HÃY CẨN THẬN VỚI TỆP TIN POWERPOINT HÀI HƯỚC

Microsoft đã chính thức khẳng định lỗi bảo mật mới được phát hiện trong MS PowerPoint và cho biết hãng sẽ phát hành bản vá vào ngày 8/8 tới đây. Trong một bản tin cảnh báo phát hành ngày hôm qua (17/7), Microsoft khuyến cáo người d&u

Microsoft đã chính thức khẳng định lỗi bảo mật mới được phát hiện trong MS PowerPoint và cho biết hãng sẽ phát hành bản vá vào ngày 8/8 tới đây. Trong một bản tin cảnh báo phát hành ngày hôm qua (17/7), Microsoft khuyến cáo người dùng không nên mở hoặc lưu trữ các tệp tin Microsoft Office không rõ nguồn gốc. Cảnh báo của Microsoft được đưa ra khi đã có một số vụ tấn công người dùng thông qua việc lợi dụng khai thác lỗi bảo mật nói trên. Tuy nhiên, cảnh báo của Microsoft đã ra chậm mất một tuần. Trước đó, lỗi bảo mật trong PowerPoint đã trở thành công cụ nuôi cấy một con trojan keylogger lây nhiễm lên các hệ thống Windows. "Tuy nhiên, các vụ tấn công chỉ có thể diễn ra nếu người sử dụng mở một tệp tin PowerPoint độc hại được gửi đi kèm theo các email hoặc bất kỳ một con đường nào khác," Microsoft khẳng định. "Vì thế khi chưa có bản vá khắc phục, người dùng nên thận trọng trong việc mở hoặc lưu trữ các tệp tin MS Office." Vụ tấn công thông qua lợi dụng lỗi bảo mật trong PowerPoint phát động chỉ đúng một ngày sau khi Microsoft phát hành bản tin bảo mật tháng 7 nhắm mục tiêu phát tán con trojan Trojan.PPDropper.B thông qua con đường email gửi đến những địa chỉ Gmail. Hãng bảo mật Sophos cho biết tệp tin PowerPoint đi kèm theo những email đó có nội dung trình diễn một triết lý hài hước về tình yêu giữa nam và nữ. Nhưng chính trong tệp tin đó lại che dấu một con trojan mà khi lây nhiễm lên hệ thống của người dùng nó sẽ thả thêm một con keylogger Backdoor.Bifrose.E. Con keylogger này được điều khiển từ một máy chủ từ xa. Mục tiêu của nó là ghi nhận lại mọi thông tin nhập từ bàn phím và ăn cắp thông tin cá nhân của người dùng. Con trojan nói trên sẽ bổ sung thêm một luồng vào trong tiến trình Explorer.exe để ghi đè tệp tin PowerPoint độc hại bằng một tệp tin khác "sạch hoàn toàn" - tức là không hề chứa bất kỳ đoạn mã độc hại nào. Các chuyên gia chống virus tin rằng đây là một giải pháp mới để loại bỏ mọi dấu vết tránh sự phát hiện của các giải pháp bảo mật. Hoàng Dũng