# CUỘC CHIẾN BẢO MẬT BƯỚC SANG GIAI ĐOẠN MỚI

Tháng tám vừa qua, Webroot Software đưa ra một thông báo làm giới công nghệ thông tin phải giật mình: 90% máy vi tính bị nhiễm các loại phần mềm gián điệp (spyware). Hacker vẫn sử dụng virus, trojan, keylogger... nhưng cách thức và mục đích c&oacut

Tháng tám vừa qua, Webroot Software đưa ra một thông báo làm giới công nghệ thông tin phải giật mình: 90% máy vi tính bị nhiễm các loại phần mềm gián điệp (spyware). Hacker vẫn sử dụng virus, trojan, keylogger... nhưng cách thức và mục đích có phần khác trước. Cuộc chiến bảo mật đang bước sang một giai đoạn mới. Không có phần mềm nào hoàn hảo ngay từ khi được viết ra. Các hacker vẫn luôn biết cách tận dụng các lỗ hổng bảo mật trong phần mềm để tiến hành tấn công. Không khe hở nào không được hacker tận dụng, từ lỗi trong một phần mềm chat như ICQ đến một lỗ hổng trình duyệt Internet Explorer. Ngay cả lỗi bảo mật trong những phần mềm văn phòng như Microsoft Word cũng không thoát khỏi "tầm ngắm". Có rất nhiều phần mềm client-side (phần mềm chạy trên máy của người sử dụng dịch vụ Internet trong kiến trúc server client) để bọn hacker có thể tận dụng. Thư điện tử (email) và tin nhắn tức thời (IM-Instant Messages) là hai trong số những "mỏ vàng lộ thiên" của giới đạo chích trong thế giới số. Các công ty cung cấp dịch vụ qua Internet có thể "xây thành đắp lũy" để bảo vệ thông tin trên máy chủ của mình, nhưng không thể bảo vệ máy tính của khách hàng từ xa. Mà không phải ai sử dụng Internet cũng có đầy đủ kiến thức cần thiết về bảo mật. Thủ đoạn tấn công quen thuộc của hacker qua các phần mềm client-side là phishing. Hacker sẽ gửi cho nạn nhân một email hay một tin nhắn, kèm theo địa chỉ một website hay một file nào đó. Nếu nạn nhân mở file đó (hay click vào địa chỉ website) thì một phần mềm độc hại (malware - từ gọi chung cả virus, keylogger, trojan, spyware...) sẽ được cài tự động vào máy và thực hiện "sứ mệnh" mà nó được giao. Phần lớn các vụ tấn công kiểu này là nhằm đánh cắp thông tin cá nhân. Mã số thẻ tín dụng, mật mã tài khoản ngân hàng hay dữ liệu quan trọng đều rất giá trị với bọn hacker. Đặc biệt, dữ liệu quan trọng có thể trở thành "con tin" để bọn hacker thực hiện các vụ bắt cóc tống tiền. Nếu nạn nhân không chịu trả tiền chuộc, "con tin" sẽ bị... xóa.

Phishing không khó phòng chống, nhưng hacker vẫn thả sức tung hoành là vì ý thức cảnh giác của người sử dụng Internet còn quá thấp. Bằng chứng là sự kiện hàng loạt máy vi tính ở VN bị nhiễm virus qua Yahoo! Messenger cách nay chỉ ít ngày. Các virus này được thiết kế rất đơn giản (theo các chuyên gia, chỉ là "Việt hóa" mã nguồn virus được chia sẻ trên Internet) và thật ra cũng không gây nguy hiểm nhiều nhưng là hồi chuông cảnh báo đối với người sử dụng Internet không chỉ ở VN, nhất là khi các hacker đang bắt đầu một chiến thuật tấn công mới nguy hiểm hơn rất nhiều lần.

Phishing cũng là cách dân "mũ đen" thiết lập các botnet (mạng máy tính bị điều khiển) để phát động tấn công từ chối dịch vụ hoặc phát tán thư rác. Các máy tính sau khi bị nhiễm virus/trojan sẽ

bị biến thành zombie (máy tính bị điều khiển). Nhiều zombie hợp lại tạo thành botnet. Khi hacker ra lệnh, các zombie trong một botnet sẽ đồng loạt gửi yêu cầu đến máy chủ của một dịch vụ Internet, khiến nó bị "lụt" trong mớ bòng bong yêu cầu, cuối cùng là mất hoàn toàn khả năng xử lý. Theo tính toán, không có một máy chủ nào trụ được trước 30.000 zombie quá 30 phút nhưng ở thời kỳ đỉnh cao của phishing (năm 2003-2004), các chuyên gia phát hiện rất nhiều botnet có "quân số" trên 100.000. Tổng thiệt hại do tấn công từ chối dịch vụ trong hai năm 2003-2004 lên đến gần 40 tỉ USD với những "tên tuổi" như Blaster, MyDoom, Sasser, Sobig... Hiện nay, qui mô botnet đã giảm, nhưng đây không phải là điều đáng mừng. Các hacker không muốn bị lộ tẩy nên chuyển sang "đánh du kích" bằng những botnet nhỏ, khoảng dưới 20.000 zombie, tiếp tục gây thiệt hại nghiêm trọng. Mặc dù các hệ thống máy chủ được bảo vệ ngày một chắc chắn hơn, nhưng các phần mềm vẫn luôn có lỗ hổng. Một số lỗi trong Ajax và Javascript có thể giúp hacker tấn công, giành quyền kiểm soát mục tiêu từ xa. Một trong những nạn nhân đầu tiên là website Samsung Telecom. Tên tuổi Samsung có lẽ đủ để trấn an những người đa nghi nhất và hacker dễ dàng phát tán trojan dưới dạng các file chương trình vô hại. Trước khi Samsung kịp khắc phục sự cố thì cũng đã có không ít người mắc bẫy. Cuộc chiến bảo mật vẫn tiếp diễn và đã bước sang một giai đoạn khó khăn hơn đối với người sử dụng. Trong cuộc chiến này, phòng tránh vẫn là giải pháp tốt nhất và để phòng tránh được thì mỗi người dùng Internet cần phải đề cao cảnh giác. Khi nguồn cung cấp nước có cặn bẩn, người sử dụng không phải làm gì cả, công ty cấp nước sẽ giải quyết vấn đề. Nhưng khi Internet "nhiễm bẩn", khách hàng cũng phải "chiến đấu".