RANSOMWARE: TỐNG TIỀN TRÊN KHÔNG GIAN SỐ

Nguyễn Đăng Tiến*
Trường Đại học Kỹ thuật Hậu cần Công an nhân dân

TÓM TẮT

Trong những năm gần đây, có một loại phần mềm mã độc không chỉ gây ra những thiệt hại về tài chính cho người dùng Internet mà còn để lại hậu quả nặng nề về tính toàn vẹn dữ liệu khó có thể khắc phục được Trong bài báo này, chúng tôi trình bày về Ransomware, một loại mã độc đã xuất hiện từ khá lâu nhưng đang có xu hướng phát triển mạnh trở lại thời gian gần đây Đầu tiên, quá trình phát triển của Ransomware sẽ được đề cập Tiếp theo, chúng tôi trình bày về một số họ Ransomware phổ biến hiện nay gồm Cerber, Locky và CryptXXX, các phương thức lây nhiễm của chúng cũng như các biện pháp phòng tránh. Cuối cùng, chúng tôi xây dựng các đoạn script trên nền tảng hệ điều hành Windows để ngăn chặn sự lây nhiễm và thực thi của các họ Ransomware này

Từ khóa: *Phần mềm tống tiền, Ransomware mã hóa, Khóa Ransomware, Crypt Ransomware, Cerber Ransomware*

MỞ ĐẦU

Ransomware là từ viết tắt của hai từ ransom (tống tiền) và software (phần mềm), là loại mã độc có khả năng thực hiện các hình thức tống tiền thông qua việc sử dụng các kỹ thuật mã hóa [1]. Ban đầu, Ransomware được tạo ra với mục đích ngăn cản sự truy cập hợp pháp của người dùng vào máy tính, bắt buộc họ phải trả một khoản tiền chuộc để lấy lại quyền kiểm soát. Về sau, các biến thể của loại mã độc này được phát triển đa dạng hơn, mã hóa các tập tin hệ thống, dữ liệu bằng các thuật toán phức tạp hơn hay tấn công trên đa thiết bị, nền tảng. Ransomware đầu tiên được ghi nhận tại Nga năm 2005 với tên gọi TROJ_CRYZIP.A [1]. Khi xâm nhập vào máy tính, mã độc sẽ lập tức mã hóa, nén các file hệ thống bằng mật khẩu, đồng thời tạo ra thông điệp với nội dung yêu cầu nạn nhân phải nộp một khoản tiền chuộc nào đó. Về sau, Ransomware vươn ra ngoài lãnh thổ Nga, tấn công tiếp vào các file văn bản, dữ liệu như .docx, .xlsx, .jpg hay .pdf... với các thủ đoạn tinh vi và thuật toán mã hóa cao cấp hơn [2].

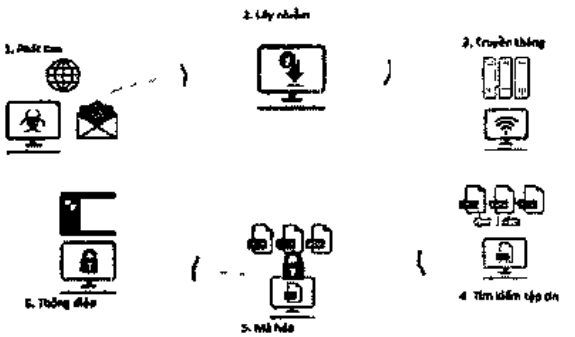
Trải qua quá trình hơn 10 năm, Ransomware đã có rất nhiều biến thể mới, phức tạp và tinh vi hơn, được chia thành hai dạng chính như sau.

- *Encrypting Ransomware* [2], [3], [4], [5], [6]: sử dụng các thuật toán mã hóa tiên tiến, được thiết kế để ngăn cản sự truy nhập vào các tập tin dữ liệu và hệ thống, yêu cầu một khoản thanh toán để cung cấp chìa khóa giải mã các nội dung bị chặn. Các Ransomware dạng này có thể kể tên như Cryptolocker, Locky hay CryptoWall

- *Locky Ransomware* [7], [8], [9], [10]: Loại mã độc này tách sự kiểm soát của người dùng đối với máy tính và hệ điều hành. Trong trường hợp này các tập tin không bị mã hóa nhưng kẻ tấn công vẫn yêu cầu một khoản tiền chuộc để mở khóa máy tính bị nhiễm. Điển hình của Ransomware dạng này có thể kể đến như Police-themed Ransomware hay Winlocker.

