SÂU PC Ổ ẠT TẤN CÔNG SYMANTEC ANTIVIRUS

Các ch

Các chuyên gia bảo mật cảnh báo người dùng Symantec Antivirus nên nhanh chóng cài đặt các bản vá lỗi cần thiết nếu không PC của họ sẽ trở thành mồi ngon cho một loại sâu máy tính mới xuất hiện.

Symantec trước đó đã phản bác thông tin về vụ tấn công bằng sâu máy tính này. Tuy nhiên, không lâu sau đó vụ tấn công này đã được chứng thực và hãng bảo mật đã phải thừa nhận sự tồn tại của nó.

Vụ tấn công nhắm mục tiêu đến các PC chạy Symantec Client Security và Symantec AntiVirus Corporate Edition phiên bản cũ thông qua một lỗi bảo mật đã được Symantec vá từ 7 tháng trước đây.

Một khi đã lây nhiễm, con sâu sẽ biến hệ thống trở thành một Zombie PC. Hay nói một cách khác PC của người dùng đã bị kẻ chủ mưu vụ tấn công bắt cóc và biến nó trở thành công cụ đắc lực của chúng trong các chiến dịch tấn công spam hoặc bất kỳ một mục đích nào khác.

Phần mềm Norton Antivirus không là mục tiêu của vụ tấn công này.

"Đó là một biến thể mới của con sâu Spybot. Nó đã xuất hiện và hoành hành kể từ tháng 12 năm ngoái cho đến nay," Vincent Weafer - Giám đốc Nhóm phản ứng nhanh với các vấn đề bảo mật của Symantec - cho biết. "Đây có thể xem là phiên bản Spybot nguy hiểm nhất".

Biến thể Spybot mới đột nhập vào PC thông qua một lỗi bảo mật đã được vá trong ứng dụng Symantec Antivirus. Khi đã đột nhập vào hệ thống con sâu này sẽ kết nối PC đến một máy chủ Internet Relay Chat nhằm cho phép kẻ chủ mưu vụ tấn công có thể điều khiển được PC đó từ xa.

Phiên bản Spybot đầu tiên tấn công Symantec Antivirus được phát hiện trong tháng 11 năm ngoái. "Chúng tôi biết chắc là Spybot tồn tại đâu đó trên Internet và đang liên tục tấn công khách hàng của chúng tôi. Các vụ tấn công bắt đầu bùng nổ mạnh mẽ kể từ ngày 20/12/2006," ông Weafer cho biết.

Ngày 25/5/2006, Symantec đã phát hành bản cập nhật bảo mật để vá lỗ hổng đã bị Spybot lợi dụng. Tuy nhiên, không phải hầu hết người dùng ứng dụng Symantec đều đã cài đặt đầy đủ bản

vá lỗi này. Một phần là do Symantec không phát hành bản vá lỗi qua tính năng tự động cập nhật. Người dùng phải lên trang web của hãng và tải về bản vá lỗi. Symantec đang cân nhắc thay đổi chính sách này.

Hãng bảo mật khuyến cáo người dùng nên nhanh chóng cài đặt các bản vá lỗi càng sớm càng tốt.

Hoàng Dũng