SÂU NYXEM.E 'TÀN SÁT' DỮ LIỆU THEO CHU KỲ

Cuối tuần qua, hãng bảo mật F-Secure đã cảnh báo người sử dụng về sự lan tràn của một loại sâu máy tính mới có tên là Nyxem.e với khả năng phá huỷ thông tin dữ liệu trong một số định dạng tệp tin phổ biến hiện nay. Hãng bảo mật có trụ sở chính tại

Cuối tuần qua, hãng bảo mật F-Secure đã cảnh báo người sử dụng về sự lan tràn của một loại sâu máy tính mới có tên là Nyxem.e với khả năng phá huỷ thông tin dữ liệu trong một số định dạng tệp tin phổ biến hiện nay. Hãng bảo mật có trụ sở chính tại Phần Lan này cho biết sâu Nyxem.e chứa các đoạn mã nguy hiểm có chức năng hướng dẫn nó thay thế dữ liệu trong các tệp tin như ".DOC, .XML, .MDB, .MDE, .PPT, .PPS, .ZIP, .RAR, .PDF, .PSD hay .DMP" bằng một chuỗi kí tự "DATA Error [47 0F 94 93 F4 K5]". Nhưng sự thay thế này còn nguy hiểm hơn khi nó lại được tiến hành theo đúng định kì vào ngày thứ 3 của mỗi tháng. Như vậy chúng ta có thể thấy loại virus này ảnh hưởng đến một loạt các ứng dụng phổ biến như Microsoft Word, Excel, PowerPoint, Access, Adobe PhotoShop và Acrobat. Sâu Nyxem.e là khá giống với chủng loại sâu VB.bi/Blackmal/MyWife.d mới được phát hiện gần đây - loại sâu mà chỉ trong 24 giờ kể từ khi xuất hiện đã leo lên tới vị trí số 3 trên bảng xếp hạng các loại virus nguy hiểm. Theo thống kê của F-Secure thì loại sâu mới này hiện chiếm 7% trong tổng số các thông báo virus gửi về cho hãng này. F-Secure đã phải quyết định nâng mức cảnh báo dành cho sâu Nyxem.e lên mức độ "2" – Đây là lần đầu tiên hãng bảo mật này sử dụng mức cảnh báo cao đến như vậy kể từ sau lỗi bảo mật Windows Metafile được phát hiện vào cuối năm ngoái.