BỘ THÔNG TIN VÀ TRUYỀN THÔNG

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**-----------------\*\*\*-----------------**

****

**NGUYỄN MINH VƯƠNG**

**ĐỀ CƯƠNG**

**LUẬN VĂN THẠC SĨ KỸ THUẬT**

**Hà Nội, tháng 10 năm 2016**

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**

NGÀNH : KHOA HỌC MÁY TÍNH

MÃ SỐ :

**ĐỀ CƯƠNG LUẬN VĂN THẠC SĨ KỸ THUẬT**

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

**Hà Nội, tháng 10 năm 2016**

## I. MỞ ĐẦU

## 1. Tính cấp thiết của đề tài

Với xu thế phát triển của Internet và mạng viễn thông, hiện tượng mất an toàn thông tin diễn ra ngày càng phức tạp, tinh vi và khó ứng biến. Tình hình mất an toàn thông tin cũng gây ra các tổn thất cho cá nhân, tổ chức thậm chí gây ra ảnh hướng lớn đến về kinh tế, chính trị, xã hội. Trong năm 2015 và năm 2016 chúng ta đã được chứng kiến rất nhiều sự kiện mất an toàn thông tin nghiêm trọng diễn ra trong nước và thế giới, vẫn tập trung vào một số phương thức tấn công nhất định như: Tấn công từ chối dịch vụ DDoS nhưng lượng thông tin rất lớn đã liên tục phá vỡ những kỷ lục trước đó; Tấn công có chủ đích (APT- Advanced Persistent Threat) âm thầm xâm nhập, thu thập thông tin và thay đổi giao diện web site, biển bảng thông báo,...

Đặc biệt không thể không kể đến mã độc mã hóa dữ liệu (được gọi là mã độc ransomware) quay trở lại với nhiều biến thể mới và nguy hiểm. Chúng sử dụng những thuật toán mã hóa mạnh mẽ, nhiều phương thức lây lan, nhiều biến thể khác nhau và dễ dàng tạo và sử dụng là điều khiến cho sự nguy hiểm của ransomware cao hơn rất nhiều cho với các trojan và virus thông thường... Ransomware có rất nhiều biến thể và phương pháp lây lan đa dạng. Một khi bị nhiễm loại mã độc này, tất cả dữ liệu gốc của nạn nhân sẽ bị mã hóa bởi thuật toán mạnh bằng key của kẻ tấn công, các bản dữ liệu gốc sẽ bị xóa hoàn toàn và không còn khả năng khôi phục dữ liệu. Nạn nhân muốn lấy lại dữ liệu cần phải trả tiền cho kẻ tấn công để lấy key giải mã mà chúng nắm giữ. Với 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, thách thức nhiều biện pháp phòng vệ an ninh.

Cách tiếp cận của những phần mềm diệt virut truyền thống dựa trên chữ ký đã không còn theo kịp sự phát triển của mã độc. Trên thực tế chúng ta đang phải đối mặt với vô vàn những nguy cơ khác nhau, từ lỗ hổng bảo mật giao thức, lỗ hổng bảo mật ứng dụng, lỗ hổng do chính người phát triển vận hành thiếu hiểu biết gây ra, thậm chí lỗ hổng con người - một mắt xích trong chuỗi vận hành hệ thống. Mặt khác nhân sự IT trong các tổ chức doanh nghiệp thường bị hạn chế về chuyên môn và tài chính, khó có khả năng triển khai những hệ thống sát SIEM, hệ thống phòng vệ dạng như IDS/IPS. Không những thế việc sử dụng những sản phẩm của nước ngoài khiến chúng ta luôn rơi vào tình trạng bị động và lệ thuộc.

Cuối cùng điều quan trọng hơn cả đó là sự chung tay trong công cuộc bảo đảm nền an toàn an ninh mạng nước nhà. Doanh nghiệp cơ quan tổ chức tự bảo vệ mình khỏi nguy cơ mât an toàn an ninh thông tin là góp phần rất lớn trong công tác đảm bảo an toàn an ninh không gian mạng của cộng đồng, Quốc gia. Tự bảo vệ mình trước những mã độc ăn cắp thông tin, mã hóa dữ liệu ransoware cũng là cách để bảo vệ uy tín, an toàn và ổn định cho doanh nghiệp tổ chức phát triển.

