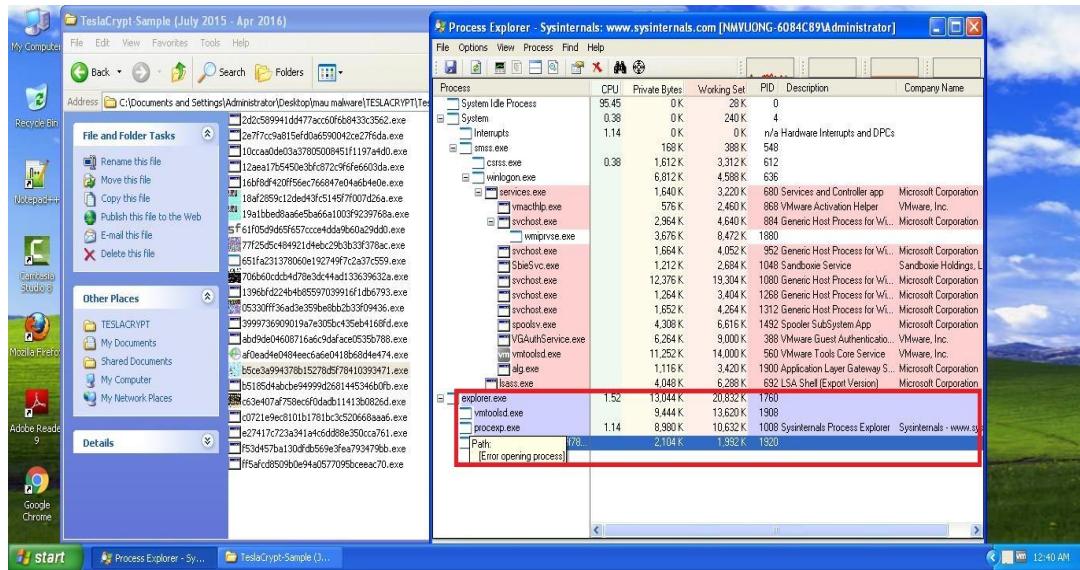
### 2.3.2.4. Thực nghiệm phân tích động mẫu mã độc Ransomware TeslaCrypt

Sử dụng các công cụ phân tích như đã trình bày tại mục 2.2.3 để thực hiện phân tích và thu thập hành vi [14] của mã độc mã hóa dữ liệu Ransomware TeslaCrypt.

#### a. Sử dụng công cụ Process Explorer

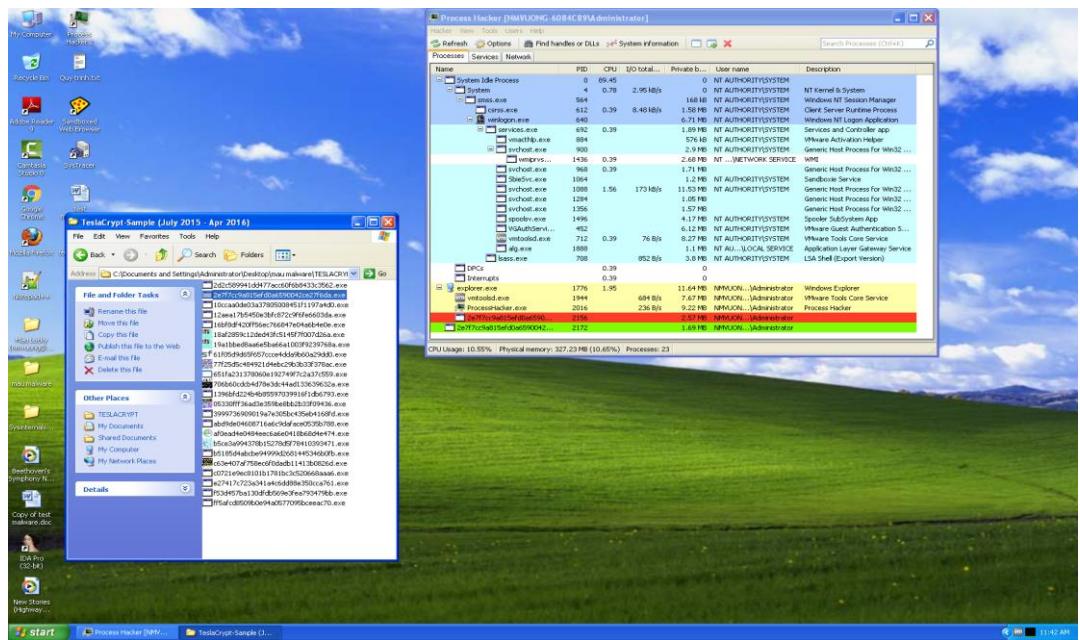
Sau khi khởi động tiến trình gốc ta thấy tiến trình đó tự nhân bản chính nó vào nhiều thư mục khác nhau và sinh ra thêm nhiều tiến trình khác. Đây được coi là một hành vi đáng nghi ngờ bởi thông thường khi các tiến trình chạy đa số chỉ gọi

các hàm hỗ trợ và các thư viện cần thiết để chạy, tuy nhiên trường hợp này mã độc tạo ra thêm tiến trình mới và trao quyền thực thi cho các tiến trình mới này.



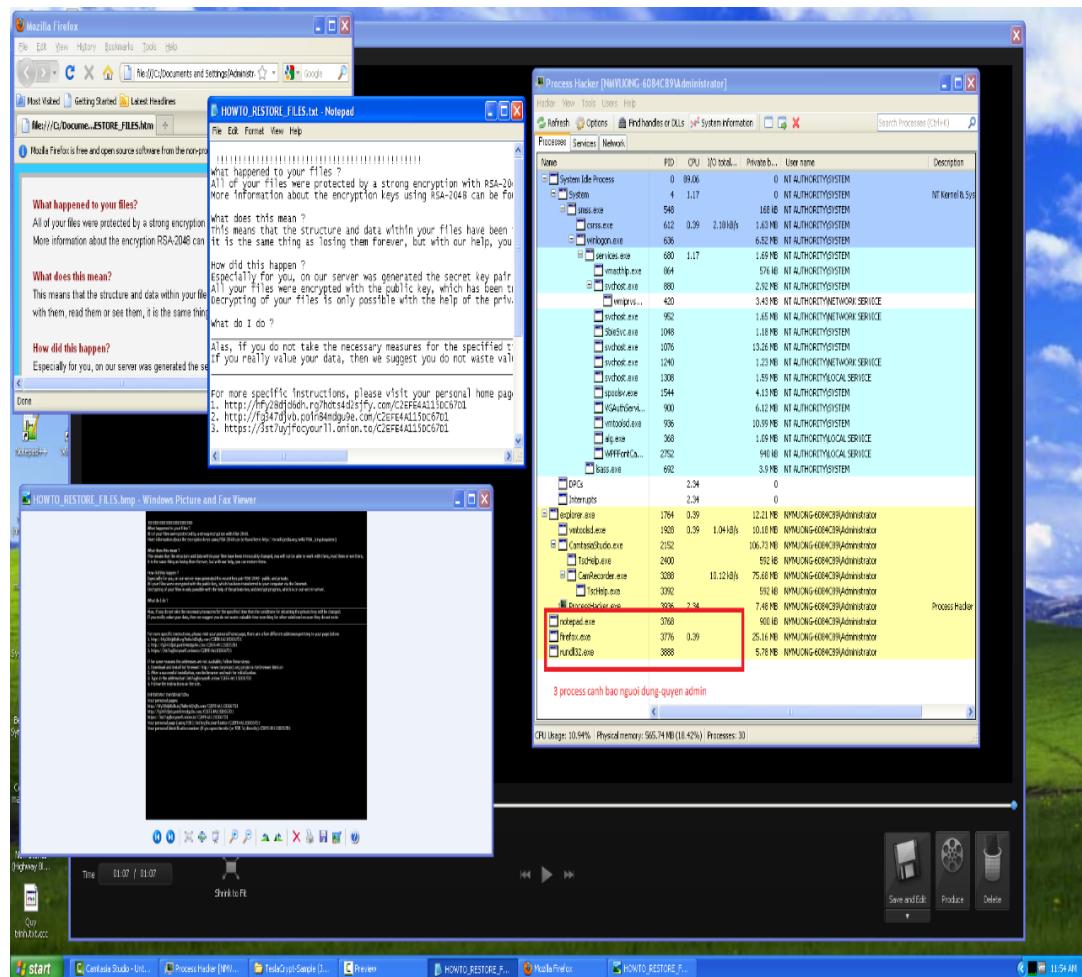
Hình 2.15: Phân tích mã độc bằng công cụ Process Monitor

Sử dụng phần mềm Process Hacker ta cũng thu được kết quả tương tự để kiểm chứng:



Hình 2.16: Kiểm chứng bằng Process Hacker

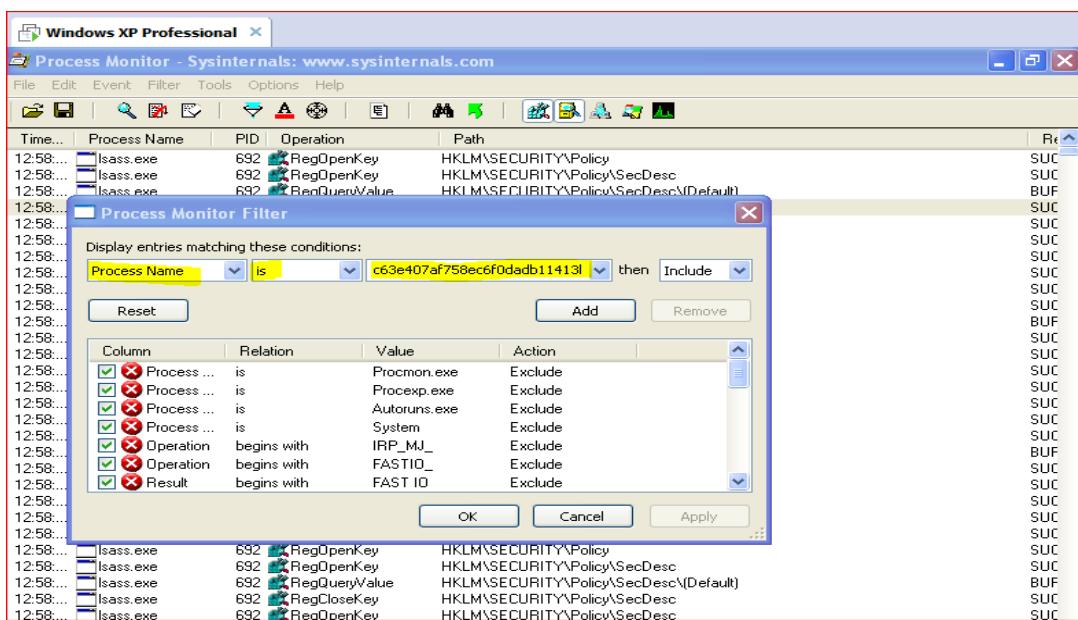
Chương trình mới được thực thi và thực hiện các hành vi lây nhiễm và mã hóa.