Trong các dạng Ransomware thì Encrypting Ransomware là loại phổ biến và gây nhiều đe dọa nhất đối với cộng đồng người sử dụng mạng Hình 2 biểu diễn thời gian phát hiện các loại Encrypting Ransomware trong 10 năm qua.

Cách hoạt động chung của các họ Ransomware dạng này được mô tả ở Hình 1 như sau:



Hình 1: *Hoạt động của Ransomware*

* *Email: dangtien136@gmail.com*

Đầu tiên, hacker phát tán mã độc qua các đợt thư rác, phương thức đính kèm email hay các trang web độc hại. Sau khi Ransomware lây nhiễm vào máy nạn nhân, chúng khởi động tiến trình truyền thông về với máy chủ, trao đổi khóa mã hóa. Bước thứ tư, Ransomware tiến hành tìm kiếm các tệp tin quan trong trong máy nạn nhân, thường là các tệp có đuôi mở rộng JPG, DOCX, XLSX, PPTX, PDF. Quá trình mã hóa kết thúc, thông điệp của hacker sẽ được hiển thị với những yêu sách đòi tiền chuộc.

Cùng với sự phát triển của Internet, các hệ thống thanh toán linh hoạt và sức hấp dẫn từ các khoản tiền chuộc, tống tiền bằng Encrypting Ransomware đã và đang là một hình thức tấn công được hacker ưa chuộng.

MỘT SỐ HỌ RANSOMWARE PHỔ BIẾN

Cerber Ransomware

Giới thiệu

Cerber là một họ Ransomware với khả năng mã hóa các tập tin của người dùng và cung cấp tính năng Text-to-Speech để nạn nhân nhận được thông điệp về khoản tiền chuộc. Sau khi mã hóa dữ liệu, Ransomware này sẽ để lại những thông báo đòi tiền chuộc dưới dạng file .TXT, .HTML hay .VBS tại các thư mục có dữ liệu bị mã hóa.

Cerber thuộc danh mục phần mềm mã độc tống tiền thế hệ thứ hai và có một số đặc điểm sau:

- Dữ liệu bị mã hóa và đổi tên file thành các kí tự ngẫu nhiên với đuôi là .cerber, cerber2 hay .cerber3...

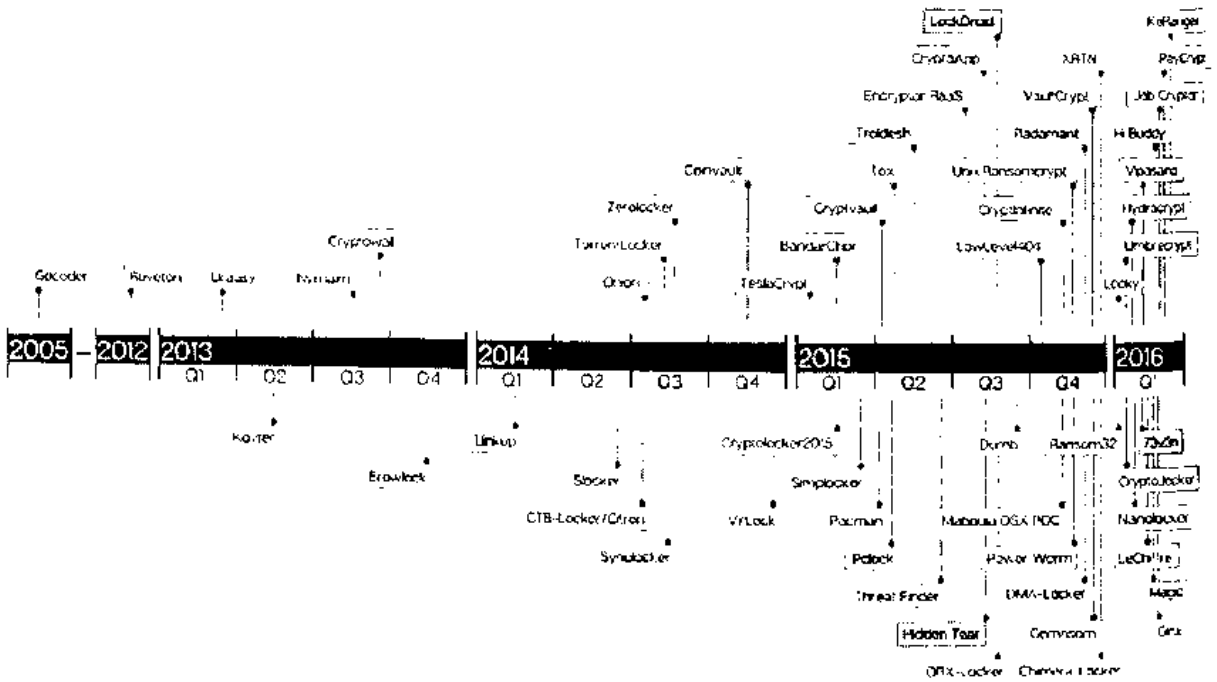
- Chủ yếu lây nhiễm qua email, các liên kết độc hại trên web hay ứng dụng chat.

