SÂU MÁY TÍNH MỚI: ĐƠN GIẢN ĐẾN KHÔNG NGỜ?

Các hãng bảo mật vừa mới cảnh báo về một loại sâu máy tính mới đang phát tán một cách vô cùng mạnh mẽ trên mạng Internet. Mặc dù mới chỉ bắt đầu xuất hiện trên mạng kể từ ngày thứ 3 (17/01) nhưng sang đến ngày hôm sau chủng loại s&acirc

Các hãng bảo mật vừa mới cảnh báo về một loại sâu máy tính mới đang phát tán một cách vô cùng mạnh mẽ trên mạng Internet. Mặc dù mới chỉ bắt đầu xuất hiện trên mạng kể từ ngày thứ 3 (17/01) nhưng sang đến ngày hôm sau chủng loại sâu máy tính mới này đã nhanh chóng leo lên chiếm lĩnh vị trí số 3 trên bảng xếp hạng các phần mềm nguy hiểm của các hãng bảo mật trên thế giới. Loại sâu máy tính mới này – có tên VB.bi theo cách gọi của hãng bảo mật F-Secure, Blackmal.e theo Symantec hay MyWife.d theo McAfee - thực chất chỉ là một cấu trúc mã lệnh Visual Basic (VB) rất đơn giản, hãng bảo mật F-Secure cho biết. Loại sâu này được phát tán theo con đường truyền thống - được đính kèm vào các bức thư điện tử. Tuy nhiên, loại sâu mới này cũng còn một con đường phát tán khác là thông qua các thư mục chia sẻ. Một khi đã lây nhiễm lên máy tính của người sử dụng loại sâu mới này sẽ nỗ lực vô hiệu hoá một loạt các ứng dụng bảo mật như các ứng dụng của Symantec, McAfee, Trend Micro, hay Kaspersky Labs Internet Storm Center (ISC) cho biết một trong những đặc điểm nổi bật của loại sâu máy tính mới này chính là khả năng tồn tại như là một tệp tin có thể tự thực thi hay là một tệp tin MIME có chứa một tệp tin tự thực thi khác. Đây là một hình thức tấn công phát tán vô cùng nguy hiểm mới do định dang MIME hiếm khi được các kẻ tấn công ác ý sử dụng để phát tán virus. Gần đây nhất mới chỉ có virus Nimda là có sử dụng phương thức này để phát động các cuộc tấn công trong năm 2001. Blackmal.e/VB.bit/MyWife.d đã nhanh chóng leo lên vị trí số 3 trên bảng xếp hạng các virus nguy hiểm nhất của F-Secure. Loại sâu này hiện đang chiếm tới hơn 11% trong tổng số các thông báo nhiễm virus được gửi về cho F-Secure chỉ trong vòng có 24 giờ đồng hồ. Virus Mytob có lẽ cũng chưa đạt được kỉ lục này. Symantec đã xếp mức độ nguy hiểm của loại virus này vào mức độ 2/5 trên bậc thang xếp hạng và đã chính thức cung cấp công cụ diệt trừ loại virus này miễn phí trên trang web của hãng. Bạn có thể tải về công cụ miễn phí này tại đây.