Hình 2.17: Thông báo đòn tiền chuột

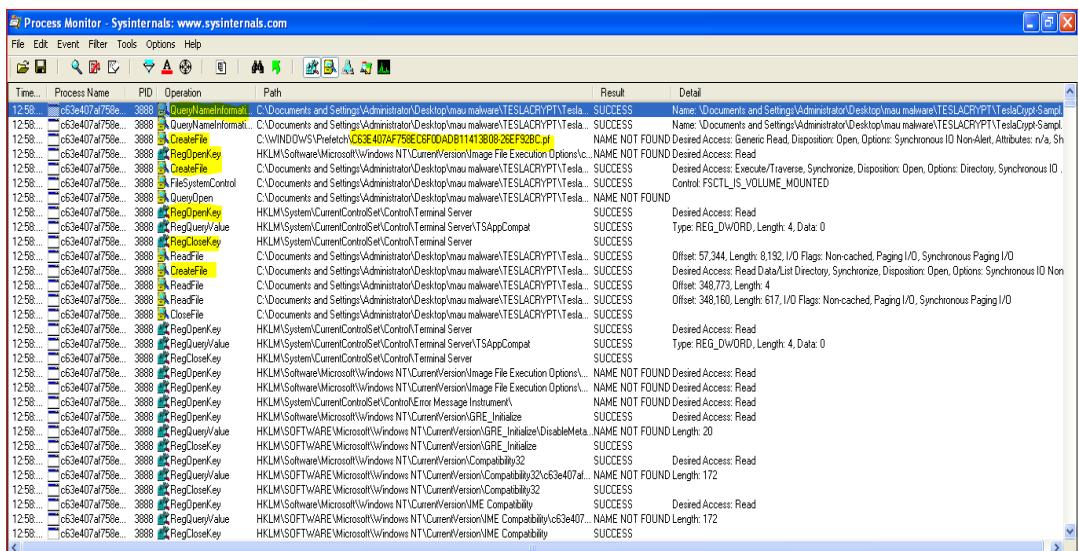
### b. Sử dụng công cụ Process Moniter

Để biết mã độc đã tạo thêm và xóa những file nào tôi thực hiện chạy chương trình Process Moniter và sử dụng bộ lọc với Process Name là tên của tệp tin thực thi mã độc thu được bảng giá trị create các tiến trình con như sau:



Hình 2.18: Sử dụng công cụ Process Monitor

Mã độc sẽ tự nhân bản mình vào các thư mục khác nhau, và thực hiện ghi danh bằng cách sửa các giá trị registry để đảm bảo quá trình lần khởi động sau cùng hệ thống và các tiến trình sẽ được thực thi.



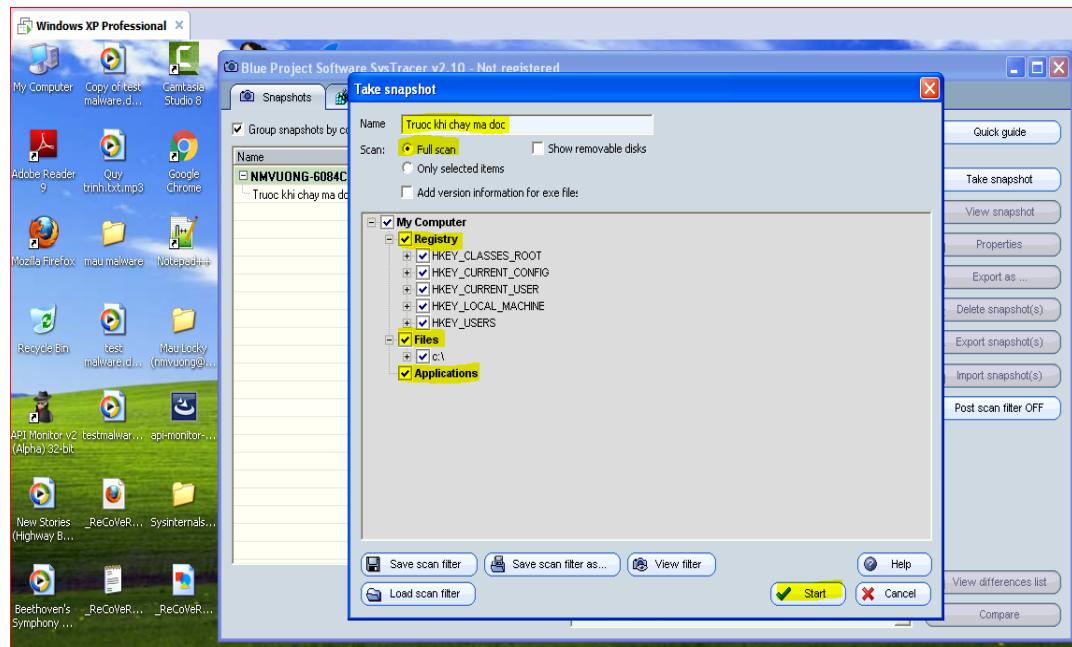
Hình 2.19: Sử dụng bộ lọc trong công cụ Process Monitor

Tiến trình con được tạo ra có tên random gồm 12 ký tự (tiến trình này sẽ có tên khác sau mỗi lần khởi chạy) trong trường hợp này tiến trình có tên “igiuleruyhnp.exe” được tiến trình gốc tạo ra và đóng vai trò là tiến trình chính sẽ

thực hiện gọi các thư viện, API, tiêm vào các tiến trình khác để thực hiện quá trình mã hóa các tệp tin trên máy nạn nhân.

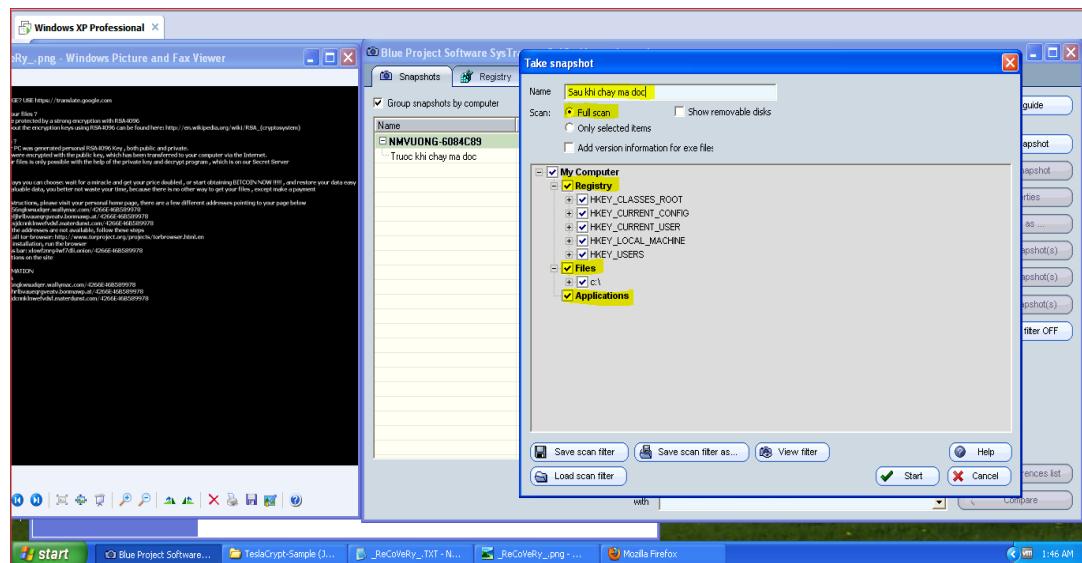
### c. Thực hiện kiểm tra các thay đổi giá trị của Registry

Sử dụng công cụ SysTracer để thực hiện kiểm tra các thay đổi giá trị registry trên máy nạn nhân. Đầu tiên ta sử dụng một bản lưu trạng thái registry sạch (trước khi chạy tệp tin mã độc).



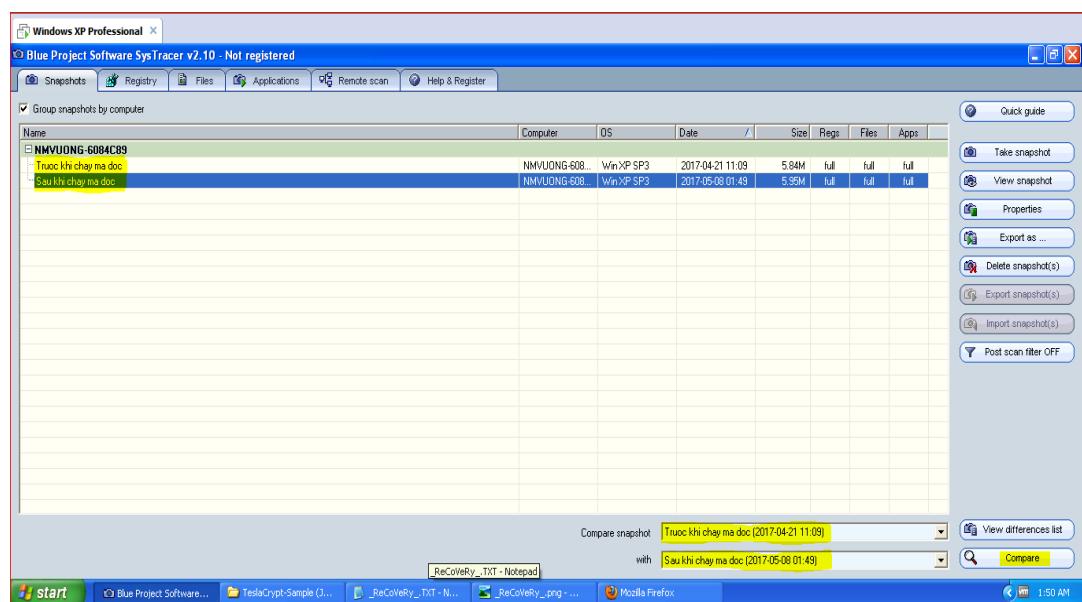
**Hình 2.20: Tạo bản Snapshot trạng thái hệ thống trước khi chạy**

Tiếp theo tiến hành thực hiện chạy mã độc và thu thập các giá trị registry đã bị thêm sửa xóa để kiểm tra hành vi của mã độc và thực hiện snapshot.



