LẠI XUẤT HIỆN MÃ ĐỘC CHUYÊN "BẮT CÓC" PC

Mới đây Symantec cảnh báo về sự xuất hiện của một phần mềm độc hại BOT mới tấn công vào hàng loạt lỗi bảo mật trong các sản phẩm của Microsoft và của chính Symantec.

Spybot.acyr chứa mã độc tấn công tới 7 lỗi bảo mật khác nhau. Trong đó có 5 lỗi bảo mật thuộ
Mới đây Symantec cảnh báo về sự xuất hiện của một phần mềm độc hại BOT mới tấn công vào hàng loạt lỗi bảo mật trong các sản phẩm của Microsoft và của chính Symantec.

Spybot.acyr chứa mã độc tấn công tới 7 lỗi bảo mật khác nhau. Trong đó có 5 lỗi bảo mật thuộc hệ điều hành Windows của Microsoft và một lỗi trong ứng dụng chống virus doanh nghiệp của Symantec.

Symantec khẳng định lỗi bảo mật bị Spybot lợi dụng để tấn công PC người dùng đã được hãng này khắc phục từ hồi tháng 5.

Còn trong 5 lỗi bảo mật thuộc về hệ điều hành Windows có cả những lỗi đã được phát hiện và khắc phục 3 năm trước đây và có cả những lỗi vừa được phát hiện và khắc phục trong tháng 8 năm nay.

"Trong thời điểm hiện tại chúng tôi ghi nhận được luồng dữ liệu đi qua cổng 2967 tăng lên một cách bất thường. Tình trạng này xảy ra nhiều nhất với các tên miền của Châu Âu - tên miền .eu," Symantec cho biết.

SANS Institute of Internet Storm Center cũng ghi nhận được sự bất thường nói trên đồng thời phát hiện ra một con trojan backdoor cũng lợi dụng tấn công các hệ thống chưa được cài đặt đầy đủ các bản vá lỗi.

Symantec khuyến cáo người dùng nên nhanh chóng cài đặt các bản vá lỗi càng sớm càng tốt. Nếu chưa thể cài đặt nên nên chặn mọi đường ra dữ liệu qua cổng 2967.

Phần mềm BOT là một dạng phần mềm độc hại được tin tặc phát tán nhắm mục tiêu tấn công PC người dùng thông qua các lỗi bảo mật. Mục đích cuối cùng của bọn tin tặc là chiếm quyền điều khiển PC mắc lỗi từ xa - hay nói nôm na là "bắt cóc" PC đó - để xây dựng nên mạng lưới các PC rộng khắp phục vụ cho việc gửi thư rác hoặc để tấn công bất kỳ mục tiêu nào trên mạng Internet.

Dấu hiệu nhận biết PC bị nhiễm phần mềm BOT là tốc độ PC và tốc độ đường truyền Internet sẽ bị chậm đi rất nhiều. Người dùng nên thường xuyên cập nhật ứng dụng bảo mật trên hệ thống nhằm chống lại những hiểm hoạ nói trên.

Hoàng Dũng