7 loại ransomware bạn không ngờ tới

Bạn đang duyệt web, kiểm tra email thì một thông báo đột ngột hiện ra. Máy tính, dữ liệu của bạn bị khóa, mã hóa bởi ransomware. Bạn không thể truy cập cho đến khi trả tiền chuộc. Hầu hết mọi người đều biết quy trình thực hiện của một ransomware, đó là lý do tại sao những kẻ tạo ra ransomware luôn tìm cách tìm tòi và sáng tạo ransomware mới để khiến bạn phải trả tiền. Dưới đây là một số loại ransomware mới bạn nên biết.

1. Cerber ransomware

Nếu máy tính của bạn bị nhiễm Cerber ransomware (thường bị tấn công qua file đính kèm email được đặt dưới tài liệu Microsoft Office), dữ liệu của bạn sẽ bị mã hóa với mỗi file có đuôi mới là **.cerber**.

Lưu ý: Trừ khi bạn ở Nga hoặc Ukraina hoặc các quốc gia Liên Xô cũ khác như Armenia, Azerbaijan, Belarus, Georgia, Kyrgyzstan, Kazakhstan, Moldova, Turkmenistan, Tajikistan hoặc Uzbekistan, bạn sẽ không bị Cerber ransomware tấn công.

Bạn biết rằng mình bị Cerber tấn công khi nhận được thông báo trên màn hình máy tính. Ngoài ra, hướng dẫn về cách thanh toán sẽ có trong mỗi thư mục trong TXT và định dạng HTML. Ngoài ra, bạn có thể tìm thấy một file VBS (Visual Basic Script) để hướng dẫn bạn cách thanh toán. Ransomware này sẽ nói cho bạn biết cách trả tiền chuộc và giải mã dữ liệu.

2. PUBG Ransomware

Vào tháng 4 năm 2018, nhiều người đã thấy PUBG Ransomware thực hiện một cách tiếp cận khác để mã hóa máy tính của người dùng để đòi tiền chuộc. Thay vì yêu cầu tiền để mở khóa file, những coder đằng sau phần mềm độc hại kỳ lạ này cung cấp cho bạn hai sự lựa chọn:

- Chơi trò chơi điện tử GameUnknown's Battlegrounds (có giá 29,99 USD trên Steam).
- Chỉ cần dán mã những kẻ lừa đảo đã cung cấp trên màn hình của bạn.

Thực tế đây không phải là phần mềm độc hại, mặc dù nó có khả năng gây phiền toán và xuất hiện như một ransomware thực sự. PUBG Ransomware chỉ là một công cụ quảng cáo cho PlayerUnknown's Battlegrounds.

Có vẻ như ransomware này không phải xấu đúng không? Đúng vậy, nhưng nó mã hóa file và đổi đuôi file thành .pubg. Tóm lại, nếu thấy xuất hiện hai lựa chọn một là dán mã và mua game bắn súng, bạn nên chọn hành động thích hợp. Nếu đây là ransomware thực sự, bạn sẽ phải trả ít nhất 10 lần số tiền mua game đó. Tuy nhiên, đây là một trong những ransomware dễ giải quyết nhất.

3. Jigsaw ransomware

Ban đầu được biết đến với cái tên BitcoinBlackmailer, Jigsaw ransomware này có tên mới nhờ sự xuất hiện của Billy the Puppet.

Được phát hiện lần đầu tiên vào tháng 4 năm 2016, Jigsaw được phát tán thông qua email spam và các file đính kèm bị nhiễm ransomware. Khi kích hoạt, Jigsaw khóa dữ liệu của người dùng và hệ thống Master Boot Record (MBR), sau đó hiển thị thông báo đính kèm.

Đây thực chất là một mối đe dọa: nếu không trả tiền chuộc (bằng Bitcoin) trong vòng một giờ, một file sẽ bị xóa khỏi máy tính của bạn. Mỗi giờ trì hoãn, con số file bị xóa sẽ tăng lên và việc khởi động lại hoặc cố gắng chấm dứt quá trình sẽ dẫn đến 1000 file bị xóa. Các phiên bản mới của Jigsaw còn đe dọa sẽ công khai thông tin nhạy cảm của nạn nhân nếu họ không trả tiền.