Hình 2.21: SysTracer Sau khi chạy mã độc

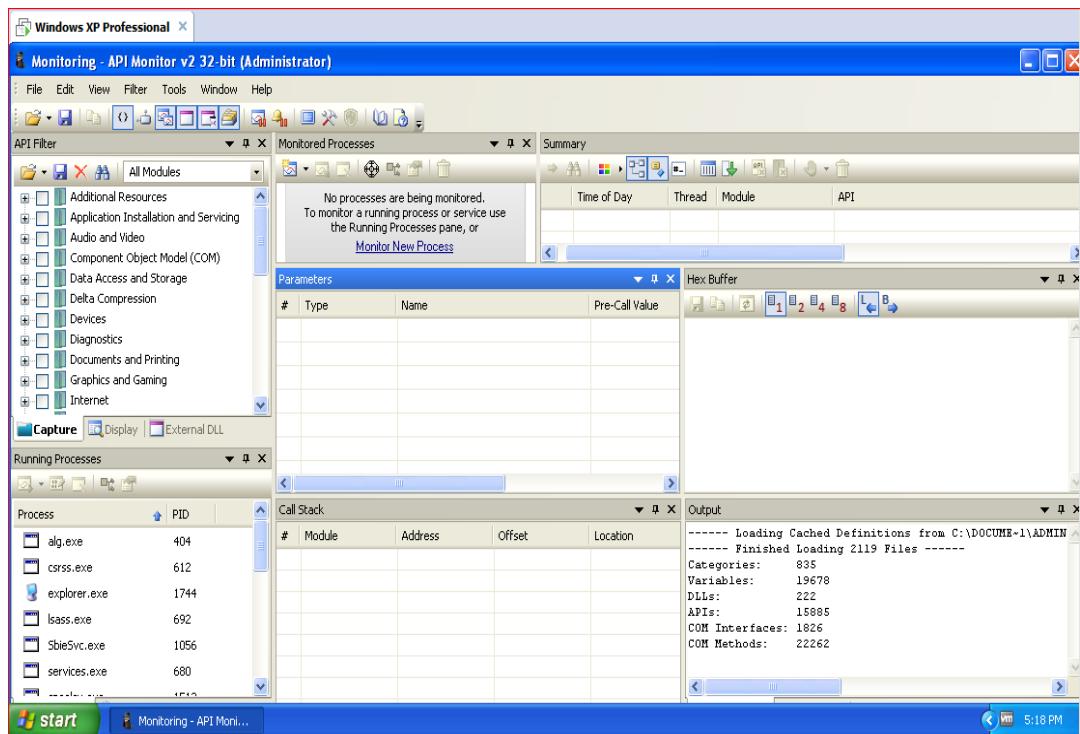
So sánh hai trạng thái:



Hình 2.22: So sánh 2 trạng thái trước và sau để thấy sự thay đổi giá trị hệ thống

Ta được kết quả những giá trị registry nào bị thay đổi và thay đổi do chương trình nào yêu cầu.

Sử dụng công cụ Monitor API để phát hiện những hàm và thư viện mà mã độc gọi trong quá trình chạy



Hình 2.23: Công cụ Moniter các API

### 2.3.2.5. Đánh giá

#### a. Ưu điểm phương pháp phân tích động

Quá trình phân tích diễn ra nhanh hơn, dễ dàng hơn. Các hành vi được ghi lại một cách rõ ràng, người phân tích không quá quan trọng về kiến thức chuyên gia trong lĩnh vực dịch ngược. Đối với công nghệ phân tích động không phải hành vi nào cũng phân tích được, đơn cử như những loại virus phát hiện ra công cụ phân tích thì nó sẽ không hoạt động nữa, hoặc virus chờ đến một lúc nào đó mới hoạt động. Chính vì điều này dẫn đến có thể bỏ qua một số hành vi quan trọng khi mã độc sử dụng kỹ thuật phát hiện môi trường máy ảo và ngẫu nhiên. Tuy nhiên với sự phát triển của công nghệ các vấn đề này gần như được khắc phục với kỹ thuật giả lập CPU, kích hoạt thời gian chạy chống ngủ đông của mã độc.

#### b. Nhược điểm phương pháp phân tích động

Quá trình phân tích động vẫn có khả năng bỏ sót một số hành vi khi mã độc sử dụng các kỹ thuật có yêu cầu đầu vào cụ thể mà môi trường phân tích không cung cấp tự động được. Mặt khác việc phân tích động đòi hỏi sử dụng nhiều công

cụ kết hợp và quan trọng nhất là môi trường để thực hiện phân tích. Nếu môi trường thực hiện phân tích không đạt chuẩn sẽ dẫn đến những sai lệch hành vi của mã độc. Tuy nhiên vẫn trong phạm vi phân tích động hiện tại một số công nghệ phân tích động dựa trên Sandbox có khả năng giải quyết bài toán này.

## **2.4. Phân tích lựa chọn công cụ, phương pháp xây dựng giải pháp phân tích hành vi mã độc Ransomware**

Phương pháp phân tích tĩnh có khả năng thu thập được nhiều hoạt động của mã độc tuy nhiên gặp nhiều khó khăn với yêu cầu lượng kiến thức chuyên gia lớn và thời gian phân tích rất lâu. Để có thể nhanh chóng theo dõi và thu thập được hành vi hoạt động của mã độc chúng ta có thể sử dụng phương pháp phân tích động cho những kết quả nhanh chóng và không cần quá phụ thuộc vào kiến thức chuyên gia. Cụ thể như mẫu mã độc Tesla phân tích trong mục 2.3.2.4 được sử dụng một thuật toán sinh ngẫu nhiên tên tiến trình con với độ dài là 12 ký tự trong bảng chữ cái và các số từ 0 đến 9. Như vậy nếu phân tích tĩnh để xác định phần mềm độc hại và lấy chữ ký để thêm vào các cơ sở dữ liệu của phần mềm antivirrut thì hoàn toàn không phù hợp khi mỗi lần chạy khác nhau (trên cùng máy hoặc khác máy) nó đều có tên tiến trình con khác nhau dẫn đến các chữ ký sẽ không còn chính xác. Tuy nhiên với cách nhìn của phân tích động người phân tích không cần quan tâm đến quá nhiều về thuật toán sinh tên ngẫu nhiên hoặc chữ ký của chương trình mã độc, mà chỉ cần chú trọng đến hành vi cụ thể ở đây là hành vi thực hiện việc tự động sinh các chương trình thực thi con, tức là sử dụng quyền “create” để tạo các tiến trình con khác.

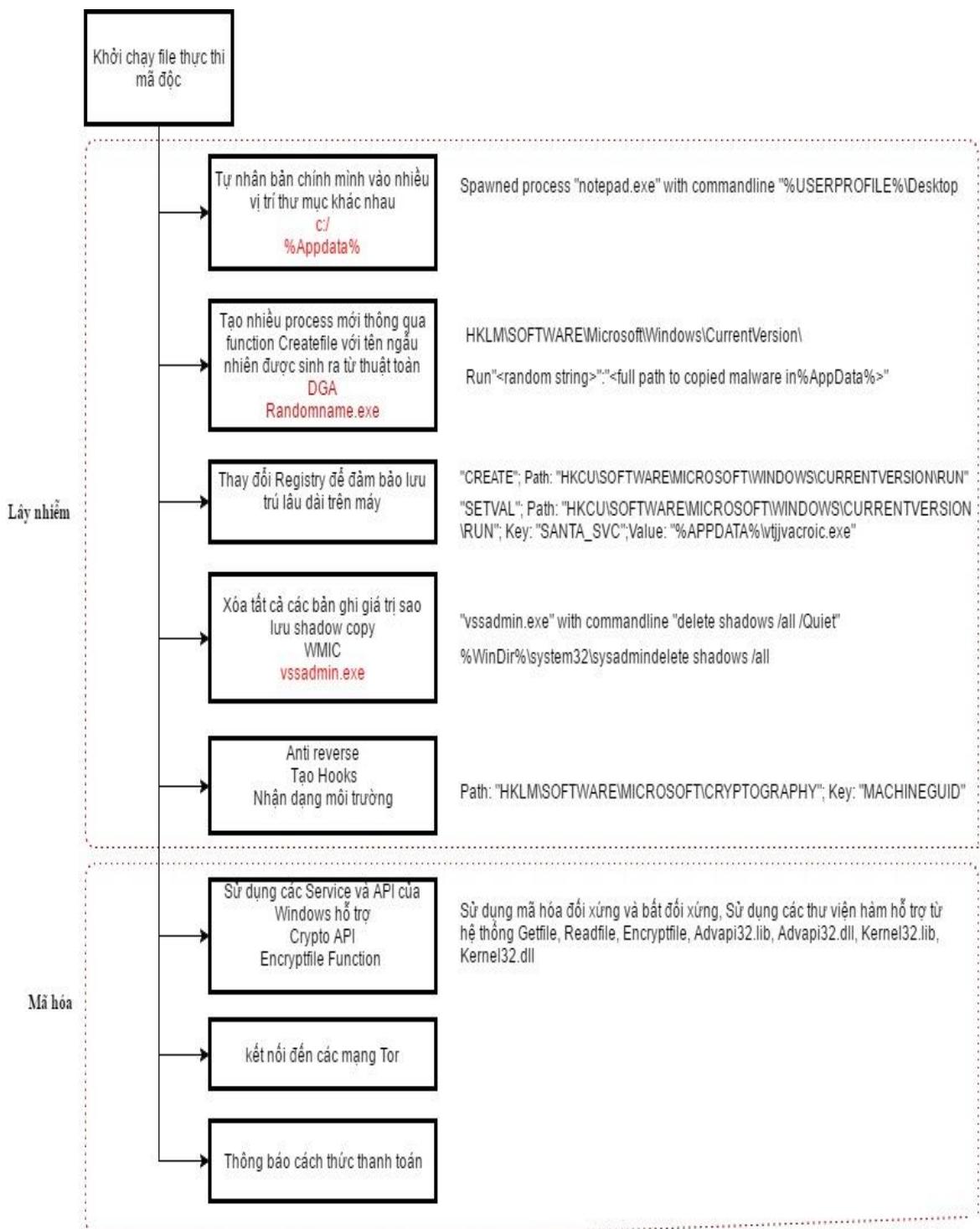
**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"<random string>":"<full path to copied malware in %AppData%>"**

Ngoài việc tạo tiến trình con khác, mã độc còn thực hiện gọi chương trình CMD để thực hiện các câu lệnh điều khiển hệ thống. Trong trường hợp này người phân tích chỉ cần quan tâm đến hành vi khi thực hiện câu lệnh đó là gọi đến dịch vụ (service) WMIC.exe và vssadmin.exe đây là service dùng để thay đổi hoặc xóa tệp

tin shadow nơi lưu trữ bản backup của các tệp tin. Hành vi xóa này nhằm mục đích nạn nhân không còn khả năng khôi phục được tệp tin gốc sau khi bị mã hóa.

