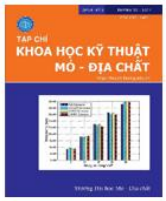
Tạp chí Khoa học Kỹ thuật Mỏ - Địa chất

Trang điện tử: http://tapchi.humg.edu.vn



THÔNG TIN KHOA HỌC

WannaCry - khóc không ra nước mắt

Đào Anh Thư *

Khoa Công nghệ Thông tin, Trường Đại học Mỏ - Địa chất, Việt Nam

THÔNG TIN BÀI BÁO

Quá trình:
Nhận bài 12/7/2017
Chấp nhận 25/8/2017
Đăng online 30/10/2017

Từ khóa:
Virus mạng
Mã độc tống tiền
Lỗ hổng
WannaCry

TÓM TẮT

Bài báo trình bày về virus mạng WannaCry đã làm chấn động cả thế giới khi tạo nên một cơn bão thiệt hại máy tính, càn quét với quy mô lớn nhất từ trước đến giờ. Không giống với các loại virus khác, WannaCry là loại mã độc tống tiền, đòi người bị hại phải trả tiền để giải mã cho máy tính bị đóng băng. Loại mã này hầu như không thể giải mã được nếu kẻ mã hóa không cung cấp thông tin. Tác giả đã trình bày các vấn đề về đặc trưng, hoạt động phá hoại và một số hướng dẫn cơ bản cho người sử dụng để tránh bị nhiễm loại virus mã độc này.

1. Mở đầu

Ngày thứ sáu 12 tháng 5 năm 2017, cả thế giới chấn động khi giới tội phạm mạng đã ghi được kỷ lục mới. Cuộc tấn công mã độc gián điệp trên toàn thế giới đã tác động tới hơn 100 quốc gia chỉ trong vòng 48 giờ, vậy là WannaCry/ WanaCrypt0r 2.0 đã gây ra cuộc tấn công lớn nhất trên thế giới từ trước đến giờ, cả về quy mô độ hư hại cũng như phạm vi và tốc độ lây nhiễm. Tính tới ngày 14 tháng 6 năm 2017, số lần giao dịch tiền chuộc là 327 với số tiền lên tới 130,634.77 đô la Mỹ.

2. WannaCry là gì?

WannaCry, WanaCrypt còn viết tắt là Wcry là phần mềm tống tiền hoạt động gián điệp có các đặc trưng hoạt động hết sức phức tạp (Limor Kessem, 2017).

Tác giả liên hệ
E-mail: daoanhthu@humg.edu.vn

Thứ nhất, mã độc này sử dụng những thông tin rò rỉ do nhóm hacker Shadow Broker khám phá ra và công bố. Hậu quả của việc rò rỉ này là nổi lên vô số phần mềm mã độc sử dụng chúng vào mục đích bất chính mà trường hợp WannCry là tồi tệ nhất.

Thứ hai, mã độc WannaCry sử dụng mã hoá bất đối xứng cực mạnh, RSA 2048 bit để mã hoá file. Mã hoá bất đối xứng tương đối chậm so với mã hoá đối xứng nhưng lại rất mạnh và hầu như không thể phá mã được.

Thứ ba, mã độc này sử dụng kiến trúc môđun, kiểu kiến trúc phổ biến trong cả phần mềm hợp pháp và phần mềm bất hợp pháp phức tạp như Trojan tấn công ngân hàng. Thông thường phần mềm gián điệp không thuộc loại mô đun, mà thường đơn giản hơn, các tác vụ cũng không chứa thành phần mô đun. Điều này có nghĩa là tác giả đằng sau Wcry dường như là cả một nhóm lập trình viên chứ không thể là một người. Thậm chí người ta còn cho rằng là cả một băng nhóm tội phạm mạng có tổ chức chuyên phát tán mã độc.

Cuối cùng, chúng ta không phải đang đối phó với những kẻ A-ma-tơ. Cuộc tấn công trên diện rộng này có tính nghiêm trọng cao và mặc dù lỗ hổng đến giờ đã được vá lại, nhưng nhiều cơ quan, tổ chức đã bị dính và con số nạn nhân tiếp tục tăng lên.

3. Tại sao WannaCry có thể lây lan nhanh đến như vậy?

Có ba yếu tố nguyên nhân chính để virus này lây lan nhanh chóng (Bill Brenner, 2017):

Mã lập trình cho phép con sâu (worm) này lan qua mạng nhanh chóng mà không cần người dùng tác động thêm gì sau khi diễn ra ra hành động lây nhiễm ban đầu. Nghĩa là chỉ cần một cú click từ người dùng là virus tự động lây nhiễm máy nạn nhân và tất cả hệ thống kết nối với máy nạn nhân.

Virus khai thác một lỗ hổng mà nhiều cơ quan, tổ chức, doanh nghiệp đã bỏ qua không vá lại. Mặc dù vá lỗ hổng hệ điều hành là việc làm đầu tiên trong chiến lược an ninh nhưng việc thường xuyên cập nhật các bản vá không phải lúc nào cũng suôn sẻ.

