TROJAN BẮT CÓC TỐNG TIỀN TÁI XUẤT GIANG HỒ

Sau mộ

Sau một thời gian tạm lắng, hacker lại đang quay lại với thủ đoạn âm hiểm: "bắt cóc" dữ liệu quan trọng bên trong máy tính để đòi tiền chuộc từ phía người dùng.

Chương trình Trojan Gpcode-AI âm thầm mã hóa dữ liệu bên trong ổ cứng của máy tính bị nhiễm trước khi chính thức đòi hỏi người dùng trả tiền để có chìa khóa giải mã. Phần mềm phá hoại này thậm chí còn tích hợp cả tính năng theo dõi bàn phím, được thiết kế để đánh cắp tài khoản ngân hàng và thẻ tín dụng của các nạn nhân.

Xảo quyệt hơn

"Gpcode-AI thuộc về họ Synowal, vốn được hacker sử dụng để đánh cắp mật khẩu và thông tin nhà băng. Tuy nhiên, biến thể này không chỉ hoàn thành xuất sắc công việc đó, mà nó còn tống tiền cả người dùng", ông Luis Corrons, Giám đốc Kỹ thuật của hãng bảo mật PandaLabs cho biết.

Một khi đã cài đặt vào hệ thống, Gpcode-AI sẽ mã hóa mọi tài liệu lưu trong ổ cứng máy tính và tạo ra một file có tên "read_me.txt" (Hãy đọc đi).

Nguồn: SecurityLabs

Nội dung của file này thông báo cho nạn nhân rằng máy tính của họ đã bị mã hóa bằng thuật toán RSA-4096. "Muốn tự giải mã, bạn sẽ phát mất ít nhất là vài năm. Toàn bộ các thông tin riêng tư trong vòng 3 tháng gần đây của bạn sẽ được tập hợp và gửi lại cho tôi".

Tất nhiên, không thể thiếu phần yêu cầu và ra giá của hacker. "Để giải mã dữ liệu, bạn cần phải mua phần mềm của chúng tôi. Giá của nó là 300 USD".

Phía dưới là địa chỉ email để nạn nhân liên hệ. Trong mọi trường hợp, thủ phạm luôn nắm đằng chuôi vì chúng ra điều kiện rằng "giao dịch thành công thì mới gửi công cụ giải mã" cho nạn nhân, đồng thời thông tin riêng sẽ được xóa khỏi cơ sở dữ liệu của hacker.

Cuối cùng là một dòng dằn mặt: "Nếu không liên hệ trước ngày 15/7/2007, toàn bộ thông tin nhạy cảm của bạn sẽ bị phát tán rộng rãi và bạn sẽ mất tất cả dữ liệu".

Tuy nhiên, theo các chuyên gia của PandaLabs thì những lời dọa nạt này chỉ là giả. Trên thực tế, Gpcode-AI thiếu một cơ chế để xóa toàn bộ các file đã bị mã hóa và thủ phạm chỉ dùng đòn tâm lý để ép nạn nhân đưa tiền nhanh cho chúng mà thôi.

Chiêu bài tâm lý

Tuy nhiên, những lời tuyên bố hùng hồn về thuật toán mã hóa của bọn chúng thì cũng không phóng đại lắm.

"Thuật toán bọn chúng sử dụng rất phức tạp. Nạn nhân khó lòng tự giải mã được nếu không có phần mềm của chúng hoặc sự trợ giúp từ các chuyên gia bảo mật. Tuy nhiên, con Trojan này sử dụng phiên bản cải biên của RC4 chứ không phải RSA-4096 như lời chúng nói", một chuyên gia khác của Kaspersky Labs cho biết.

Theo khuyến cáo của các chuyên gia, nạn nhân không nên trả tiền cho thủ phạm bởi điều đó chỉ càng khuyến khích chúng phạm tội thêm mà thôi. Các hãng bảo mật đang tích cực nghiên cứu những công nghệ vừa chặn được phần mềm bắt cóc tống tiền, vừa khôi phục được dữ liệu đã bị khóa.

Lấy thí dụ, Kaspersky Labs đã phát triển được một thuật toán giải mã và sẽ sớm bổ sung nó vào cơ sở dữ liệu chống virus của hãng.

Trên thực tế, phần mềm tống tiền không phải là ý tưởng mới. Trước đây đã từng có Ransom-A đe dọa cứ 30 phút lại xóa một file dữ liệu nếu như nạn nhân không chịu trả tiền cho hacker.

Một loại malware khác là Arhiveus-A lại ép nạn nhân phải mua thuốc từ một website bán thuốc trực tuyến thay vì đòi tiền trực tiếp.

Trọng Cầm