**%WinDir%\system32\sysadmin delete shadows /all**

Qua việc phân tích có thể chia quá trình thực hiện mã hóa dữ liệu nạn nhân thành hai quá trình đó là lây nhiễm và mã hóa, hai quá trình này tương ứng với các hành vi và được mô tả cụ thể trong mô hình:



**Hình 2.24: Mô hình hành vi**

Tuy nhiên việc phân tích động thủ công bằng các công cụ như luận văn đã thực hiện ở phần trên cho thấy số lượng công cụ phải sử dụng rất nhiều, sẽ rất khó khi phân tích với số lượng biến thể lớn, bên cạnh đó người phân tích gặp nhiều khó

khăn trong việc lưu trữ kết quả khi thu thập những hành vi của mã độc. Để giải quyết bài toán này luận văn đề xuất một phương pháp phân tích hành vi tổng hợp nhằm phát hiện mã độc bằng kỹ thuật theo dõi hành vi kết hợp với kỹ thuật phân tích Heuristic. Công nghệ Sandbox là phù hợp với thực tiễn và hiện tại công nghệ Sandbox đang có rất nhiều những bước tiên tiến trong việc phân tích hành vi mã độc, giúp đỡ các chuyên viên và chuyên gia trong lĩnh vực phân tích thu thập hành vi của các chương trình thực thi. Sandbox tạo ra môi trường cách ly những phần mềm ứng dụng chạy bên trong để đảm bảo nó sẽ không ảnh hưởng đến bên ngoài. Hiện tại thế giới đang có một số các công nghệ Sandbox được đánh giá cao như: Sandbox Cuckoo, Joe Sandbox, VxStream Sandbox...

Trong luận văn này sử dụng VxStream Sandbox. VxStream Sandbox [17] là một hệ thống quy mô lớn xử lý hàng trăm nghìn tệp tin tự động, và có thể hoạt động như một dịch vụ web để phân tích phản lại ứng sự cố. Giao diện đơn giản và khả năng tích hợp với rất nhiều nhà cung cấp công nghệ khác, nó giúp đầy đủ thông tin hơn cho một SOCs ứng phó sự cố bảo mật. VxStream Sandbox hiện đang được sử dụng bởi các nhóm SOCs, CERTs, DFIR, các phòng thí nghiệm pháp lý an ninh công nghệ thông tin, các nhà nghiên cứu và các nhà cung cấp dịch vụ tình báo về các mối đe dọa từ mã độc trên khắp thế giới. Nhiều tổ chức và các cơ quan chính phủ Hoa Kỳ đang sử dụng Vbox Sandbox. Nếu sử dụng phiên bản đầy đủ của VxStream sẽ được hỗ trợ rất nhiều như: Các API, thời gian chạy, bộ điều khiển cân bằng tải, công nghệ phân tích, báo cáo, các chỉ số bất thường, các chữ ký và kịch bản... Sandbox này hỗ trợ phân tích rất nhiều định dạng tệp tin PE (.exe, .scr, .pif, .dll, .com, .cpl, etc.), Office (.doc, .docx, .ppt, .pptx, .xls, .xlsx, .rtf, .pub), PDF, APK, executable JAR, Windows Shortcut (.lnk), Windows Help (.chm), HTML Application (.hta), Windows Script File (\*.wsf), Javascript (.js), Visual Basic (\*.vbs, \*.vbe), Shockwave Flash (.swf), Powershell (.ps1, .psd1, .psm1), Scalable Vector Graphics (.svg), MIME RFC 822 (\*.eml) and Outlook \*.msg files. Tuy nhiên trong giới hạn bài luận văn sử dụng sản phẩm VxStream Sandbox ở dạng tài khoản miễn phí để phân tích hành vi của mã độc một cách tự động. Muốn sử dụng

các tiện ích mở rộng của VxStream người dùng cần trả khoảng 128 Euro để được nâng cấp quyền cho tài khoản.

## 2.5. Kết luận chương

Môi trường phân tích là yếu tố rất quan trọng, ảnh hưởng trực tiếp đến kết quả phân tích chính vì vậy cần lựa chọn và thiết lập môi trường ổn định và phù hợp với mục tiêu phân tích. Ngoài ra việc lựa chọn kỹ thuật phân tích và công cụ cũng cần được phân tích kỹ để thấy những điểm mạnh và điểm yếu của từng công cụ. Việc lựa chọn những công cụ đơn giản dễ sử dụng được ưu tiên để giải quyết nhu cầu cần phân tích nhanh mà thu thập được các hành vi, các lệnh gọi hàm hệ thống. Sau khi phân tích điểm mạnh yếu các phương pháp phân tích luận văn đã thực nghiệm phân tích bằng phương pháp phân tích động để lựa chọn ra một số các hành vi đặc trưng. Chương tiếp theo luận văn sẽ tiến hành xây dựng một chương trình có khả năng phát hiện mã độc mã hóa dữ liệu dựa trên hành vi đã thu thập được.

## Chương 3: XÂY DỰNG VÀ THỬ NGHIỆM GIẢI PHÁP PHÁT HIỆN RANSOMWARE

### 3.1. Kiến trúc và các thành phần của giải pháp

#### 3.1.1. Ý tưởng đề xuất

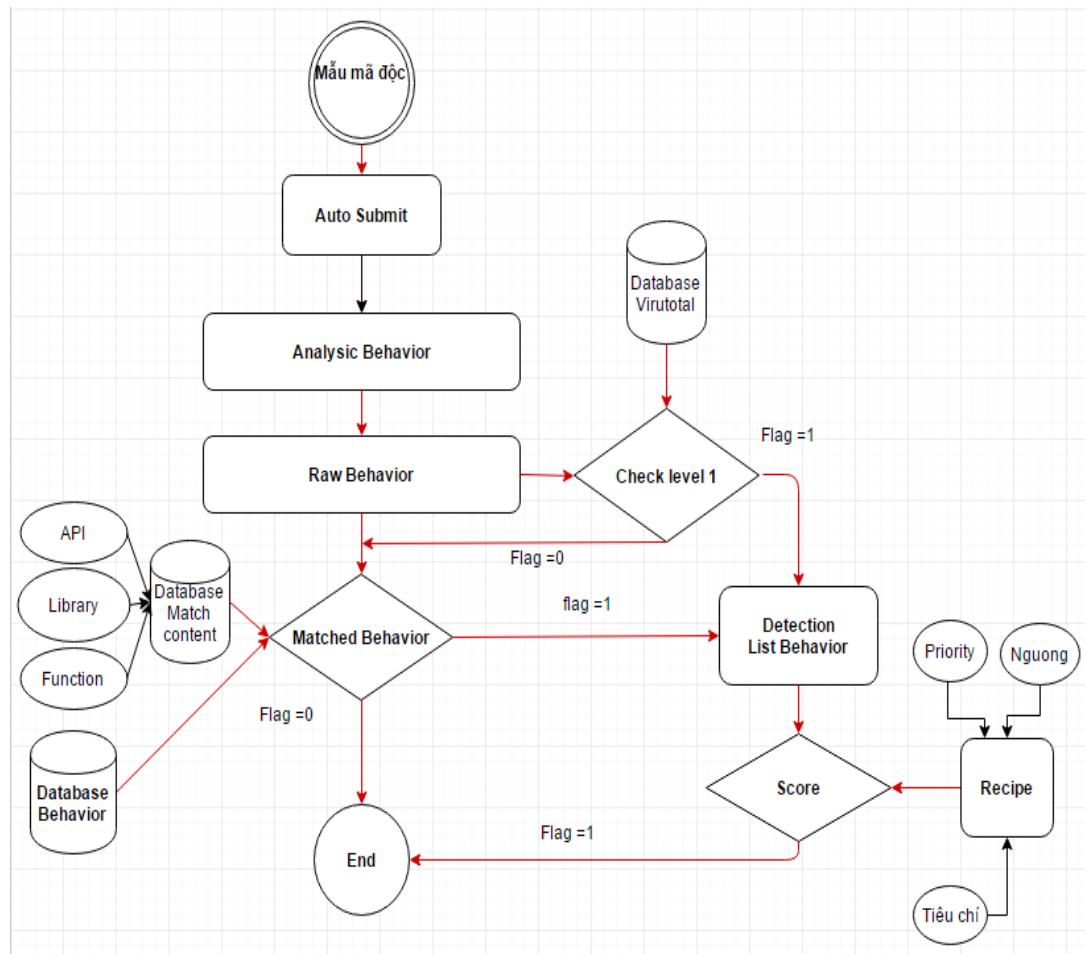
Qua việc phân tích một số mẫu mã độc điển hình trong Chương 2 của luận văn cho thấy mã độc Ransomware được thiết kế rất tinh vi và có nhiều kỹ thuật nhằm vượt qua các phần mềm phát hiện và phòng chống mã độc. Điểm hình như kỹ thuật làm rối mã, kỹ thuật chống phân tích, kỹ thuật khai thác lỗ hổng trên hệ điều hành, kỹ thuật rẽ nhánh... Trong khi đó các giải pháp phát hiện đều đang có những điểm yếu nhất định. Kỹ thuật heuristic có thể giúp phát hiện ra được các hàm và thư viện có khả năng được sử dụng bởi mã độc. Tuy nhiên điểm bất cập của nó là trong các trường hợp khác nhau thì việc gọi hàm cũng có mục đích khác nhau, không phải tất cả đều là mục đích phá hoại. Kỹ thuật phát hiện dựa trên hành vi có phần chính xác hơn tuy nhiên không phải hành vi nào của mã độc cũng được thể hiện rõ ràng khi hoạt động. Kỹ thuật sử dụng chữ ký tuy không phát hiện được biến thể mới nhưng chúng vẫn nên được sử dụng để phát hiện sớm trong các cuộc tấn công sau và làm giàu thông tin cơ sở dữ liệu. Với những ưu nhược điểm của các kỹ thuật phát hiện mã độc cùng với những kỹ thuật che dấu sẵn có dẫn đến việc phát hiện chính xác mã độc và không bị cảnh báo sai là nhu cầu cần thiết. Xuất phát từ quá trình nghiên cứu tìm hiểu này luận văn đề xuất xây dựng một giải pháp kết hợp giữa các kỹ thuật phát hiện nêu trên nhằm mục đích phát hiện sớm mã độc mã hóa dữ liệu Ransomware.