Nhiều cơ quan, tổ chức, doanh nghiệp vẫn còn sử dụng Windows XP, mặc dù Microsoft đã ngừng hỗ trợ Windows XP và không còn phát hành các bản vá lỗi cho hệ thống này. Vì vậy mà nó đã trở thành mục tiêu của cuộc tấn công.

Phần mềm tống tiền Wcry đã nhắm đến các thành phần chia sẻ (share-holder) chính trong hệ điều hành chứ không phải bản thân hệ điều hành Windows. Vì thế mà nó nhắm tới tất cả các phiên bản: Windows XP, Windows Vista, Windows 7, Windows 8 và Windows 10.

Với sự sử dụng phổ biến của hệ điều hành Microsoft Windows, có nghĩa là lỗ hổng xuất hiện khắp nơi, dẫn tới danh sách các hệ thống bị ảnh hưởng trên diện rộng rất lớn: hệ thống máy bán lẻ (POS - Point of Sale), hệ thống máy rút tiền tự động ATM, hệ thống điều khiển giao thông, ngân hàng, bệnh viện, nhà hàng, máy chủ, và còn rất nhiều nữa.

Sự kết hợp chết người này làm cho nạn nhân lâm vào tình cảnh tồi tệ và khiến cho WannaCry trở thành phần mềm tống tiền hiệu quả nhất trên thế giới. Chỉ trong vòng một ngày, nó đã chu du qua 150 quốc gia và lây nhiễm tới 230,000 máy tính.

Hình 1. Giao diện đòi tiền của WannaCry.

Khi tấn công vào Dịch vụ Y tế Quốc gia tại nước Anh, cơ quan này buộc phải từ chối bệnh nhân, huỷ các cuộc phẫu thuật và sắp xếp lại lịch khám, chỉ có thể xử lý các trường hợp bệnh nhân cấp cứu. Và sau đó là hàng loạt báo cáo tê liệt hệ thống lớn nhỏ ở khắp các nước.

Hình ảnh đòi tiền của WannaCry trở thành nỗi ám ảnh với nạn nhân vì nhìn thấy nó nghĩa là toàn bộ tệp tin, thư mục trên máy đã bị khoá mã toàn bộ, không thể thao tác được gì trên máy ngoài bật và tắt máy. Nếu không muốn trả tiền chuộc thì chỉ còn cách chịu mất hết dữ liệu, format toàn bộ ổ cứng và cài đặt lại tất cả mọi thứ từ đầu. Quả thực virus WannaCry đã đẩy nạn nhân vào tình cảnh trớ trêu, khóc không ra nước mắt.

Khác với hầu hết các phần mềm tống tiền khác, Wcry không sử dụng ảnh để đòi tiền chuộc mà sử dụng một file thực thi. Bản thân file chạy này không phải là phần mềm mã độc mà chỉ là một chương trình đơn giản hiển thị thông báo cho nạn nhân (Limor Kessem, 2017).

Hình ảnh hiện lên cho từng nạn nhân phụ thuộc vào dải địa chỉ IP ánh xạ cho quốc gia của nạn nhân. Tác giả của phần mềm này đưa ra nhiều định dạng ngôn ngữ cho Wcry, các phiên bản này dịch máy và thường mắc lỗi cú pháp cứng nhắc. Để đảm bảo nạn nhân nhìn thấy thông báo ngay lập tức, nó đặt thông báo tại một cửa sổ trên cùng của màn hình desktop.

Có một câu hỏi ở đây là liệu trả tiền chuộc thì máy tính người dùng có trở lại nguyên vẹn như trước được không? Vì có vẻ số tiền không quá lớn. Tuy nhiên không ai dám đảm bảo điều này cả mà nạn nhân nếu có trả tiền thì kết quả có thế nào họ cũng im hơi lặng tiếng vì điều này là bất hợp pháp.

4. Phần mềm tống tiền trở thành mối nguy hại gia tăng toàn cầu

Phần mềm tống tiền không còn mới mà cũng chẳng xa vời như trên phim ảnh. Loại phần mềm mã độc này xâm nhập hệ thống của người sử dụng để mã hoá toàn bộ các file trên đó sau đó đòi một khoản tiền chuộc mới trả lại quyền sử dụng cho nạn nhân. Trở lại năm 1989, phần mềm tống tiền từng bùng nổ trên đĩa mềm gửi cho người sử dụng máy tính. Năm 2014, loại mã độc này manh nha trở lại cùng hàng loạt các vụ khoá mã trên toàn cầu, cho phép tội phạm mạng nặc danh đòi tiền từ bất kỳ ai.

Năm 2016, mã độc tống tiền là mối đe doạ trực tuyến phổ biến nhất, mỗi ngày có tới hơn 40,000 cuộc tấn công cùng một lúc và chiếm tới hơn 65% mail rác có chứa mã độc. Kết quả nghiên cứu của IBM X-Force khi theo dõi mail rác cho thấy mail chứa mã độc tống tiền năm 2016 tăng vọt 6,000%, so với 0.6% năm 2015, chiếm 40% lượng mail rác (Kelly Kane, 2016). Tình trạng này còn tồi tệ hơn nữa trong năm 2017 này.

