Danh sách 3 loại virus Ransomware siêu nguy hiểm và đáng sợ nhất

Nếu từ trước đến giờ bạn nghĩ rằng **virus** và **key-logger** là những mối đe dọa chết người thì đừng vội khẳng định lại điều đó bởi vẫn còn mối đe dọa nguy hiểm hơn thế nữa.

Trong khi các giải pháp bảo mật để bảo vệ chúng ta khỏi các mối đe dọa, hacker (tin tặc) ngày càng được cải thiện dần thì các chương trình độc hại (malware) cũng ngày càng "*tinh ranh*" hơn. Và một trong những mối đe dọa mới xuất hiện gần đây đó là cách thức tống tiền thông qua ransomware.

Virus ransomware là một loại phần mềm độc hại, mã hóa và khóa tất cả hoặc một số tập tin trên máy tính của người dùng, sau đó yêu cầu người dùng phải trả một khoản tiền chuộc để mở khóa.

Mức độ nghiêm trọng của các vụ tấn công phụ thuộc vào loại tập tin mà ransomware ảnh hưởng. Trong một số trường hợp, nó chỉ mã hóa một vài tập

tin phần mềm mà người dùng tải về từ trên mạng Internet mà hệ điều hành không có các tính năng đó. Trong một số trường hợp khác, các phần mềm độc hại có thể ảnh hưởng đến toàn bộ ổ đĩa cứng và làm cho máy tính của người dùng không sử dụng được.

Dưới đây là 3 loại **virus Ransomware siêu nguy hiểm và đáng sợ nhất** từ trước đến nay.

1. Locky Ransomware

Locky được phát hiện đầu tiên vào tháng 2 năm 2016. Loại ransomware này thường được gửi dưới dạng file đính kèm email, có tiêu đề '*Invoice J-00*'. Email có chứa tài liệu văn bản mà macro "*lập trình*" trong đó.

Tài liệu này nói rằng nếu người nhận không thể nhìn thấy các hóa đơn, họ nên cho phép macro chạy. 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 khá là thông minh, nó 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.

Mới đây, một dạng thức mới của mail Locky đã được phát hiện ra đó là '*Receipt of Order – 00*' thay vì dạng thức các hóa đơn.

2. Cerber Ransomware

Cerber là có một dạng phần mềm độc hại (malware) thông minh và thậm chí là còn khá "mạnh". Lí do là bởi vì nó là phần mềm miễn phí, có sẵn để người dùng tải về, cài đặt và vô tình bị phần mềm này "tấn công" hệ thống mà không hề hay biết.

Loại ransomware này sử dụng hai phương pháp "vận chuyển":

- Phương pháp đầu tiên cũng giống như Locky, Ceber cũng được gửi như một file 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.

Khi Cerber "lây nhiễm" và "tấn công" hệ thống của bạn, nó sẽ "cướp" quyền kiểm soát hơn 400 loại tập tin và mã hóa chúng trước khi yêu cầu tiền chuộc. Các khoản tiền chuộc có thể cao đến khoảng 500 $ và nếu không trả tiền, bạn sẽ không được phép sử dụng máy tính của mình.

3. CryptoWall Ransomware

CryptoWall là loại ransomware có nhiều "*mối nguy hại*", đe dọa người dùng nhiều nhất. Loại ransomware này không sử dụng bất kỳ các thủ đoạn như đính kèm email mà nó dựa vào các lỗ hổng trong Java và "lây lan" thông qua các quảng cáo độc hại chạy trên các trang web phổ biến như Facebook và Disney.

Virus này xâm nhập vào máy tính "âm thầm" chủ yếu thông qua các thư mục**% APPDATA%** và sau đó bắt đầu quét ổ đĩa cứng để tìm các tập tin mà nó nhắm đích đến. Một khi đã nắm danh sách các tập tin có thể mã hóa, nó sẽ bắt đầu quá trình của mình.

Điểm đáng chú ý nhất của CryptoWall lethal là khả năng chạy trên cả phiên bản hệ điều hành 32-bit và 64-bit.

Tuy nhiên, người dùng có thể "giảm bớt" sức ảnh hưởng của **CryptoWall** bằng cách thay thế tạm thời các tập tin sao lưu ổ đĩa cứng. Tất nhiên đây chỉ là giải pháp tạm thời chứ không phải là giải pháp vĩnh viễn, nhưng nó kéo dài thêm thời gian để bạn có thể áp dụng các giải pháp bảo mật khác.

4. Một số giải pháp bảo vệ bạn khỏi các cuộc tấn công của Ransomware

Virus Ransomware ngày càng phổ biến và trở nên đáng sợ. Do đó để tự bảo vệ mình khỏi các cuộc tấn công của Ransomware bạn nên thực hiện sao lưu máy tính thường xuyên, cập nhật các phiên bản hệ điều hành mới nhất và quan trọng nhất là "*đừng dại gì*" mà click chuột vào các tập tin được gửi từ các nguồn không rõ trên các tập tin đính kèm email.