#### 3.1.2. Kiến trúc và các thành phần chương trình

Chương trình gồm 2 module, module 1 và module 2. Module 1 có chức năng tải (upload) mã độc vào môi trường giả lập để tiến hành phân tích và lấy dữ liệu về hành vi của mã độc, sau đây gọi là module chuyển đổi tập dữ liệu mẫu (Module tiền xử lý). Module 2: ngoài chức năng phân tích các hành vi và sử dụng CSDL hành vi

mẫu để phát hiện mã độc, module này còn tích hợp chức năng tính điểm đánh giá mức độ nguy hiểm và thống kê.

Sơ đồ kiến trúc tổng thể của chương trình như sau:



### Hình 3.1: Kiến trúc chương trình

Kiến trúc chương trình được chia làm hai thành phần chính là: Thành phần xử lý dữ liệu và thành phần phát hiện mã độc.

## Thành phần xử lý dữ liệu

Đầu vào là các tệp tin thực thi chưa mã độc và được tiến hành phân tích thông qua Sandbox, các hành vi thu thập được ở dạng thô sẽ được xử lý thông qua việc so khớp với một số hành vi đặc trưng đã được phân tích, thu thập trước đó. Chi tiết được mô tả bên dưới.

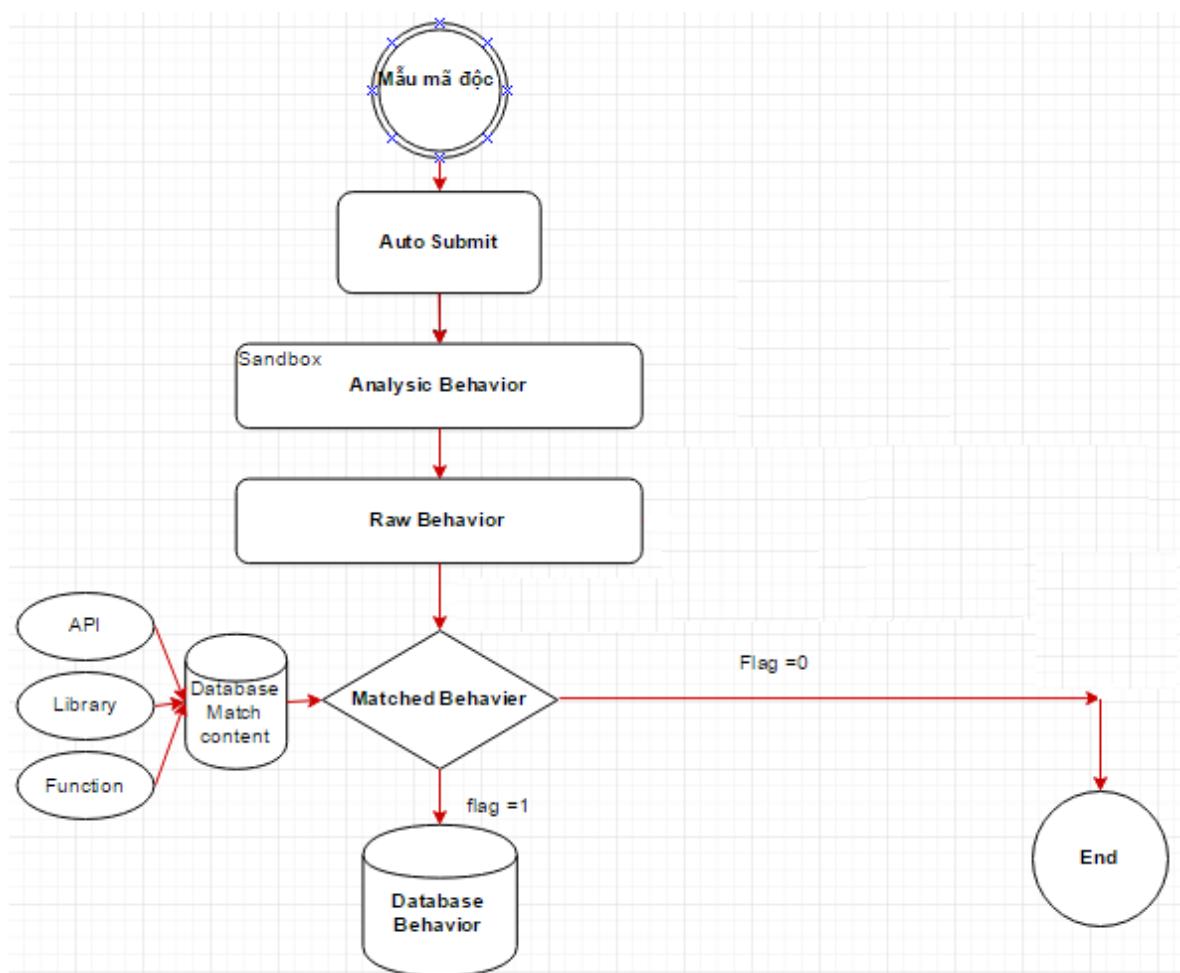
## Thành phần phát hiện mã độc

Đây là thành phần quan trọng nhất của hệ thống, ngoài việc xử lý các hành vi thu thập được như đã nói trong phần trên, thành phần này còn có thêm phần tính toán điểm được áp dụng công thức tính điểm cũng như đưa ra được kết luận về tệp tin được phân tích và đưa ra thông kê báo cáo. Chi tiết được trình bày bên dưới.

### 3.1.3. Các Module chương trình

#### a. Xây dựng module xử lý dữ liệu

Module chuyển đổi tập dữ liệu (tiền xử lý) có chức năng thực hiện thu thập các hành vi của mã độc sau khi chạy phân tích động. Đầu ra của module là bảng CSDL các hành vi của các mẫu và biến thể.

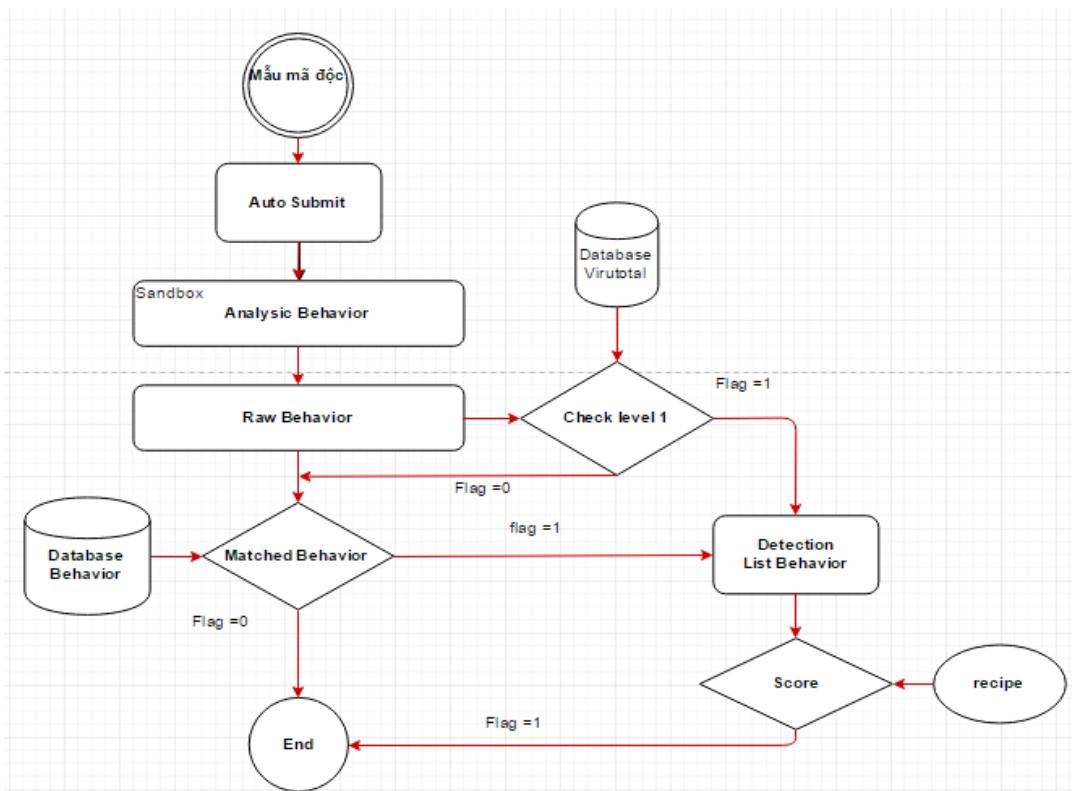


Hình 3.2: Xử lý dữ liệu

## b. Xây dựng module phát hiện mã độc

Module phát hiện mã độc với khả năng chính là phát hiện mã độc nó còn có chức năng cập nhật hành vi vào database, tính điểm để đưa ra kết luận và thống kê số liệu khi cần.

Công thức tính điểm được mô tả như sau:



Hình 3.3: Module phát hiện mã độc

### Tính điểm đánh giá mức độ nguy hiểm

Chương trình tham khảo cách tính điểm theo nghiên cứu của Robert J. Bagnall và Geoffrey French: “The Malware Rating System (MRS)TM” [15] theo các nội dung sau.

- Tiêu chí đánh giá phần mềm độc hại.
- Các ngưỡng để xuất xác định xếp hạng hành vi.
- Xếp hạng cho phần mềm độc hại.

Các căn cứ để tính điểm đánh giá gồm:

- Căn cứ vào hành vi của mã độc được đánh giá là nguy hiểm theo mức độ ảnh hưởng vào hệ thống.
- Căn cứ vào các kỹ thuật được sử dụng để xác định mức độ ưu tiên của hành vi (priority).