- Cerber có thể tấn công cả các file chia sẻ của những máy tính khác trong cùng mạng.

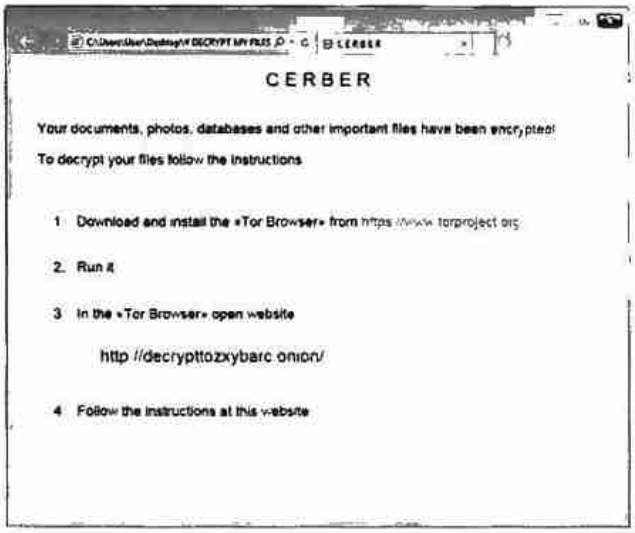
Cerber là dạng mã độc tống tiền sớm thay đổi với đội ngũ và kỹ thuật chuyên nghiệp, chúng đã tạo ra các phần mềm rất thành công với các bản cập nhật liên tục.

Quá trình mã hóa

Cerber lây nhiễm vào máy tính bằng các hình thức lừa đảo lợi dụng sự bất cẩn của người dùng. Trước khi cài đặt lên hệ thống, Cerber sẽ tiến hành kiểm tra và chắc chắn rằng nó sẽ không cài đặt trên các hệ thống sử dụng bàn phím ngôn ngữ Nga như 1049-Russian, 1058-Ukrainian, 1059-Belarusian, 1064-Tajik...



Hình 2. *Các họ Encrypting Ransomware được phát hiện trong 10 năm qua*



Hình 3. *Thông điệp đòi tiền chuộc trong file decryptmyfiles.html*

Sau khi kiểm tra, Cerber sẽ tự cài đặt tại thư mục %AppData%, xóa các bản sao lưu và vô hiệu quá chế độ Safe-boot Mode:

```
Bcdedit.exe "/set {default} recoveryenabled no"
Bcdedit.exe "/set {default} bootstatuspolicy ignoreallfailure"
```

Việc ngăn chặn chế độ Safe-boot Mode làm cho người dùng Windows không thể khởi động lại máy tính ở chế độ Safe mode để cố gắng phục hồi hệ thống.

