TROJAN, HIỂM HỌA AN NINH TÀI CHÍNH

Photo: Fotosearch

Photo: Fotosearch

Tội phạm công nghệ sẽ online cùng bạn trong các cuộc giao dịch để đánh cắp tiền. Lời cảnh báo của các chuyên gia về một thực trạng mới đáng lo ngại trong an ninh giao dịch tài chính.

Các Trojan ăn cắp tài khoản đang hoạt động rất dữ dội. Phần mềm này sẽ ẩn mình trên máy tính của bạn ngay sau khi bạn mở một file đính kèm trong e-mail hoặc viếng thăm một website có mã độc. Thế nhưng, thay vì để được "thừa nhận" bởi các chế độ kiểm soát và chứng thực ngày càng gắt gao, các tội phạm công nghệ đang có xu hướng thay đổi chiến lược hoạt động của mình. Ông Alex Shipp, chuyên gia "lão làng" về công nghệ chống virus của MessageLabs, phát biểu tại buổi thảo luận ở hội nghị RSA 2006 (16-2): "Chúng tôi nhận thấy một xu hướng dịch chuyển từ việc ăn cắp tài khoản và mật mã của bạn. Các loại Trojan mới sẽ đợi cho đến khi nạn nhân, tức là bạn, đã đăng nhập hoàn toàn vào tài khoản ngân hàng của mình, sau đó chuyển tiền ra ngoài. Chính vì thế, tất cả các biện pháp chứng thực, những tiểu thuật nào là mật mã hình ảnh, sinh trắc học không còn là vấn đề lớn đối với họ nữa. Những kẻ xấu chỉ việc đợi lúc bạn hoàn tất việc đăng nhập là đã có thể tấn công". Loại Trojan mới này đang trên đà phát triển dữ dội, hiện đang đứng ở vị trí thứ ba trong danh sách những mối nguy hiểm thường trực của MessageLabs. Đứng đầu trong danh sách này là điều khiển từ xa bằng các mã độc, biến một máy tính hoặc một mạng máy

tính thành các Zombie PC (các máy tính bị kiểm soát và điều khiển từ xa bởi các hacker, trở thành trung tâm phát tán thư rác, quảng cáo hoặc để tấn công các máy tính khác). Đứng vị trí thứ hai chính là các trò lừa đảo lấy tài khoản tài chính của người dùng, thường gọi là phising scams, như nặc danh website ngân hàng, người thân của bạn... Hạn chế của loại Trojan mới này là chỉ hoạt động chuyên biệt với tài khoản của một ngân hàng nhất định. Tuy nhiên, danh sách ngân hàng hiện ngày càng nhiều hơn. Các loại Trojan trong nhóm này thường lây nhiễm vào máy qua con đường email, với các liên kết nếu nhìn sơ qua thì có vẻ vô hại, ví dụ một thiệp online, thậm chí một lời quảng cáo mang ý nghĩa từ thiện. Tuy nhiên, nếu bạn có lỡ tay "sờ vào" nó, ngay lập tức, một chương trình mã độc đã âm thầm cài vào máy tính và không hề hoạt động cho đến khi bạn truy xuất vào ngân hàng. Sự phát triển của các hình thái tấn công là một thách thức rất lớn đối với khách hàng, ngay cả với các chuyên gia bảo mật như Jeanette Jarvis của Boeing. Ông cho biết, kể từ năm 2002, Boeing đã chứng kiến sự tăng trưởng 110 lần lượng mã độc mà họ chặn lại tại cổng kết nối vào mạng của họ. Ông Javis cho biết: "Ngay khi chúng tôi vừa có một chiến lược chống lại, họ đã có một kế hoạch và phương thức tấn công mới". Trong quá khứ, các hacker và nhà viết virus chủ yếu vì mục đích là danh tiếng hoặc là sự tai tiếng, thì ngày nay, mục đích tài chính xếp hàng đầu. Những kẻ tội phạm chuyên nghiệp cũng nhận thấy rằng, có lẽ tấn công trên mạng sẽ an toàn hơn là ăn cướp nhà băng với việc vượt qua những bức tường thép với súng ống vũ khí. Ông David Perry, giám đốc toàn cầu về giáo dục của hãng Trend Micro cho rằng, nền công nghiệp phải hướng tới việc tìm một giải pháp ngăn chặn hiểm họa "suy giảm lòng tin vào Internet" của khách hàng, nếu không Internet sẽ không còn mấy ý nghĩa đối với nền thương mại điện tử hiện hành. TRẦN HUY