Table 3: Tiêu chí đánh giá phần mềm độc hại

Bảng 3: Tiêu chí đánh giá phần mềm độc hại	
Tiêu chí	Mô tả
Tải trọng tiềm ẩn	Tải trọng tiềm ẩn của module có thể làm suy giảm hoặc làm hỏng mục tiêu
Tiềm năng phát triển	Sự nhanh chóng hoặc dễ dàng để các mã có thể chạy trên hệ thống
Mức độ nguy hại	Mục tiêu ẩn chứa trong payload

Table 4: Các ngưỡng xếp loại Payload

Bảng 4: Đề nghị các ngưỡng xác định xếp loại Payload	
Rating	Mô tả
10	Đa hình, chưa xác định trước
9	Xóa các tập tin cần thiết, lây nhiễm mạng; có thể sụp đổ một mạng do làm tràn băng thông
8	Xóa, sửa đổi hoặc ghi đè lên các tệp tin thiết yếu và lây nhiễm mạng
7	Sửa đổi hoặc ghi đè lên các tập tin không cần thiết, lây nhiễm mạng; Tràn dung lượng băng thông
6	Xóa các tập tin không cần thiết, lây nhiễm mạng
5	Xóa các tệp tin không cần thiết
4	Làm tràn băng thông mạng

3	Lây nhiễm các tệp tin cần thiết
2	Lây nhiễm các tệp tin không cần thiết
1	Không có ảnh hưởng lâu dài

Table 5: Phân loại mức độ nguy hiểm theo điểm

Bảng 5: Phân loại điểm theo mức độ nguy hiểm		
Điểm	Phân loại	Mô tả mức độ nguy hiểm
0-20	1	Tối thiểu
21-40	2	Thấp
41-60	3	Nguy hiểm
61-80	4	Rất nguy hiểm
81-100	5	Thảm họa

### Tính mức ưu tiên (Priority) khi đánh giá các hành vi

Luận văn đưa ra cách sắp xếp các hành vi theo mức độ ưu tiên và cách tính điểm đánh giá như sau. Bảng 6 có 8 hành vi đặc trưng của mã độc Ransomware và có tổng điểm ưu tiên là 36 điểm.

Table 6: Tính mức ưu tiên (Priority) khi đánh giá các hành vi

Bảng 6: Mức độ ưu tiên theo hành vi và điểm ưu tiên			
Số TT	Hành Vi	priority	score
Behavior 1	Create new process	1	1/36
Behavior 2	Modifie Regedit	2	2/36
Behavior 3	Creates mutants	4	4/36
Behavior 4	Delete Shadow	5	5/36
Behavior 5	Anti Environment	3	3/36
Behavior 6	Call API Crypt	7	7/36

Bảng 6: Mức độ ưu tiên theo hành vi và điểm ưu tiên

Số TT	Hành Vi	priority	score
Behavior 7	Alert	8	8/36
Behavior 8	Connect TOR or BL Network or GET POST	6	6/36

### Công thức tính điểm đánh giá hành vi

Điểm được tính bằng trung bình điểm của các hành vi tương ứng với mức độ ảnh hưởng và được cụ thể hóa bằng điểm ưu tiên (priority). Số lượng các hành vi và tổng các giá trị ưu tiên (priority) sẽ được tính làm trung bình cho điểm với mỗi mẫu mã độc như sau.

$$Score = \sum_{i=1}^n (W_i) * 100 \quad (1)$$

Với

$$W_i = \frac{P_{HV_i}}{\sum_{i=1}^n P_{HV_i}} \quad (2)$$

Trong đó:

$P_{HV_i}$ : Mức độ ưu tiên tính theo bảng priority

$W_i$ : Điểm trung bình tính theo tổng số các hành vi

Ví dụ cách tính điểm:

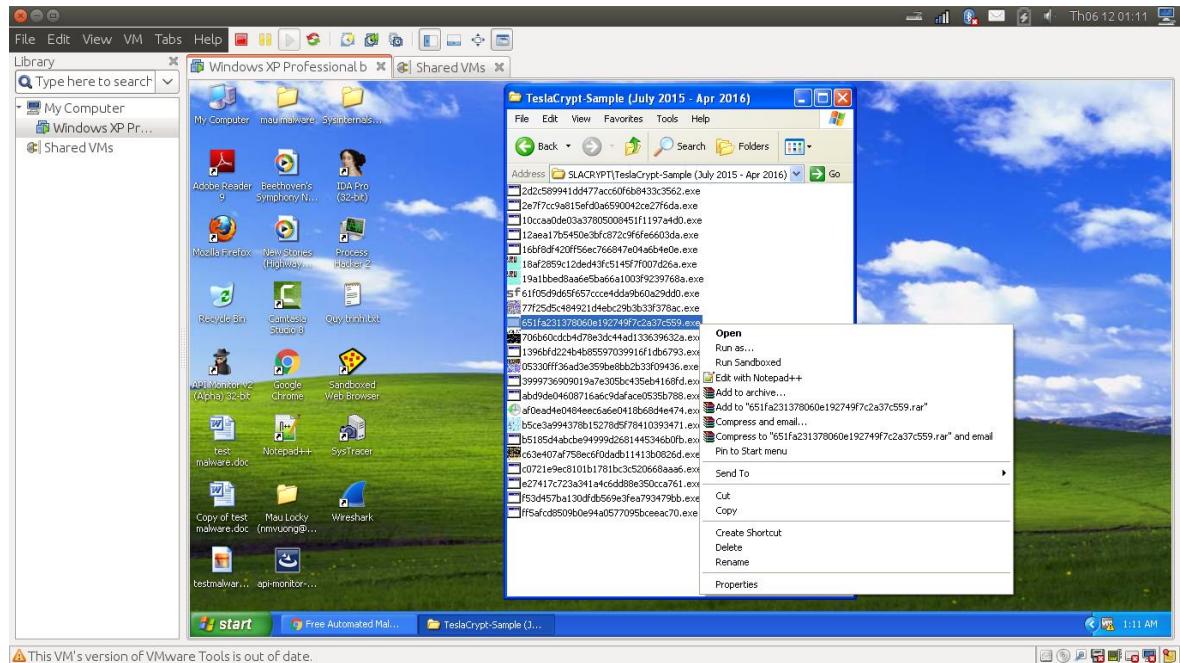
Giả sử mẫu mã độc “A” có các hành vi 1, 3, 6 và 7 tương ứng với Create new process (Score = 1/36), Creates mutants (Score = 4/36), Call API Crypt (Score = 7/36) và Alert (Score = 8/36). Vậy tổng điểm hành vi của mã độc “A” là 20/36 tương ứng với số điểm thực tế là 55.5 điểm.

## 3.2. Thủ nghiệm giải pháp

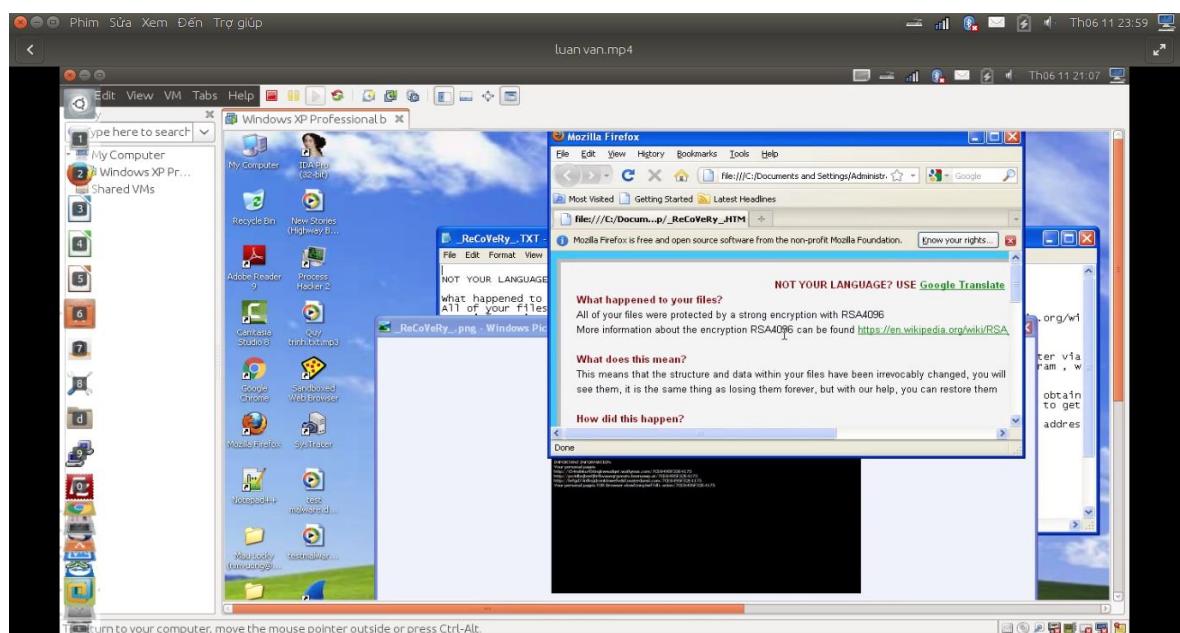
### 3.2.1. Kịch bản thử nghiệm 1

Thực hiện phân tích 1 mẫu mã độc cùng họ TestlaCrypt đã biết

**Pha 1:** Thực hiện chạy 1 mẫu trên máy ảo để xem quá trình mã hóa file trên máy ảo và quan sát kết quả. Máy ảo được cài đặt trên hệ điều hành Vmware phiên bản 12.0, trên máy ảo được cài đặt một số phần mềm hỗ trợ cần thiết gồm: phần mềm adobe, firefox ver39.x, python2.7 library, office 2003, netframework 2.x...

