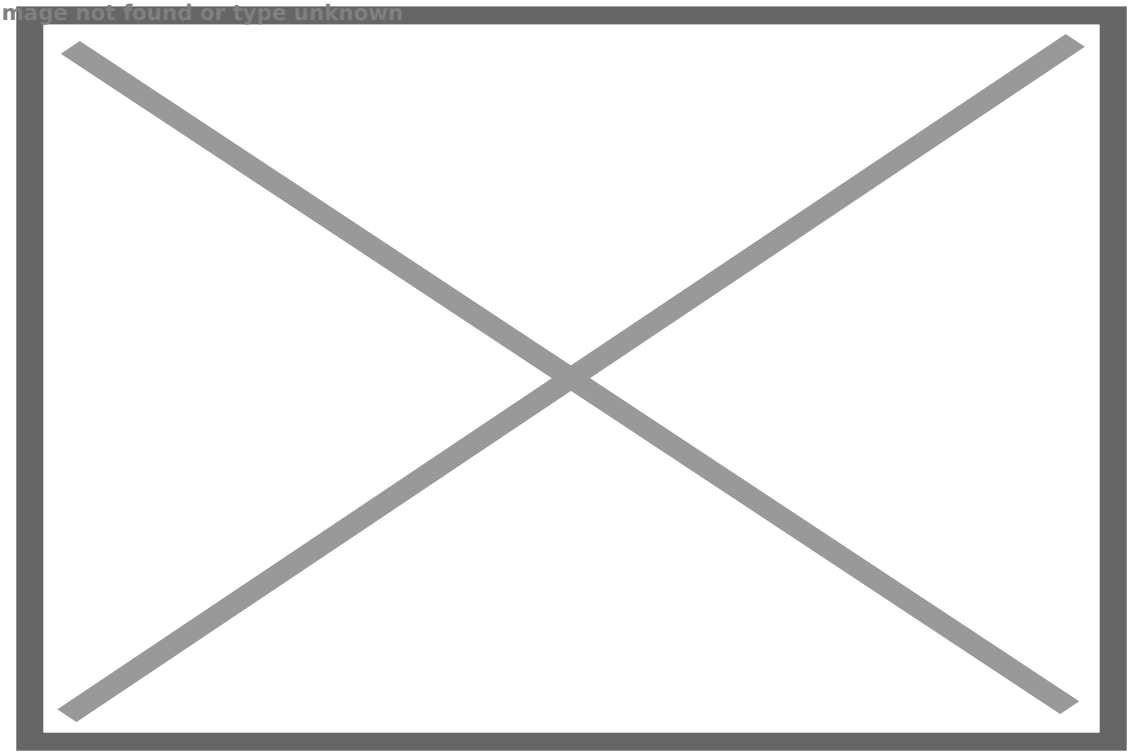
Việt Nam xếp thứ 2 ở khu vực châu Á bị mã độc tấn công

23:21 08/02/2017

Tác giả: Từ Hải

Báo cáo An ninh mạng (SIR Volume 21) do Microsoft châu Á công bố ngày 8/2 cho thấy, Việt Nam là quốc gia đứng thứ 2 trong khu vực châu Á-Thái Bình Dương bị mã độc tấn công.



Ảnh chỉ có tính minh họa. (Nguồn: pandasecurity.com)

SIR Volume 21 chỉ ra châu Á-Thái Bình Dương, đặc biệt thị trường mới nổi, là những nước gặp nguy cơ cao nhất về các mối đe dọa an ninh mạng.

Báo cáo này dựa trên phân tích các thông tin hiểm họa từ hơn 1 tỉ hệ thống khắp toàn cầu của Microsoft. Báo cáo cũng bao gồm các dữ liệu định hướng dài hạn và các hồ sơ hiểm họa chi tiết từ hơn 100 thị trường và khu vực.

Trong 5 nước đứng đầu toàn cầu về nguy cơ nhiễm mã độc thì có hai thuộc khu vực Đông Nam Á là Việt Nam (thứ 2) và Indonesia (thứ 4) (trong khi đó, Mông Cổ đứng thứ nhất, Pakistan thứ ba, Nepal và Bangladesh đứng ở vị trí thứ 5). Việt Nam và Indonesia là hai nước có tỷ lệ nhiễm mã độc hơn 45% vào quý 2/2016, nhiều hơn gấp đôi so với mức trung bình 21% của thế giới.

Vẫn theo danh sách này, các nước bị nhiễm mã độc cao bao gồm các thị trường lớn đang phát triển và các nước Đông Nam Á như Mông Cổ, Pakistan, Nepal, Bangladesh, Campuchia, Philippines, Thái Lan và Ấn Độ với tỉ lệ hơn 30%. Trong khi đó, các quốc gia phát triển cao về công nghệ thông tin trong khu vực như Nhật Bản, Australia, New Zealand, Hàn Quốc, Singapore... có tỉ lệ nhiễm mã độc ở mức thấp hơn so với trung bình thế giới.

Theo Microsoft, danh sách mã độc xuất hiện nhiều ở châu Á-Thái Bình Dương gồm Gamarue, sâu máy tính cung cấp một điều khiển mã độc chiếm quyền trên máy tính người dùng, ăn cắp thông tin và thay đổi các thiết lập bảo vệ trên máy; Lodbak, dạng trojan thường được cài trên các ổ di động bị điều khiển bởi Gamarue, và luôn cố cài đặt Gamarue khi ổ đĩa bị nhiễm kết nối với máy tính và Dynamer, trojan có thể ăn cắp các thông tin cá nhân, tải thêm mã độc hoặc giúp các hacker truy cập vào máy tính.
Ông Keshav Dhakad, Giám đốc khu vực, Trung tâm Phòng chống Tội phạm mạng, Microsoft châu Á cho rằng, với sự gia tăng lượng mã độc kèm lượng tấn công ngày càng tinh vi, an ninh mạng đang trở thành nhiệm vụ ưu tiên quan trọng với hầu hết các tổ chức.

“Các tổ chức thường mất trung bình tới 200 ngày để biết rằng họ đã bị tấn công và điều này không giảm nhiệt trong tương lai nên điều các doanh nghiệp cần phải tích hợp tốt các đầu tư và năng lực bao gồm ‘Bảo vệ - Phát hiện - Đáp ứng’ với một chiến lược tập trung vào những cột trụ cốt lõi là Định danh - Ứng dụng, Dữ liệu, Cơ sở hạ tầng và Thiết bị.

Ngoài ra, các tổ chức, doanh nghiệp nên xem xét việc sử dụng mạnh mẽ các dịch vụ dựa trên đám mây đáng tin cậy để được bảo vệ dữ liệu ở mức độ cao nhất,” ông Keshav Dhakad khuyến nghị./.

Theo TTXVN

Link bài viết: https://nguoilambao.vn/microsoft-viet-nam-xep-thu-2-o-khu-vuc-chau-a-bi-ma-doc-tan-cong