Cerber sử dụng thuật toán mã hóa là sự kết hợp giữa mã hóa đối xứng và bất đối xứng. Nó bắt đầu với một khóa công khai RSA-2048 bit được lưu trong chính nó, khóa riêng được lưu trên máy chủ thanh toán Cerber. Tiếp theo nó tạo một cặp khóa RSA-576 bit để mã hóa tập tin, dữ liệu trên hệ thống của nạn nhân

Sau khi tạo xong khóa, Cerber sẽ lập một danh sách các file cần mã hóa.

Cuối cùng, Cerber tìm kiếm và ngắt các tiến trình sau nếu nó đang hoạt động:

```
outlook.exe
steam.exe
thebat.exe
thebat64.exe
thunderbird.exe
```

Cerber mã hóa hơn 200 đinh dạng tệp tin khác nhau, trong đó có một số tệp tin phổ biến như: .docx, .xlsx, .gif, .png, .dat, .mp3, .mp4, .jpg...Kết quả, Cerber mã hóa các file hệ thống, đổi tên file ngẫu nhiên với các đuôi mở rông .cerber, .cerber2 hay .cerber3 tùy phiên bản

Biện pháp phòng chống:

Trong khi Cerber tiếp tuc phát triển và nhóm hacker đứng phia sau liên tuc thay đổi phương pháp để tránh bị phát hiện và giải mã, người dùng cần nâng cao nhận thức để tự bảo vệ bằng các biện pháp sau đây:

- Định kỳ kiểm tra và sao lưu hệ thống, dữ liệu. Các hệ điều hành như Windows hay các phần mềm thông thường đều hỗ trợ sao lưu và phục hồi.

- Vô hiệu hóa tính năng Macro trong các tài liệu Microsoft Office.

- Cập nhật các bản vá lỗi mới nhất cho hệ thống, ứng dụng

Locky Ransomware

Giới thiệu

Ransomware này lần đầu tiên được phát hiện vào tháng 2/2016, được đặt tên là Locky vì

các file bị mã hóa có phần mở rộng là .locky. Chúng lây nhiễm vào máy tính của người dùng thông qua các đợt phát tán thư rác [3]. Có ba phương pháp hiệu quả mà hacker sử dụng để lây nhiễm mã độc vào máy của nạn nhân đó là:

- Đính kèm các file Word document macro với đuôi .docm theo email, khi người dùng mở file để xem nội dung thì đồng thời macro cũng được thực thi.

- Đính kèm các tập tin nén zip hoặc rar chứa các đoạn mã Javascript đã được làm rối để qua mặt người dùng và các chương trình diệt virus.

- Ẩn mình trên các trang web độc hay lợi dụng lỗ hổng của Adobe Flash.

Việc giải mã cho Locky gần như bất khả thi. Hệ thống chỉ có thể khôi phục từ các bản sao lưu hoặc chấp nhận nộp tiền chuộc.

Quá trình mã hóa

Khi lây nhiễm vào máy tính, mã độc Locky sẽ tự động sao chép đến %TEMP%\svchost.exe đồng thời xóa luồng dữ liệu NTFS trên ổ đĩa cứng. Locky sẽ được khởi chạy từ thư mục %TEMP%.

Locky sử dụng thuật toán mã hóa là sự kết hợp của RSA và AES. Cặp khóa RSA tạo ra từ máy chủ điều khiển và được sử dụng để tạo khóa AES. Sau khi hoàn thành, Locky thay đổi hình nền và hiển thị thông báo đòi tiền chuộc.

Biện pháp phòng chống:

Một số biện pháp sau đây giúp người dùng tự bảo vệ mình trước nguy cơ bị lây nhiễm bởi Locky:

- Chặn các email spam, cẩn thận với các email có nội dung và địa chỉ nơi gửi đáng ngờ.

- Tắt tính năng Macro trong bộ công cụ Microsoft Office.

- Không cho phép thực thi các file Javascript trên máy tính. Việc vô hiệu hóa có thể được thực thi bằng việc đặt giá trị "0" cho bản ghi.

