NHỮNG CON SỐ GIẬT MÌNH VỀ PHẦN MỀM PHÁ HOẠI

Nhiều máy tính Windows đã bị biến thành thây ma (zombie), nhưng rất may là rootkit chưa thật phổ biến. Một phát hiện khiến người ta giật mình là cứ sau 311 lần scan hệ thống, công cụ bảo mật của hãng - Windows Malicious Software Removal Tool (WMSRT), lại phát hiệ

Nhiều máy tính Windows đã bị biến thành thây ma (zombie), nhưng rất may là rootkit chưa thật phổ biến. Một phát hiện khiến người ta giật mình là cứ sau 311 lần scan hệ thống, công cụ bảo mật của hãng - Windows Malicious Software Removal Tool (WMSRT), lại phát hiện thấy một máy tính dính phần mềm độc hại (malware). Những dữ liệu mà Microsoft công bố rất đáng chú ý, bởi nó được thu thập từ hơn ... 270 triệu khách hàng đang dùng WMSRT- công cụ được phát hành kèm với hệ điều hành Windows.

Nguồn: SecurityLabs

Trong khoảng thời gian từ tháng 1/2005 đến tháng 3/2006, WMSRT đã loại bỏ được hơn 16 triệu phần mềm phá hoại các loại bên trong 5,7 triệu máy tính. Nó đã được sử dụng để quét hệ thống 2,7 tỷ lần và phát hiện được "gương mặt khả nghi" với tỷ lệ 0,32%, tức là tương đương với 1/311 lần quét. Vài năm trở lại đây, không có đợt virus nào bùng phát thật sự mạnh mẽ, song người dùng lại phải đối mặt với hàng loạt nguy cơ khác như trộm danh tính, rootkit, phishing. Bản thân Microsoft nghĩ thế nào về thực tế này, rằng mọi chuyện đang được cải thiện hay thực chất là tồi tệ hơn? "Một câu hỏi thật khó trả lời", Matthew Braverman, giám đốc bộ phận chống malware của Microsoft nhún vai. Braverman lưu ý rằng ghi được một bức tranh toàn cảnh về nhất cử nhất động của kẻ xấu là chuyện "bất khả thi", nhưng có vẻ như tình hình cũng khả quan hơn đôi chút. Trong suốt 15 tháng theo dõi, Microsoft nhận thấy số lượng malware phát tán đã giảm từ 53 họ sâu, rootkit và virus các loại xuống còn 41. Và thực ra, con số 21 biến thể cũng là cả một "tiến triển" lớn, giảm tới 71% so với cách đây 2 năm. "Rõ ràng là vấn đề malware đã trở nên sáng sủa hơn", Braverman nói. Trojan - mối nguy phổ biến nhất Trojan cửa sau chính là nguy cơ đáng kể nhất, hiển hiện nhất đối với người dùng Windows, Microsoft khẳng định. Sau khi dính Trojan cửa sau, máy tính có thể bị hacker giành lấy quyền kiểm soát và biến thành zombie bất cứ lúc nào. Nhiều zombie hợp thành một botnet và đây chính là công cụ để hacker "điều binh khiển tướng", thực hiện các phi vụ của chúng. Chưa hết, hacker còn đánh cắp thông tin cá nhân của người dùng, cài đặt spyware và adware lên máy nhằm kiếm thêm thù lao từ phía các nhà quảng cáo. Sau Trojan là sâu email - chúng đã được phát hiện và loại bỏ ra khỏi hơn 1 triệu máy tính. Hình thức tấn công trong đó nạn nhân bị lừa chạy malware là dạng phổ biến nhất. Sâu phát tán qua email, mạng P2P và phần mềm chat IM chiếm tới hơn một phần ba số máy tính mà công cụ của Microsoft quét được. Rootkit- mối nguy chưa lộ mặt

Nguồn: SecurityLabs

Tuy nhiên, không phải malware nào mà nhóm của Braverman phát hiện được cũng xuất phát từ hacker. Thí dụ điển hình nhất chính là phần mềm rootkit "lừng danh" của Sony BMG Music. Rootkit này đã được tìm thấy trên 420.000 lần và được cài đặt trên hơn 250.000 máy tính. Điều này cho thấy nhiều người dùng đã ... cài đặt lại rootkit này sau khi xóa chúng ra khỏi máy. Sau vụ bê bối này, Sony đã buộc phải thu hồi hàng triệu đĩa CD có cài phần mềm rootkit nói trên. Mọi việc càng trở nên tệ hơn khi hacker bắt đầu khai thác rootkit này để phát tán phần mềm phá hoại. Microsoft nhận định xu hướng rootkit bắt tay cùng các dạng malware khác sẽ còn tiếp diễn và gia tăng trong thời gian tới. Họ phát hiện thấy rootkit trong 14% máy tính bị nhiễm sâu, virus, Trojan các loại. WMSRT hiện có phiên bản bằng 24 thứ tiếng, dành cho người dùng Windows 2000, Windows XP và Windows Server 2003. Phiên bản mới nhất có khả năng phát hiện và loại bỏ 61 họ malware khác nhau. Bạn có thể truy cập và cài đặt nó từ website của Microsoft. Thiên Ý