XUẤT HIỆN TROJAN ĂN CẮP TỰ HUỶ

Tin tặc vừa tung lên mạng một loại trojan mới nhắm mục tiêu tấn công ăn cắp thông tin tài khoản ngân hàng của người sử dụng máy tính. Con trojan Briz-F được xem là một loại trojan rất phức tạp được "cấy" vào các trang web phát tán hình ản

Tin tặc vừa tung lên mạng một loại trojan mới nhắm mục tiêu tấn công ăn cắp thông tin tài khoản ngân hàng của người sử dụng máy tính. Con trojan Briz-F được xem là một loại trojan rất phức tạp được "cấy" vào các trang web phát tán hình ảnh khiêu dâm hoặc lợi dụng các lỗ hổng trong các phần mềm để khởi động một cuộc tấn công với mức độ phức tạp khá cao lên các hệ thống PC mắc lỗi. Mặc dù tính năng chính của cuộc tấn công qua trojan Briz-F là "drive-by download", cho phép con trojan này tải về các đoạn mã nguy hiểm lên hệ thống của nạn nhân thông qua chia sẻ tệp tin ngang hàng, Internet … Cách thức vận hành của trojan Briz-F là tương đối phức tạp. Rất nhiều tệp tin của con trojan này được cài đặt lên hệ thống bị nhiễm có khả năng tự phá huỷ mỗi khi thực hiện xong nhiệm vụ của mình khiến việc nhận biết cuộc tấn công trở nên rất khó khăn. Một số tệp tin còn có khả năng vô hiệu hoá các phần mềm bảo mật. Riêng tệp tin ieschedule.exe lại có nhiệm vụ gửi các thông tin trên hệ thống bị nhiễm như tên, địa chỉ IP, vị trí … tới một địa chỉ đặt trước của kẻ tấn công. Trong khi đó, phần mềm độc hại này còn tải về các tệp tin khác – ví dụ tệp tin ieredir.exe có khả năng chuyển địa chỉ truy cập của vào một dịch vụ trực tuyến bất kỳ, đặc biệt là các dịch vụ ngân hàng trực tuyến, về một trang web giả mạo. Phần mềm độc hại còn có khả năng thu thập thông tin nằm trong Windows Protected Storage hay các phần mềm như Outlook, Eudora và The Bat để gửi về cho kẻ tấn công.

Hãng bảo mật Panda Software cho rằng sự xuất hiện của cuộc tấn công này là hậu quả của các trò lừa đảo trực tuyến và việc phát tán kinh doanh cho phép chỉnh sửa con trojan Briz. Luis Corrons, giám đốc PandaLabs, khẳng định tính năng đặc điểm của con trojan Briz cho thấy tác giả của những trò lừa đảo trực tuyến đã quyết định chuyển sang mục tiêu kiếm lời từ việc tinh chỉnh các con trojan, thiết lập một hệ thống cho phép mua bán và tạo ra các phần mềm độc hại.

Hoàng Dũng