- Chặn sự khởi tạo các cuộc gọi ra ngoài không giống như một số Ransomware khác, Locky cần sự kết nối tới máy chủ điều khiển bên ngoài để trao đổi khoá. Việc chặn các cuộc gọi ra bên ngoài giúp cho quá trình mã hóa không thể diễn ra được bình thường. Một lệnh cảnh báo của Snort cho một trường hợp được viết như sau:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"MALWARE-CNC Win.Trojan.Locky variant outbound connection";
flow:to_server,established; content:"POST"; http_method;
content:"/main.php"; fast_pattern:only; http_uri; urilen:9,norm;
content:!"|0D 0A|Accept|2D|Language|3A|"; http_header;
content:!"|0D 0A|Referer|3A|"; http_header;
```

Trong mọi trường hợp, cần có sự phát hiện và ngăn chặn Locky trước khi chúng kịp gây ra thiệt hại. Điều này đòi hỏi sự hiểu biết và các công cụ chính xác.

CryptXXX Ransomware

Giới thiệu

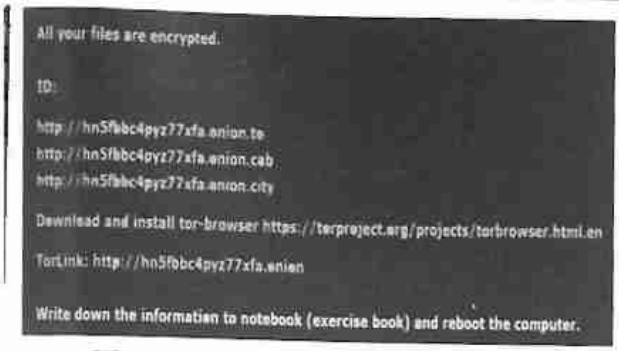
CryptXXX lần đầu xuất hiện vào tháng 3/2016 và nhanh chóng phát triển thành một trong những họ Ransomware phổ biến nhất. CryptXXX có những đặc trưng riêng không giống với hầu hết các loại mã độc tống tiền khác, cụ thể:

CryptXXX là dạng Ransomware duy nhất được phát hiện với định dạng file DLL (Dynamic Link Library - Thư viện liên kết động) chứ không phải là một file thực thi. Điều này khiến cho các chương trình diệt virus truyền thống dễ bị qua mặt.

- CryptXXX không chỉ mã hóa dữ liệu đòi tiền chuộc mà còn thực hiện đánh cắp Bitcoin, thông tin cá nhân của người dùng.

Quá trình mã hóa

CryptXXX sử dụng một số thuật toán mã hóa khác nhau để mã hóa file trên máy nạn nhân. Các phiên bản trước của CryptXXX sử dụng thuật toán Rivest Cipher 4 (RC4). Sau khi Kaspersky đưa ra công cụ để giải mã, nhóm hacker đứng đằng sau CryptXXX đã thay đổi chuỗi mã hóa để nhúng vào các file .dll.



Hình 4. *Thông báo đòi tiền chuộc của Ransomware CryptXXX*

Ở bước khởi tạo ban đầu, CryptXXX tạo ra một hạt nhân ngẫu nhiên dựa trên thời gian của hệ thống, sử dụng nó để tạo ra RandomInt, kết hợp với các tham số khác để tao nên khóa mã. Khóa mã này được dùng để mã hóa từng khối dữ liệu.

Biện pháp phòng chống

Trong phần này, chúng tôi đưa ra các biện pháp để phòng chống CryptXXX. Nhìn chung các họ Ransomware có một số phương pháp tương tự nhau, nhưng cũng có các phương pháp đặc thù đối với từng họ .

- Gỡ bỏ các ứng dụng tiềm ẩn nguy cơ bị khai thác nếu không thực sự cần thiết như Adobe Flash, Java hay Microsoft's Silverlight.

- Sử dụng các hệ thống DNS Firewalls hay phát hiện xâm nhập (IDS) để ngăn chặn sự truy nhập và truyền thông tới các tên miền chứa mã độc:

- Những IDS như Snort cũng rất hiệu quả trong trường hợp này để phát hiện bộ công cụ Neutrino. Tuy nhiên, cần lưu ý rằng Snort chỉ hoạt động hiệu quả nếu được cung cấp một bộ dấu hiệu đầy đủ. Một luật Snort để phát hiện sự lây nhiễm của Ransomware qua bộ công cụ Neutrino Exploit được cấu hình như sau:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
(msg:"EXPLOIT-KIT Neutrino exploit kit landing page detected";
flow:to_client, established; file_data; content:"return";
content:"join"; within:8;
content:"MSIE |28 5C|d+|5C|.|5C|d+|29 3B|"; distance:0;
content:"navigator["; within:60; content:!"]"; within:10;
metadata:policy balanced-ips drop, policy security-ips drop,
service http; classtype:attempted-user; sid:36535; rev:3;)
```

