

2007: TROJAN SIÊU TÍNH VI SẼ HOÀNH HÀNH DỮ DỘI

Kỹ thu

Kỹ thuật cực kỳ tinh vi mà loại Trojan này sử dụng sẽ trở nên phổ biến trong năm 2007, một chuyên gia bảo mật cảnh báo.

Được đặt tên là "Rustock", họ Trojan của sau này xuất hiện lần đầu tiên cách đây gần một năm. "Kỹ thuật mà Rustock sử dụng sẽ trở thành nền tảng cho các malware trong tương lai. Những kẻ tấn công đang kiểm tra xem kỹ thuật nào có hiệu quả để nhân rộng mô hình. Chính vì thế, chúng tôi dự đoán Rustock sẽ tràn ngập trong thời gian tới", chuyên gia Patrick Martin của Symantec cho biết.

Một đặc điểm nổi bật của Rustock và việc nó dựa dẫm rất nhiều vào các công cụ rootkit hiện đại để ẩn mình trước các phần mềm bảo mật. Ngoài ra, nó còn có khả năng thay đổi giống như tắc kè hoa mỗi khi lây nhiễm một file nào đó.

"Bất cứ một malware nào cũng phải tìm cách xâm nhập hệ thống, bám trụ và tải về máy bất cứ thứ gì mà tác giả của nó chỉ định", Martin nói, vạch ra ba nhiệm vụ quan trọng nhất của mọi loại phần mềm phá hoại. Theo ông, Rustock hội đủ cả 3 "đức tính" này với trình độ cực cao.

Siêu tinh vi

Nguồn: Techtree

Ngay khi đặt được một chân vào trong hệ thống, nó sẽ đào bới cật lực để chui sâu vào bên trong. Càng né tránh tốt các công cụ bảo mật, thời gian tồn tại của Trojan trong máy tính càng lâu và nó càng mang về nhiều lợi nhuận cho chủ nhân.

Cũng giống như nhiều loại Trojan đang nổi đình nổi đám khác, Rustock được thiết kế để phát tán thư rác từ mạng máy tính Zombie. "Chuyên môn" của nó là thư rác có hình, vấn nạn đã tăng đột biến về số lượng trong suốt 2 tháng 10 và 11 vừa qua.

Rustock "dính" vào lõi 32-bit của Windows và bịt lại một số API (Giao diện lập trình ứng dụng) để che giấu mã registry mới cũng như những file mà nó cài đặt vào máy tính.

Bên cạnh đó, nó còn được trang bị một số đặc tính của phần mềm phát hiện rootkit, khiến cho các công cụ bảo mật rất khó đánh hơi ra. Chưa hết, Rustock còn có khả năng thay đổi chức năng của một số bộ phận bên trong Windows để qua mặt tường lửa.

Rustock liên tục biến hình, đây là một kỹ thuật hacker rất thông dụng trước đây. "Nó giống như một nhạc chuông đa âm sắc vậy", có nghĩa là trong khi thuật toán gốc vẫn còn nguyên vẹn thì phần mã thể hiện chúng lại thay đổi mỗi khi lây nhiễm được một file mới.

Trọng Cẩm