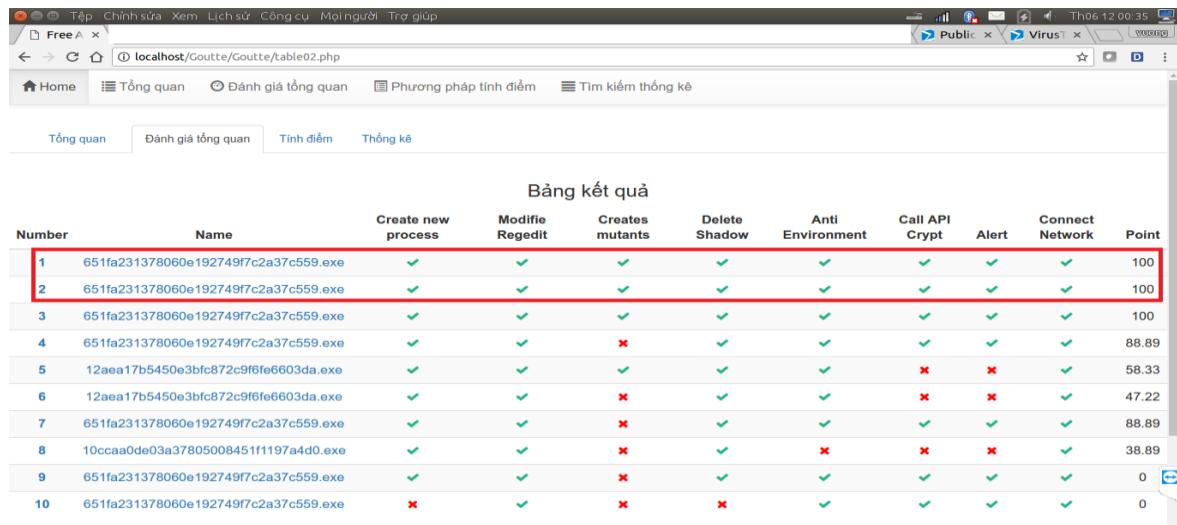


Hình 3.4: Chạy mã độc TeslaCrypt



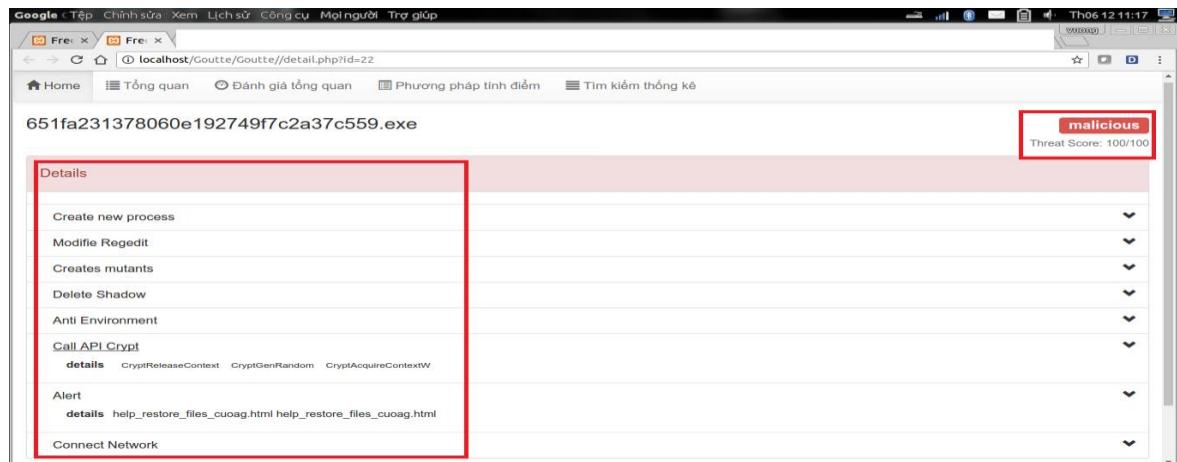
Hình 3.5: Dữ liệu bị mã hóa và thông báo đòi tiền chuộc

**Pha 2:** Thực hiện phân tích hành vi của mẫu mã độc thông qua sandbox, dữ liệu đầu ra sẽ được module phát hiện mã độc sẽ tiến hành phân tích hành vi và đưa ra điểm số tương ứng với các hành vi đã thu thập được là cơ sở để kết luận tệp tin thực thi là mã độc Ransomware.



Number	Name	Create new process	Modify Regedit	Creates mutants	Delete Shadow	Anti Environment	Call API Crypt	Alert	Connect Network	Point
1	651fa231378060e192749f7c2a37c559.exe	✓	✓	✓	✓	✓	✓	✓	✓	100
2	651fa231378060e192749f7c2a37c559.exe	✓	✓	✓	✓	✓	✓	✓	✓	100
3	651fa231378060e192749f7c2a37c559.exe	✓	✓	✓	✓	✓	✓	✓	✓	100
4	651fa231378060e192749f7c2a37c559.exe	✓	✓	✗	✓	✓	✓	✓	✓	88.89
5	12aea17b5450e3bfc872c9f6fe6603da.exe	✓	✓	✓	✓	✓	✗	✗	✓	58.33
6	12aea17b5450e3bfc872c9f6fe6603da.exe	✓	✓	✗	✓	✓	✗	✗	✓	47.22
7	651fa231378060e192749f7c2a37c559.exe	✓	✓	✗	✓	✓	✓	✓	✓	88.89
8	10ccaa0de03aa37805008451f1197a4d0.exe	✓	✓	✗	✓	✗	✗	✗	✓	38.89
9	651fa231378060e192749f7c2a37c559.exe	✓	✓	✗	✓	✓	✓	✓	✓	0
10	651fa231378060e192749f7c2a37c559.exe	✗	✓	✗	✗	✓	✓	✓	✓	0

Hình 3.6: Chương trình phát hiện mã độc



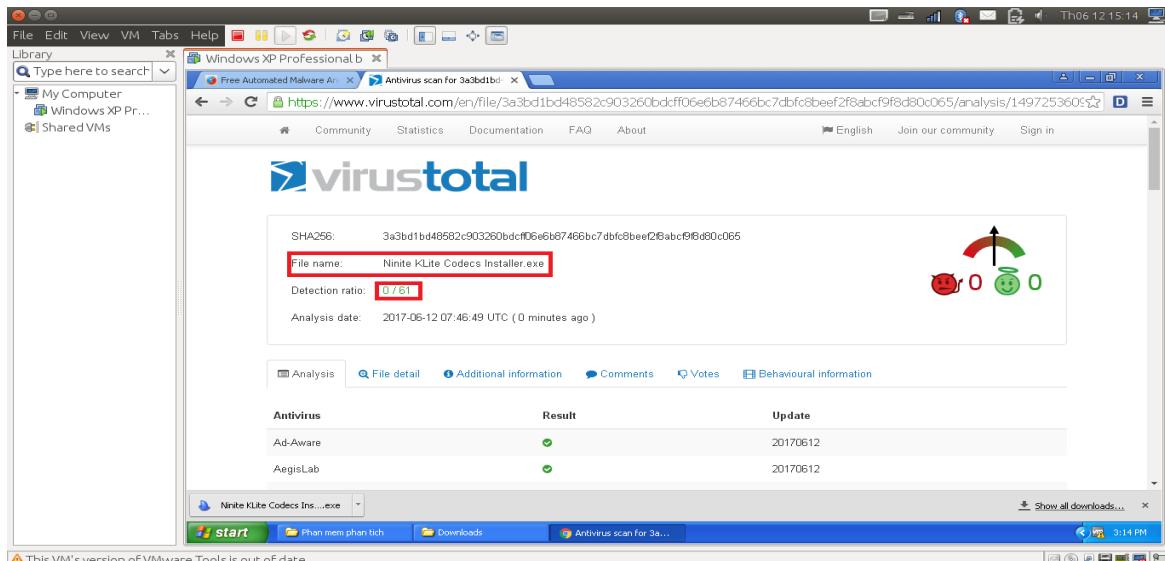
Details
Create new process
Modify Regedit
Creates mutants
Delete Shadow
Anti Environment
Call API Crypt
details CryptReleaseContext CryptGenRandom CryptAcquireContextW
Alert
details help_restore_files_cuaoag.html help_restore_files_cuaoag.html
Connect Network

Hình 3.7: Liệt kê các hành vi nguy hiểm

### 3.2.2. Kịch bản thử nghiệm 2

Thực hiện kiểm tra một tệp tin cài đặt có đuôi mở rộng .exe sạch được tải từ trang chủ <https://ninite.com/> (đây là chuyên trang cung cấp các phần mềm sạch được cộng đồng thế giới đánh giá cao và sử dụng) có tên là: “Ninite KLite Codecs Installer.exe”.

**Pha 1:** Thực hiện chạy mẫu “Ninite KLite Codecs Installer.exe” trên chuyên trang phân tích virustotal cho kết quả đánh giá 0/60. Ý nghĩa của giá trị 0/60 thể hiện tập tin được quét bằng 60 phần mềm phát hiện mã độc và 0 phần mềm không phát hiện mã độc.

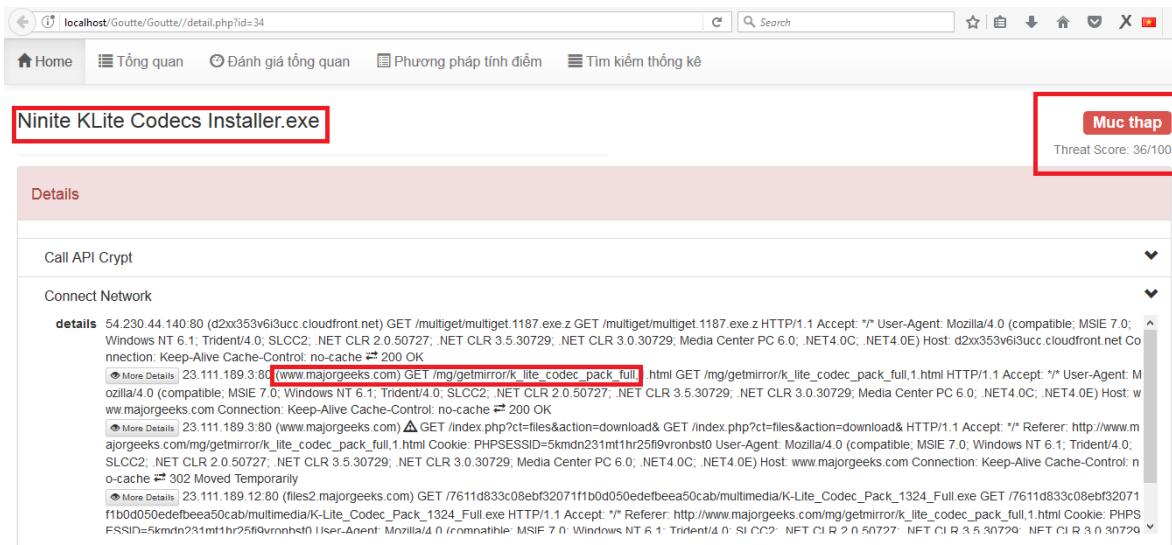


Hình 3.8: Thử nghiệm quét tệp tin trên virustotal

**Pha 2:** Chạy tệp tin thực thi “Ninite KLite Codecs Installer.exe” [21] trong môi trường Sandbox và chạy qua giải pháp phát hiện mã độc mã hóa dữ liệu Ransomware. Sau khi được đánh giá các hành vi mà phần mềm tác động lên hệ thống với phương pháp tính điểm của chương trình phát hiện mã độc Ransomware. Số điểm đánh giá phần mềm là 36.11.