CryptXXX là một Ransomware năng động với đội ngũ phát triển chuyên nghiệp và nhận được nhiều sự tài trợ, giúp cho nó thường xuyên thay đổi để thích nghi với các biện pháp phòng chống

XÂY DỰNG SCRIPT ĐỂ PHÁT HIỆN VÀ NGĂN CHẶN RANSOMWARE

Ransomware thường nhắm đến các hệ điều hành họ Windows bởi lượng người dùng đông đảo có thể khai thác. Trong phần này, chúng tôi trình bày về sử dụng Windows Batch Scripting để ngăn các hành động Ransomware trên hệ thống. Các script này có nhiệm vụ ngăn chặn Ransomware quét các thư mục của nạn nhân, gửi các file tập tin lên server của kẻ tấn công. Hiện nay có một giải pháp tốt hơn được các phần mềm diệt virus sử dụng như phân tích hành vi với Sandbox

Ta có thể chia các script này thành hai loại phục vụ cho hai đối tượng khác nhau như. Script thứ nhất bảo vệ máy chủ chống lại Ransomware bằng các tập luật được cài đặt bởi người dùng.

ActivarAntiRansomwareAD.bat

```
@echo off
Color 1A
echo "Kich hoat bao ve...Vui long cho trong giay lat.."
reg add "HKLM\Software\Microsoft\Windows Script Host\Settings" /v Enabled /t
REG_DWORD /d 0 /f 2> nul > nul
reg add "HKCU\Software\Microsoft\Windows Script Host\Settings" /v Enabled /t
REG_DWORD /d 0 /f 2> nul > nul
```

Đoạn đầu tiên của script có chức năng tạo ra các đăng ký (registry) khởi động cùng hệ thống. Tiếp theo, script tiến hành tạo các luật giới hạn quyền thực thi trên các thư mục đặc biệt.

```
icacls
"%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files" /deny
*S-1-1-0:(OI)(IO)(X) 2> nul > nul
icacls "%userprofile%\AppData\Local\Microsoft\Windows\INetCache" /deny *S-1-1-
0:(OI)(IO)(X) 2> nul > nul
icacls "%ProgramData%" /deny *S-1-1-0:(OI)(IO)(X) 2> nul > nul
icacls "%Temp%\" /deny *S-1-1-0:(OI)(IO)(X) 2> nul > nul
echo "Bao ve da duoc kich hoat."
```

Script trên ngăn chặn sự lây nhiễm Ransomware từ các máy trong mạng nội bộ hoặc các máy được kết nối Internet, được phát triển để sử dụng trong môi trường doanh nghiệp hoạt động trên môi trường Active Directory.

AntiRansomwareHOME.bat

```
@echo off
cls
TITLE Antiransomware
Color 1A
echo Kich hoat bao ve...Vui long cho trong giay lat.."
reg add "HKLM\Software\Microsoft\Windows Script Host\Settings" /v Enabled /t
REG_DWORD /d 0 /f 2> nul > nul
"%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files" /deny
*S-1-1-0:(OI)(IO)(X) 2> nul > nul
icacls
```

Script trên làm giảm đáng kể sự lây nhiễm các ransomware, hạn chế thực thi khác thường trong các thư mục. Script này thường được sử dụng cho các máy tính cá nhân, hoạt động độc lập. Một vấn đề cần lưu ý là chế độ Windows Script Host access phải được cấu hình cho phép và việc từ chối một số dịch vụ có thể hạn chế một số tính năng khi truy cập Internet

Một phương pháp khác để tránh sự lây nhiễm của Ransomware là sử dụng công cụ Sandbox cách ly chúng với môi trường thật như Sandboxie hay Cuckoo Sandbox.

