**https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis**

**Cách lây lan**..

1. Phát tán qua phương thức thông thường là nhúng vào các bản crack, các trang web có nhiều người truy cập. Người dùng tải về các file không rõ nguồn gốc hoặc truy cập đường Link độc hại sẽ có nguy cơ bị nhiễm mã độc này.  
(Về kỹ thuật thì nó vẫn đang phát tán malware qua các mạng lưới phát tán malware (tức là tổ chức chuyên phát tán malware) và các exploitkit vd như lỗ hổng MS17-010 tận dụng công cụ bị lỗ cua NSA)

2. WannaCry lây lan mạnh vì nó không chỉ phát tán theo cách truyền thống như trên mà nó còn lây lan qua mạng LAN do tận dụng các công cụ khai thác lỗi SMB mà NSA (Cơ quan an ninh quốc gia Hoa Kỳ) phát triển bí mật, nhưng bị nhóm ShadowBroker đánh cắp và tung ra public từ tháng trước.

Nếu một máy trong mạng LAN bị nhiễm WannaCry thì toàn bộ các máy trong mạng LAN cũng có thể bị nhiễm chung nếu như không được vá lỗ hổng trước đó.:)

Vì cách lây lan như trên mà việc thực hiện các bước an toàn như tắt SMBv1 và cập nhật cho Windows bản vá lỗi mới nhất cũng KHÔNG HOÀN TOÀN AN TOÀN. Nó chỉ ngăn việc con virus này lây lan từ máy khác cùng mạng LAN với nhau. Không ngăn việc tải file có chứa mã độc từ internet.

Con này chỉ lây lan trên Windows và mạng máy tính Windows, hiện không có phiên bản biến thể nào hoạt động trên Mac và Linux (Tính đến ngày 16/5) Trừ những máy tính linux nhưng cài Wine. Hiện tại tính đến chiều qua 15/5 mã độc đã update lên phiên bản 4.0 hiện tại vẫn chưa có thông tin mới về phiên bản này.

**Cách phòng chống**.

1. Update bản vá lỗi mới nhất cho Windows.

2. Disable tính năng SMB bằng cách vào Start, search Windows Features, bỏ dấu check chỗ SMB

3. Cập nhật các Antivirus. Hiện Windows Defender, McAfee, Symantec, ESET, Bitdefender... Sau khi cập nhật AV cần bật tính năng bảo vệ Realtime Protection để ngăn việc máy tính bị nhiễm.

4. BACKUP DỮ LIỆU QUAN TRỌNG LÀ CÁCH DUY NHẤT CHỐNG RANSOMWARE.

5. Nên dùng các dịch vụ Cloud Drive như Google Drive, OneDrive, DropBox để thường xuyên sync (đồng bộ) dữ liệu lên Mây (Cloud). Chú ý đối với thông tin quan trọng cần mã hóa hoặc đặt mật khẩu mạnh để chống lộ lọt thông tin.

**Cách xử lý khi bị nhiễm Ransomware WannaCry.**

1. Ngắt ngay lập tức các máy tính bị nhiễm khỏi mạng LAN, tránh để nó lây lan qua các máy khác

2. Nếu thông tin quan trọng nên cất giữ ổ lưu trữ cẩn thận chờ khi có tool giải mã. Hiện có thông tin là mã độc WannaCry có lỗi trong cách thức nó mã hóa dữ liệu, nên các chuyên gia bảo mật đang thử tìm cách khai thác và viết công cụ giải mã.

3. Nếu dữ liệu không quan trọng thì format toàn bộ ổ cứng và cài lại win, phải FORTMAT TOÀN BỘ Ổ CỨNG mới sạch, chỉ format ổ C rồi cài lại vẫn sẽ bị.

**Thông tin về phiên bản 4.0.**

[https://www.bleepingcomputer.com/…/with-the-success-of-wan…/](https://www.bleepingcomputer.com/news/security/with-the-success-of-wannacry-imitations-are-quickly-in-development/)

Tài liệu tiếng anh phân tích chuyên sâu:

<https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis>

**Tham khảo công văn của VNCERT**

http://vncert.gov.vn/baiviet.php?id=60