MICROSOFT: "HÃY CẨN THẬN VỚI TROJAN CỔNG SAU"

Rất nhiều hệ thống PC chạy hệ điều hành Windows đã bị bọn tin tặc biến thành các "zombie" trong khi đó rootkit lại không lan tràn mạnh đến như vậy. Microsoft đã đưa ra con số thống kê cho thấy có tới hơn 60% các hệ thống PC chạy Windows đã được phát h

Rất nhiều hệ thống PC chạy hệ điều hành Windows đã bị bọn tin tặc biến thành các "zombie" trong khi đó rootkit lại không lan tràn mạnh đến như vậy. Microsoft đã đưa ra con số thống kê cho thấy có tới hơn 60% các hệ thống PC chạy Windows đã được phát hiện là có nhiễm phần mềm "bot" độc hại khi được quét bằng công cụ Windows Malicious Software Removal Tool. Công cụ của Microsoft đã gỡ bỏ ít nhất một phiên bản các phần mềm cho phép điều khiển hệ thống từ xa trên khoảng 3,5 triệu PC. "Trojan cổng sau là những mối đe doạ hữu hình thực sự đối với người sử dụng các hệ thống PC chạy hệ điều hành Windows," Microsoft khẳng định. Các PC bị lây nhiễm các loại trojan - hay thường được biết đến với tên gọi "zombie PC" - có thể được sử dụng để xây dựng nên các hệ thống "bot" - còn gọi là "botnet" - phục vụ mục đích cho việc gửi spam hoặc khởi động các vụ tấn công. Không những thế, tin tặc còn có thể ăn cắp được các thông tin trên chính hệ thống "zombie PC" hoặc cài đặc phần mềm gián điệp, phần mềm quảng cáo lên đó nhằm mục đích thu lợi từ phía những người lập trình sản xuất phần mềm spyware và adware. Microsoft chính thức ra mắt công cụ Windows Malicious Software Removal Tool trong năm ngoái. Hàng tháng Microsoft cũng đều cho nâng cấp phần mềm song hành cùng với bản cập nhật bảo mật. Công cụ nhằm mục tiêu xác định và gỡ bỏ mọi phần mềm độc hại trên hệ thống của người dùng. Kể từ ngày xa mắt đến nay, công cụ này đã vận hành khoảng 2,7 tỉ lần trên 270 triệu hệ thống. Trong hơn 15 tháng hoạt động, công cụ này đã phát hiện ra tổng cộng 5,7 triệu hệ thống chạy hệ điều hành Windows bị nhiễm phần mềm độc hại và gỡ bỏ 16 triệu phần mềm độc hại trên những hệ thống này. Backdoor trojan là mối hiểm hoạ phổ biến nhất. Tiếp theo là sâu máy tính phát tán qua email - thống kê cho thấy loại hình hiểm hoạ bảo mật này được phát hiện trên hơn 1 triệu hệ thống PC. Trong khi đó, rootkit chỉ mới được phát hiện và loại bỏ trên 780.000 hệ thống PC. Rookit là một mối hiểm hoạ bảo mật tiềm tàng đang nổi lên nhưng mà vẫn chưa đạt được mức độ phổ biến rộng, Microsoft kết luận. Điều này lại hoàn toàn trái ngược với nghiên cứu của hãng bảo mật McAfee trong tháng 4 vừa qua khi mà hãng này khẳng định số lượng rootkit đang gia tăng một cách vô vùng mạnh mẽ. Windows Malicious Software Removal Tool mới chỉ phát hiện được rookit trên 14% trong tổng số 5,7 triệu hệ thống PC có lây nhiễm phần mềm độc hại. Và trong khoảng 20% số lượng trường hợp nhiễm rootkit thì cũng đồng thời nhiễm luôn backdoor trojan. 5 mối hiểm hoạ bảo mật hàng đầu mà Microsoft đưa ra là bot, Sdbot, Parite, Gaobot và FURootkit.

Hoàng Dũng