KẾT LUẬN

Trong bài báo này, chúng tôi đã trình bày về quá trình phát triển và phương thức lây nhiễm của Ransomware, một loại phần mềm mã độc đang phát triển mạnh và gây tác động lớn đến vấn đề an toàn dữ liệu hiện nay. Bài báo cũng tập trung phân tích quá trình lây nhiễm và mã hóa của ba họ Ransomware phổ biến gồm Cerber, Locky và CryptXXX để người dùng hiểu rõ cơ chế hoạt động của chúng. Trong bài, chúng tôi đưa ra một số phương pháp giúp ngăn chặn sự lây nhiễm và thực thi cho ba họ Ransomware trên. Trong đó, phương pháp sử dụng các luật Snort để phát hiện sự lây nhiễm và ngăn chặn tiến trình mã hóa của Locky và CryptXXX, cũng như các họ Ransomware có cơ chế tương tự, dựa trên các dấu hiệu đặc trưng đã được mô tả.

Để phòng tránh mã độc hiệu quả cao, ta cần có sự kết hợp của nhiều công cụ bảo vệ như tường lửa, phần mềm quét virus, phát hiện mã độc. Những biến thể Ransomware mới vẫn đang tiếp tục được sinh ra, với những tính năng cao cấp và thuật toán mã hóa mạnh mẽ hơn. Do đó, mỗi người dùng cần nâng cao cảnh giác, trang bị kiến thức để tự bảo vệ mình, để không trở thành nạn nhân của những kẻ tống tiền trên không gian số.

TÀI LIỆU THAM KHẢO

1. McAfee Labs (2016), *Understanding Ransomware and Strategies to Defeat it*, White paper

2 Alexandre Gazet (2008), *Comparative analysis of various ransomware virii*, EICAR conference.

3 Krzysztof Cabaj, Piotr Gawkowski (2015) "Network activity analysis of CryptoWall

ransomware". *Warsaw University of Technology* doi.10.15199/ 4, pp 11 48
4. Richard Shillam, *The Effect of Ransomware on Small to Medium Enterprises*, University of Derby Derbyshire, UK.
5 Dr P B Pathak (2016), "A dangerous trend of cybercrime Ransomware growing challenge", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 5 Issue 2, February 2016
6 Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda, Northeastern University (2016), *UNVEIL. A Large-Scale, Automated Approach to Detecting Ransomware*, Proceedings of the 25th USENIX 10–12, 2016
7 Nikolai Hampton, Zubair A Baig (2015), *Ransomware: Emergence of the cyber-extortion menace*, Proceedings of 13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015
8 Lee Garber (2014), "Security, Privacy, Policy, and Dependability Roundup" *IEEE Security & Privacy*, Vol. 12, Issue 4, July-Aug
9. Ms. Prachi Sharma, Mr. Shubham Zawar, Dr. Suryakant B Patil, *Ransomware analysis*, International Conference on Recent Innovations in Engineering and Management. ISBN 987-81-932074-5-1.
10. Akashdeep Bhardwaj, Vinay Avasthil, Hanumat Sastry and G V. B. Subrahmanyam (2016), "Ransomware Digital Extortion: A Rising New Age Threat", *Indian Journal of Science and Technology*, Vol 9(14), DOI. 10.17485/ijst/2016/v9i14/82936, April 2016.

SUMMARY
RANSOMWARE: RANSOM SOFTWARE IN COMPUTER NETWORK

Nguyen Dang Tien*
Academy of Logistics People's Public Security

Recently, there are many types of viruses that not only cause financial damages but also threat the data integrity and privacy of internet users. In this paper, we present Ransomware which appeared a long time ago but tend to significantly develop these days Firstly, the Ransomware's process of development is mentioned Secondly, we present some popular types of Ransomware such as Cerber, Locky and Crypt Ransomware. We also describe the popular way of Ransomware infection as well as the method to avoid them Finally, we construct the program to prevent the infection and the diffusion of these types of Ransomware.

Keywords: *Ransomware, Cerber Ransomware, Locky Ransomware, Crypt Ransomware, Encrypting Ransomware*

Ngày nhận bài: 20/3/2017; Ngày phản biện: 02/4/2017; Ngày duyệt đăng: 31/5/2017

* *Email. dangtien136@gmail.com*