CẢNH BÁO VỀ MỘT DÒNG TROJAN LỪA ĐẢO MỚI

Các chuyên gia bảo mật vừa phát hiện một con trojan mới sử dụng một thủ tục giao tiếp khác với các loại phần mềm độc hại khác để gửi dữ liệu đi nhằm tránh bị phát hiện. Con trojan "chưa được đặt tên" gửi các thông tin ăn cắp được về cho kẻ phát tán th&

Các chuyên gia bảo mật vừa phát hiện một con trojan mới sử dụng một thủ tục giao tiếp khác với các loại phần mềm độc hại khác để gửi dữ liệu đi nhằm tránh bị phát hiện. Con trojan "chưa được đặt tên" gửi các thông tin ăn cắp được về cho kẻ phát tán thông qua thủ tục ICMP (Internet Control Message Protocol) thay vì email hoặc thủ tục HTTP như các loại phần mềm độc hại khác. Sau khi lây nhiễm thành công lên hệ thống, con trojan sẽ giả mạo là một đối tượng Internet Explorer Browser Helper Object (BHO) và chờ đợi để ăn cắp các thông tin nhạy cảm của người dùng khi họ nhập vào các form mẫu trên các trang web. Và thay vì gửi dữ liệu đi qua con đường email hoặc HTTP POST, con trojan mã hoá những dữ liệu ăn cắp được và sử dụng một thuật toán đơn giản XOR trước khi đưa các dữ liệu vào trong phiên làm việc gói dữ liệu PING ICMP để gửi đi. Trong con mắt của các nhà quản trị mạng và các thiết bị lọc dữ liệu thì các gói tin ICMP có vẻ như là những gói tin hợp pháp. Tuy nhiên, trên thực tế đó lại là các thông tin cá nhân của người dùng đã được mã hoá. Kẻ phát tán con trojan sẽ thu nhận những gói tin đó và giải mã từ một máy chủ ở xa. Chúng sẽ có được cái mà chúng mong muốn. Đây là loại trojan đầu tiên sử dụng thủ tục này để gửi dữ liệu đi. Nó là minh chứng cho thấy các phần mềm độc hại đang ngày càng trở nên nguy hiểm hơn. Hoàng Dũng