Với những yêu cầu thực tiễn như vậy, cần có những giải pháp phòng chống mã độc hiệu quả, dễ sử dụng, phần nào thay thế chuyên gia mà chi phí thấp cho phép cơ quan, tổ chức phát hiện các mối đe dọa của mã độc mã hóa dữ liệu ransomware, từ đó đưa ra các phương án xử lý ngăn chặn các mối đe dọa này. Từ nhu cầu thực tiễn cấp thiết đã nêu trên, tôi đã chọn đề tài “NGHIÊN CỨU, XÂY DỰNG VÀ THỬ NGHIỆM GIẢI PHÁP PHÁT HIỆN MÃ ĐỘC RANSOMWARE”.

Ý nghĩa khoa học của đề tài: Tạo ra mối liên hệ về mặt phương pháp luận giữa lý thuyết với thực tiễn đồng thời đưa ra một giải pháp phân tích phát hiện mã độc ransomware hiệu quả mà chi phí thấp.

Ý nghĩa thực tiễn của đề tài: Người dùng chủ động phát hiện được mã đôc và từ đó có cơ chế phòng tránh loại mã độc nguy hiểm này, giảm thiểu tối đa thiệt hại do mã độc gây ra, góp phần ổn định, giữ uy tín để kinh doanh và phát triển.

## 2. Mục đích nghiên cứu

Nghiên cứu phương pháp phân tích, phát hiện mã độc ransomware và xây dựng một giải pháp phân tích thử nghiệm phát hiện mã độc ransomware.

### 3. Đối tượng và phạm vi 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.
* Xây dựng tập dữ liệu mẫu về hành vi phổ biến của một số họ mã độc ransomware.
* Các thành phần của giải pháp phát hiện mã độc dựa trên hành vi.

## 4. Các nhiệm vụ chính cần thực hiện

## Thu thập mẫu mã độc, hành vi mã độc.

## Xây dựng tập dữ liệu mẫu hành vi mã độc.

## Xây dựng một giải pháp thử nghiệm phát hiện mã độc ransomware.

## 5. Kết quả dự kiến

## Nghiên cứu khái quát về một số họ mã độc Ransomware tiêu biểu và biện pháp phòng chống.

## Nghiên cứu phương pháp phân tích, phát hiện mã độc ransomware.

## Xây dựng một giải pháp phát hiện mã độc Ransomware và thực hiện thử nghiệm.

## 6. Phương pháp và công cụ nghiên cứu

## Phương pháp nghiên cứu

## Nghiên cứu lý thuyết, khảo sát thực tiễn.

## Phương pháp phân tích mã độc.

## Phương pháp phân tích, thiết kế hệ thống.

## Thực nghiệm.

## Công cụ nghiên cứu

* Sử dụng công cụ phân tích Kết quả tìm kiếm Cuckoo Sandbox, process\_hacker
* Sử dụng các công cụ moniter hành vi: WireShark, pcap, tcpdump
* Phát triển thêm các module nhờ vào các ngôn ngữ lập trình khác: PHP, Java,...

# II. DỰ KIẾN NỘI DUNG BÀI

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

## Vấn đề an toàn thông tin nói chung và mã độc Ransomware.

## Đặt vấn đề nghiên cứu.

## Tóm tắt nội dung chính.

## Chương 1: Khái quát mã độc và các phương pháp phân tích mã độc

* Tổng quan về mã độc ransomware.

+ Khái niệm.

+ Lịch sử phát triển, các biến thể.

+ Mức độ nguy hiểm, nguy cơ, hậu quả.

+ Hiện trạng tại Việt Nam và thế giới.

+ Nhu cầu phân tích phát hiện mã độc ransomware.