Number	Name	Create new process	Modifies Registry	Creates mutants	Delete Shadow	Anti Environment	Call API Crypt	Alert	Connect Network	Point
1	Ninite KLite Codecs Installer.exe	✗	✗	✗	✗	✗	✓	✗	✓	36.11
2	1D3DE3D1.vXE	✗	✗	✗	✗	✗	✓	✗	✗	19.44
3	651fa231378060e192749f7c2a37c559.exe	✓	✓	✓	✓	✓	✓	✓	✓	100
4	651fa231378060e192749f7c2a37c559.exe	✓	✓	✓	✓	✓	✓	✓	✓	100
5	651fa231378060e192749f7c2a37c559.exe	✓	✓	✓	✓	✓	✓	✓	✓	100
6	651fa231378060e192749f7c2a37c559.exe	✓	✓	✗	✓	✓	✓	✓	✓	88.89
7	12aea17b5450e3bfc872c9f6fe6603da.exe	✓	✓	✓	✓	✓	✗	✗	✓	58.33
8	12aea17b5450e3bfc872c9f6fe6603da.exe	✓	✓	✗	✓	✓	✗	✗	✓	47.22
9	651fa231378060e192749f7c2a37c559.exe	✓	✓	✗	✓	✓	✓	✓	✓	88.89

**Hình 3.9: Kết quả chạy trên chương trình thử nghiệm**



**Hình 3.10: Hành vi của phần mềm thực thi**

### Giải thích điểm số đánh giá phần mềm

Phần mềm có hành vi gọi các hàm mã hóa và giải mã vì đây là một file thực thi đã được mã hóa trước khi tải về từ trang web <https://ninite.com>. Tệp tin cần phải giải mã để cài đặt vào máy người dùng chính vì vậy sử dụng thư viện giải mã CryptUnprotectData. Sau khi phát hiện hành vi này hệ thống tính điểm căn cứ theo hành vi số 7 trong bảng 6 sẽ tính điểm cho hành vi này là 7/36. Phần mềm “Ninite KLKite Codecs Installer.exe” tiếp tục gửi lệnh GET đến trang web <http://www.majorgeeks.com/> để tải tệp tin “k\_lite\_codec\_pack\_full” và cài đặt vào máy tính người dùng đây là hành vi GET hoặc POST dữ liệu nào đó từ bên ngoài tương ứng với hành vi số 8 trong bảng 6 và nhận điểm số 6/36. Như vậy tổng điểm số đánh giá tệp tin “Ninite KLKite Codecs Installer.exe” sẽ được tính theo công thức (1) và có số điểm là 36,11. Với số điểm này hệ thống đánh giá mối nguy hại từ phần mềm ở mức thấp. Sau khi phân tích có thể kết luận được đây là tệp tin thực thi sạch.

### 3.2.3. Đánh giá thử nghiệm và kết luận

Quá trình thử nghiệm thực hiện phân tích 2 mẫu, một mã độc và một mẫu không phải là mã độc, kết quả chương trình phát hiện được chính xác được tệp tin độc hại và đạt yêu cầu bài toán đặt ra.

Giải pháp đã đề xuất được đánh giá tóm tắt trong bảng sau.

Đạt mục tiêu như thiết kế	Chưa đạt được như mục tiêu
<p>1. Hệ thống có khả năng xử lý chính xác các dữ liệu cần lấy theo các tiêu chí đã được đặt ra.</p> <p>2. Hệ thống có khả năng phát hiện các hành vi nguy hiểm dựa vào dữ liệu báo cáo phân tích từ hệ thống Sandbox.</p> <p>3. Có khả năng giảm thiểu được phát hiện sai thông qua cơ chế tính điểm theo mức độ nguy hiểm của từng hành vi.</p>	<p>1. Thời gian xử lý chậm, chưa có chức năng báo cáo cho quản trị viên.</p> <p>2. Chưa thu thập được nhiều họ mã độc để thực hiện phân loại mã độc cũng như so sánh các hành vi để tạo bộ dữ liệu mẫu đủ lớn, đủ đa dạng, giảm thiểu phát hiện sai và áp dụng học máy để tăng chính xác và khả năng phân tích số lượng lớn mã độc.</p>

## KẾT LUẬN

### 1. Các kết quả đạt được

Qua quá trình nghiên cứu, luận văn đã đạt được các kết quả nghiên cứu chính như sau:

- Đã nghiên cứu về mã độc Ransomware, biện pháp nhận biết và phòng chống mã độc, một số phương pháp phát hiện nhanh mã độc.
- Đã nghiên cứu, phân tích, đánh giá hai phương pháp phân tích mã độc điển hình là: phân tích tĩnh và phân tích động.
- Phân tích, lựa chọn công cụ, phương pháp phân tích hành vi mã độc Ransomware. Nghiên cứu thiết lập môi trường phân tích mã độc. Đề xuất được một mô hình cụ thể cho phân tích hành vi mã độc.
- Thu thập mẫu mã độc, nghiên cứu các hành vi, hoạt động của một số loại mã độc. Đưa ra mức ưu tiên và tiêu chí, cách tính điểm tiêu chí đánh giá mức độ nguy hiểm của mã độc.
- Xây dựng được một giải pháp phát hiện mã độc Ransomware, cụ thể là một phần mềm phân tích dựa trên hành vi và phân tích heuristic gồm các mô đun: xử lý dữ liệu mẫu mã độc thu thập được, lưu giữ mẫu, đánh giá mức nguy hiểm và phát hiện mã độc.
- Thủ nghiệm giải pháp.
- Trong quá trình nghiên cứu, học viên đã viết và gửi bài báo khoa học có tiêu đề “Phương pháp kết hợp cho phân tích mã độc Ransomware” đến tạp chí an toàn thông tin ngày 21-5-2017.

Kết quả thực hiện đề tài nghiên cứu có ý nghĩa về mặt khoa học và thực tiễn. Về mặt khoa học, luận văn đã có nghiên cứu về cơ sở lý thuyết phân tích mã độc, so sánh đánh giá hai phương pháp phân tích động và tĩnh; đề xuất một mô hình cụ thể

và chương trình phân tích hành vi mã độc, phát hiện mã độc theo mức ưu tiên và đánh giá mức nguy hiểm.

Về mặt thực tiễn, kết quả nghiên cứu đưa ra một giải pháp phân tích, phát hiện mã độc Ransomware hiệu quả, thay thế một phần kiến thức chuyên gia, dễ sử dụng, có khả năng làm chủ công nghệ, áp dụng được vào thực tiễn.

## 2. Một số hạn chế

- Hạn chế số lượng các mẫu mã độc, chưa đa dạng về chủng loại, điều này có khả năng gây ảnh hưởng đến kết quả.

- Luận văn tập trung phân tích hai mẫu Ransomware phổ biến tại Việt Nam và chưa thực hiện được trên một số mẫu Ransomware mới khác để kiểm tra thêm về khả năng xử lý của chương trình.

## 3. Hướng phát triển

- Thu thập nhiều mẫu và biến thể nhằm xây dựng bộ hành vi đặc trưng hoàn chỉnh hơn. Khi đã có bộ dữ liệu đủ lớn có khả năng áp dụng học máy để tăng hiệu xuất phát hiện Ransomware.

- Nghiên cứu công nghệ phân tích tĩnh tự động để nâng cao hiệu xuất cũng như chất lượng của tập hành vi mẫu, làm cơ sở phát triển các giải pháp ngăn chặn Ransomware.

## TÀI LIỆU THAM KHẢO

- [1] Pearson Education, Inc (2004), The Tao Of Network Security Monitoring
- [2] Practical Malware Analysis (2012), The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig.
- [3] AAE Elhadi, MA Maarof, et.al. Malware detection based on hybrid signature behaviour application programming interface call graph. American Journal of Applied Sciences, 2012
- [4] AD Schmidt, SA Camtepe, S Albayrak. Static smartphone malware detection. eprints.qut.edu.au. 2010.
- [5] M Wagner, F Fischer, R Luh, A Haberson. A Survey of Visualization Systems for Malware Analysis. Eurographics Conference on Visualization (EuroVis) 2015.
- [6] Y Cao, Q Miao, J Liu, W Li. Osiris: a malware behavior capturing system implemented at virtual machine monitor layer. Mathematical Problems in Engineering, 2013.
- [7] KS Han, BJ Kang, EG Im. Malware analysis using visualized image matrices. The Scientific World Journal, 2014
- [8] S Cesare, Y Xiang, W Zhou. Malwise&# x2014; an effective and efficient classification system for packed and polymorphic malware. IEEE Transactions on Computers, 2013
- [9] LX Min, QH Cao. Runtime-based behavior dynamic analysis system for android malware detection. Advanced Materials Research, 2013.
- [10] S Feldman, D Stadther, B Wang. Manalyzer: automated android malware detection through manifest analysis. IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2014 .

[11] J Jang, HK Kim. Function-Oriented Mobile Malware Analysis as First Aid. *Mobile Information Systems*, 2016.

[12] DF Guo, JJ Hu, AF Sui, GZ Lin, T Guo . The Abnormal Mobile Malware Analysis Based on Behavior Categorization. *Advanced Materials Research* (Volumes 765-767). 9/2013.

[13] K Rami, V Desai . Performance Base Static Analysis of Malware on Android. *International Journal of Computer Science and Mobile Computing*. 9/2013, p.247-255.

[14] S Naval, V Laxmi, MS Gaur, P Vinod . ESCAPE: Entropy score analysis of packed executable. *Proceedings of the Fifth International Conference on Security of Information and Networks*. Pages 197-200. 2012.

[15] Robert J. Bagnall, Geoffrey French: The Malware Rating System (MRS). 2015 ( Track7/105\_tr7)

### **Một số website**

[16] <https://www.vxstream-sandbox.com>

[17] <https://www.wireshark.org>

[18] <https://www.hex-rays.com/products/ida/>

[19] <https://blog.kaspersky.com/tag/ransomware/>

[20] <https://ninite.com>