FBI và các lực lượng hành pháp quốc tế cũng cảnh báo về nguy cơ phần mềm tống tiền. FBI dự đoán mã độc tống tiền giúp tội phạm mạng kiếm chác tới 1 tỉ đô la cuối năm 2016, mà con số này còn lớn hơn nữa trong năm 2017. Cybersecurity Ventures dự đoán chi phí thiệt hại do mã độc tống tiền gây ra trong năm 2017 vượt quá 5 tỉ đô la Mỹ (Steve Morgan, 2017)

5. Người dùng trước hết cần tự bảo vệ máy của mình

Các cơ quan luật pháp về an ninh mạng đưa ra khuyến cáo từ chối trả tiền chuộc vì việc trả tiền càng khuyến khích tội phạm mạng tiếp tục phát tán mã độc và thu về tiền mặt. Trước hết người sử dụng cần phải tự bảo vệ máy của mình khỏi nguy cơ mã độc này. Dưới đây là một số chỉ dẫn sử dụng máy tính lên mạng an toàn, tránh được WannaCry:

Không click vào các đường dẫn nguy hiểm trong hòm thư điện tử.

Rất thận trọng khi vào các trang web có cảnh báo không an toàn (unsafe) hoặc không đáng tin cậy (unreliable).

Không bao giờ được click vào đường link không đánh tin cậy trên trang web hoặc khi truy cập Facebook, Zalo, Viber hay các ứng dụng mạng xã hội và nhắn tin khác.

Nếu người dùng nhận được tin nhắn có kèm link từ bạn bè thì hỏi họ trước khi mở link ra để chắc chắn link đó an toàn (máy tính bị lây nhiễm mã độc thường tự động gửi đường dẫn qua tin nhắn cho danh sách bạn bè trên máy đó).

Thường xuyên lưu các bản sao dự phòng cho các file quan trọng.

Cảnh giác với thư điện tử giả mạo có tên gần giống với các dịch vụ thanh toán điện tử, ngân hàng trực tuyến, chúng có thể giả mạo giao diện web giống hệt nên cần xem kỹ tên địa chỉ trang web. Ví dụ địa chỉ đúng của ngân hàng Vietcombank là vietcombank.com.vn thì địa chỉ

trang web giả mạo có thể là vietcombank.net.vn hoặc vietconbank.com.vn.

Sử dụng phần mềm diệt virus (anti-virus) và luôn cập nhật bản mới nhất.

Cập nhật liên tục hệ điều hành Windows, các bản vá lỗi mới nhất.

6. Kết luận

Tác hại của mã độc tống tiền là rất lớn vì tác động trên diện rộng và sự hư hại khó phục hồi của nó. Nghiên cứu cách thức hoạt động gây hại của WannaCry, sâu máy tính mã độc tống tiền mới nhất cũng chỉ rõ khả năng khôi phục lại hoạt động của máy tính sau khi bị nhiễm là rất thấp. Nên cách thức xử lý tốt nhất vẫn là các biện pháp đề phòng cho tình huống xấu nhất.

Hiện tại Microsoft đã đưa ra các hướng dẫn xử lý tắt dịch vụ lỗ hổng bị WannaCry lợi dụng, các công cụ cũng được phát triển từ các nhà an ninh mạng trên thế giới để xử lý máy bị nhiễm cũng đạt được thành công. Tuy nhiên người dùng luôn phải cảnh giác vì loại phần mềm tống tiền này chắc chắn sẽ trở lại với các hình thức che giấu khôn khéo hơn và tác hại ghê gớm hơn nữa.

Tài liệu tham khảo

Bill Brenner, 2017. *WannaCry: the ransomware worm that didn't arrive on a phishing hook*. nakedsecurity.sophos.com.

Kelly Kane, 2016. *IBM Study: Businesses More likely to Pay Ransomware than Consumers*. ibm.com.

Limor Kessem, 2017. *WannaCry Ransomware Spreads Across the Globe, Makes Organizations Wanna Cry About Microsoft Vulnerability*. securityintelligence.com.

Steve Morgan, 2017. *Ransomware damages rise 15X in 2 years to hit $5 billion in 2017*. csoonline.com.

ABSTRACT

Wannacry - cry without tears

Thu Anh Dao

Faculty of Information Technology, Hanoi University of Mining and Geology, Vietnam.

The article presents information about WannaCry, the network virus which made the global assault, quickly spreaded more than a storm, caused damages to billions of computers, which made it the most severe malware attack so far in 2017. Unlike other network malwares, WannaCry is a new type of ransomeware which demands the victim to pay for unfreezing the infected computer. This type of encrypted code of virus almost can not decrypted, except its creator. This article includes characteristics, damaging actions and some guide lines for computer users to protect their computers from WannaCry and other ransomwares.

Keywords: network virus, ransomware, vulnerability, WannaCry.