* Biện pháp phòng chống ransomware.
* Kết luận chương

## Chương 2. Phương pháp phân tích, phát hiện mã độc ransomware

* Một số phương pháp phát hiện nhanh trong thực tiễn.
* Môi trường hỗ trợ phân tích, phát hiện mã độc.

+ Cơ sở lý thuyết.

+ Công cụ trợ giúp.

* Phân tích, đánh giá các phương pháp

+ Phương pháp phân tích tĩnh

+ Phương pháp phân tích động

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

+ Sự cần thiết xây dựng giải pháp phát hiện ransomware

* Kết luận chương.

## Chương 3: Xây dựng và thử nghiệm giải pháp phát hiện mã độc ransomware

* Kiên trúc và các thành phần giải pháp.
* Xây dựng module chuyển đổi tập dữ liệu mẫu.
* Xây dựng module phát hiện mã độc.
* Thử nghiệm.
* Kết luận chương.

**KẾT LUẬN**

* Kết quả dự kiến

+ Báo cáo về một số họ mã độc Ransomware tiêu biểu và biện pháp phòng chống.

+ Trình bày phương pháp phân tích tĩnh và động, phát hiện mã độc ransomware.

+ Hoàn thiện giải pháp phát hiện mã độc Ransomware dựa vào hành vi và thực hiện thử nghiệm.

**III. 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 malwaredetection. Advanced Materials Research, 2013.

[10] S Feldman, D Stadther, B Wang. Manilyzer: 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] P Faruki, A Bharmal, V Laxmi . Android security: a survey of issues, malware penetration, and defenses. IEEE Communications Surveys & Tutorials ( Volume: 17, Issue: 2, Secondquarter 2015 )

**Một số website**

[1] https://cuckoosandbox.org/

[2] Wireshark, https://www.wireshark.org

[3] https://www.hex-rays.com/products/ida/

[4] https://blog.kaspersky.com/tag/ransomware/

**IV. DỰ KIẾN KẾ HOẠCH THỰC HIỆN**

|  |  |  |
| --- | --- | --- |
| STT | Thời gian | NỘI DUNG THỰC HIỆN |
| 1 | 02 Tuần:  Từ 01/10/2016  Đến 15/10/2016 | XÂY DỰNG ĐỀ CƯƠNG CHI TIẾT |
| 2 | 01 tháng:  Từ 16/10/2016  Đến 15/11/2016 | NGHIÊN CỨU HOÀN THIỆN NỘI DUNG CHƯƠNG I |
| 3 | 01 tuần:  Từ 16/11/2016  Đến 23/11/2016 | BÁO CÁO TIẾN ĐỘ |
| 4 | 01 tháng:  Từ 24/11/2016  Đến 24/12/2016 | NGHIÊN CỨU HOÀN THIỆN NỘI DUNG CHƯƠNG II |
| 5 | 01 tuần:  Từ 25/12/2016  Đến 02/01/2017 | BÁO CÁO TIẾN ĐỘ |
| 6 | 03 tháng:  Từ 03/01/2017  Đến 03/04/2017 | NGHIÊN CỨU HOÀN THIỆN NỘI DUNG CHƯƠNG III |
| 7 | 01 tuần:  Từ 04/04/2017  Đến 10/04/2017 | BÁO CÁO TIẾN ĐỘ |
| 8 | 02 tháng:  Từ 11/04/2017  Đến 11/06/2017 | HIỆU CHỈNH VÀ HOÀN THIỆN LUẬN VĂN |

|  |  |
| --- | --- |
| **Ý KIẾN CỦA CÁN BỘ HƯỚNG DẪN**  *(Ký ghi rõ họ tên)*  **PGS.TSKH. HOÀNG ĐĂNG HẢI** | **NGƯỜI LẬP ĐỀ CƯƠNG**  *(Ký ghi rõ họ tên)*  **NGUYỄN MINH VƯƠNG** |
| **DUYỆT CỦA TRƯỞNG TIỂU BAN CHẤM ĐỀ CƯƠNG**  *(Ký ghi rõ họ tên)* | |