ĐÁNH CẮP TÀI KHOẢN NGÂN HÀNG BẰNG TROJAN

Một nh

Một nhóm hacker đã đánh cắp các tài khoản ngân hàng tại 4 quốc gia bằng cách sử dụng những Trojan hết sức tinh vi được xây dựng riêng cho mục đích lừa đảo lấy các thông tin trên mạng.

Đặc tính nổi bật nhất của những Trojan này là khả năng bắt chước các thao tác chủ tài khoản thực hiện để rút tiền. Don Jackson, chuyên gia nghiên cứu bảo mật cao cấp tại SecureWorks Inc., cho biết: "Nó không phát tán rộng rãi, nhưng lại vô cùng nguy hiểm. Nó đã lấy đi hơn 200.000$ từ những tài khoản chúng tôi giám sát, và vượt qua tất cả mọi chương trình phòng chống".

Loại Trojan mới này có tên là Prg Banking, và đã đánh cắp hàng trăm ngàn tài khoản từ những ngân hàng lớn nhất ở Mỹ, Anh, Tây Ban Nha và Ấn Độ. Jackson cũng cho biết ông đã phát hiện ra ít nhất 4 máy chủ chứa các file định dạng Prg và những phiên bản ma của những ngân hàng hợp pháp, cũng như cache những thông tin thu thập được bởi Trojan.

Tài khoản ngân hàng là mục tiêu chính của Trojan Prg

Những kẻ tấn công thực sự thông minh và điêu luyện đến kinh ngạc. "Bạn sẽ không thể phân biệt được đâu là giao dịch thực hiện bởi Trojan và đâu là giao dịch thực hiện bởi con người", Jackson nói. Cũng theo Jackson, những hacker này đã khai thác dữ liệu thu thập từ trước bởi một phiên bản Trojan Prg yếu hơn để định vị các tài khoản ngân hàng, bao gồm URL cụ thể của những ngân hàng hoặc chỉ dẫn của các giao dịch. Chúng nhắm vào các tài khoản ngân hàng vừa bởi những tài khoản này có số dư lớn và thường được tích hợp khả năng thực hiện các giao dịch trực tuyến. Một khi chúng đã xâm nhập được vào tài khoản, hacker chúng có thể nhanh chóng lấy tiền bằng cách chuyển vào tài khoản chúng kiểm soát.

Sau khi lựa chọn được nạn nhân, những hacker sẽ sử dụng hình thức lừa đảo lấy thông tin qua

mạng hết sức thuyết phục và gửi chúng đến chủ sở hữu tài khoản đã được xác định dựa trên dữ liệu ăn cắp trước đó. “Chúng thường bao gồm số tài khoản, họ và tên của chủ sở hữu, cũng như những chi tiết bảo mật khác của tài khoản. Hacker sẽ yêu cầu người sử dụng "download" một mật khẩu mới, nhưng đường link sẽ dẫn vào trang do hacker tạo ra, và Trojan Prg sẽ được tự động tải xuống. Với khả năng bắt chước các thao tác trên bàn phím, Trojan sẽ chuyển khoản số tiền trong các tài khoản bị đánh cắp đến một tài khoản khác."

“Đây thực sự là một phần rất thông minh của Trojan”, Jackson nhận xét. “Cái cách nó tải JavaScript từ máy chủ ra lệnh-và-điều khiển chẳng khác gì một con người. Những trojan kém tinh vi hơn thường đi thẳng đến trang chuyển khoản, chứ không đi qua những trang mà một người thực sự sẽ phải ghé thăm trước khi đến được trang để chuyển khoản, như Prg có thể làm. Bởi vì hầu hết các chương trình chống gian lận chỉ có tác dụng với những hành vi tự động, chúng trở nên vô hiệu trước Prg.”

“Cho đến lúc này đã có gần 20 ngân hàng bị tấn công, nhưng đây đều là những ngân hàng lớn ở Mỹ, Anh, Tây Ban Nha và Ý.” Jackson cũng tỏ ý khen ngợi tài năng của những kẻ phạm tội.

Cách tốt nhất để bảo vệ mình trước Trojan Prg, Jackson kết luận, đó là cảnh giác với bất kỳ email nào từ ngân hàng: “Ngay cả khi bạn biết người gửi đến, bạn cũng nên chắc chắn rằng người đó gửi bức thư trước khi click vào bất cứ link nào.”

K.Huyền