THẾ HỆ SÂU MỚI "SIÊU CÔNG PHÁ" CÁC MẠNG IM

Hacker đã tạo ra được những loại sâu đủ khả năng xuyên phá mọi mạng chat IM hiện nay, trên cả nền tảng máy Mac lẫn PC, giới chuyên gia bảo mật vừa đưa ra cảnh báo.

Nguồn: SecurityLabs

Theo hãng bảo mật

Hacker đã tạo ra được những loại sâu đủ khả năng xuyên phá mọi mạng chat IM hiện nay, trên cả nền tảng máy Mac lẫn PC, giới chuyên gia bảo mật vừa đưa ra cảnh báo.

Nguồn: SecurityLabs

Theo hãng bảo mật Kaspersky, thời gian tới sẽ chứng kiến sự nhảy vọt của một thế hệ sâu IM mới có thể phát tán "xuyên mạng IM". Chúng sẽ hất cẳng hoàn toàn những loại sâu IM truyền thống như Bropia, Kelvia và Prex, vốn chỉ có khả năng lây lan trên một dịch vụ chat IM duy nhất, hoặc MSN, hoặc Yahoo, hoặc AOL... Những con sâu IM như IRCBot.lo tiềm tàng một nguy cơ cực lớn, vì chúng có thể nhảy cóc từ mạng này sang mạng khác và sử dụng nhiều biến thể tin nhắn cùng đường link download khác nhau, khiến cho người dùng rất khó đề phòng. "Trong đa số trường hợp, sâu IM không thể được coi là một malware độc lập. Nói đúng hơn, nó giống như một "nô lệ", được sử dụng để giúp IRCBot phát tán mà thôi", chuyên gia Roel Schouwenberg của Kaspersky Lab cho biết. "Sự xuất hiện của IRCBot.lo cho thấy chức năng phá hoại của sâu IM đã đạt đến cấp độ thượng thừa và vô cùng sung sức". Điều đáng lo ngại nhất là đoạn mã của IRCBot.lo có thể được sao chép vô cùng dễ dàng, mà hệ quả là những con sâu IM "xuyên mạng" có thể sinh sản với tốc độ gà đẻ trứng. Schowenberg tin rằng những con sâu tinh vi như IRCBot.lo cũng báo hiệu sự tuyệt chủng của thế hệ sâu IM truyền thống. "Kể từ khi sâu IM xuất hiện lần đầu, đã có những thay đổi rất lớn trong phương thức phát tán, trong mức độ tinh vi của đoạn mã sử dụng và mục tiêu nhắm đến của chúng. Bên cạnh đó, những tin nhắn IM gửi đi không mệt mỏi của người dùng cũng giúp kéo dài vòng đời của các malware và botnet". Không chỉ có máy tính Windows yếu ớt trước sâu IM, máy tính Macs cũng gặp nguy hiểm không kém. Ngày 13/2/2006, loại sâu đầu

tiên ngắm bắn vào hệ điều hành Mac OS X đã được phát hiện : một sâu IM có tên OSX/Leap.A phát tán thông qua ứng dụng iChat. "Thị phần bé nhỏ của Apple trên thị trường máy tính toàn cầu đã giúp Macs thoát khỏi sự chú ý của malware. Tuy nhiên, càng ngày, hệ thống của Apple càng trở nên phổ biến hơn và chắc chắn, malware sẽ bắt đầu đổ bộ". Mặc dù OSX/Leap.a chỉ là một đoạn mã tấn công "proof-of-concept", song nó cũng đủ để chứng minh hệ điều hành Mac có lỗ hổng. "Và một khi phát hiện được sơ hở, nên nhớ rằng tác giả malware không bao giờ bó tay ngồi yên". Schowenberg cảnh báo. Trọng Cầm