4. Ranscam ransomware

Chúng ta đã quen thuộc với cách thức hoạt động của ransomware. Bạn bị nhiễm phần mềm độc hại mã hóa dữ liệu quan trọng hoặc toàn bộ máy tính, sau đó buộc bạn trả một khoản tiền để giải mã dữ liệu thông qua key giải mã.

Các ransomware thông thường sẽ như vậy nhưng Ranscam thì khác. Nó không mã hóa dữ liệu để lấy tiền chuộc mà dữ liệu của bạn sẽ bị xóa vĩnh viễn.

5. FLocker ransomware

Vào tháng 6 năm 2016, người ta đã phát hiện ra rằng FLocker ransomware (ANDROIDOS_FLOCKER.A) đã từng phát triển trên điện thoại và máy tính bảng Android. Những chiếc TV thông minh hỗ trợ Android đã được thêm vào danh sách các mục tiêu của nó.

Có thể bạn đã từng nghe về Flocker ngay cả khi bạn không biết tên của nó. Đây là một trong các loại ransomware hiển thị cảnh báo "thực thi pháp luật", thông báo bạn đã xem tài liệu bất hợp pháp này trên hệ thống. Ngoài ra, nó còn nhắm mục tiêu đến người dùng ở Tây Âu và Bắc Mỹ; thực tế là tất cả mọi người trừ những người ở Nga, Ukraina, hoặc bất kỳ quốc gia Liên Xô cũ nào khác.

Người bị hại được yêu cầu thanh toán thông qua iTunes voucher, đây thường là mục tiêu của kẻ lừa đảo và khi nhận được tiền, bạn sẽ nhận lại quyền kiểm soát điện thoại hoặc TV Android.

6. Ransomware giả mạo

Thật ngạc nhiên khi biết rằng có một số ransomware không thực sự làm điều gì cả. Không giống như PUBG Ransomware, những ransomware này đơn giản chỉ là quảng cáo giả mạo, tuyên bố có quyền kiểm soát trên máy tính của bạn.

Loại ransomware này rất dễ giải quyết nhưng "sức mạnh" của ransomware thực sự đã đủ để nó sinh lời. Nạn nhân trả tiền mà hoàn toàn không biết họ thực sự không cần làm điều đó vì dữ liệu của họ không bị mã hóa.

Kiểu tấn công của các loại ransomware này thường xuất hiện ở cửa sổ trình duyệt. Khi xuất hiện, bạn không thể đóng cửa sổ và thông báo "file của bạn đã bị mã hóa, hãy trả 300 USD bằng Bitcoin, đây là giải pháp duy nhất".

Nếu muốn kiểm tra xem ransomware bạn gặp có phải là thật không hay chỉ là lừa đảo, nhấn **Alt + F4** trên Windows và **Cmd + W** trên Mac. Nếu cửa sổ đóng, hãy cập nhật phần mềm diệt virus của bạn ngay lập tức và quét máy tính.

7. Cách ngụy trang của ransomware

Cuối cùng, hãy xem xét cách ransomware lừa dối nạn nhân qua ngoại hình của nó. Bạn đã biết rằng các file đính kèm email giả thường có ransomware. Trong trường hợp này, file đính kèm sẽ xuất hiện dưới dạng file DOC hợp lệ, gửi bằng email spam và yêu cầu đòi tiền, file đính kèm này chính là hóa đơn đòi tiền. Sau khi tải xuống, hệ thống của bạn bị tấn công.

Tuy nhiên có một cách ngụy trang khác, ví dụ, DetoxCrypto ransomware (Ransom.DetoxCrypto) mạo nhận phần mềm nổi tiếng Malwarebytes Anti-Malware với thay đổi tên nhỏ Malwerbyte. Ngoài ra còn có biến thể Cryptolocker mạo nhận là Windows Update.

Bạn nghĩ rằng mình đã biết hết các ransomware, nhưng không phải, hãy nghĩ lại đi. Những kẻ lừa đảo sẽ không dừng lại cho đến khi lấy được tiền của bạn và chúng luôn xuất hiện với kiểu dáng mới.

Nếu lo lắng về ransomware, hãy thử một số biện pháp phòng ngừa như thường xuyên sao lưu dữ liệu, cập nhật máy tính, tránh xa các file nghi ngờ và có đuôi lạ, sử dụng tính năng lọc mail, và chạy một số bộ bảo mật Internet.