

Việt Nam bị mã độc tấn công dữ dội

08:10 12/02/2017

Trong Báo cáo an ninh mạng Microsoft châu Á vừa công bố, Việt Nam nằm trong top 5 nước toàn cầu bị mã độc tấn công dữ dội nhất.

THCL Trong Báo cáo an ninh mạng Microsoft châu Á vừa công bố, Việt Nam nằm trong top 5 nước toàn cầu bị mã độc tấn công dữ dội nhất.

Báo động đỏ an ninh mạng

Việt Nam đã trở thành một điểm nóng trong bản Báo cáo an ninh mạng phiên bản 21 mà Microsoft châu Á vừa công bố. Báo cáo mới nhất chỉ ra rằng khu vực châu Á-Thái Bình Dương (APAC), đặc biệt các thị trường mới nổi, là những nước gặp nguy cơ cao nhất về các mối đe dọa an ninh mạng. Trong báo cáo về tình



Nam nằm trong top 5 nước toàn cầu bị mã độc tấn công dữ dội nhất

Cụ thể, Việt Nam có tỉ lệ 45,9% (quý I-2016) và 45,7% (quý II-2016). Trong khi đó tỉ lệ bình quân toàn thế giới là 18,3% và 21,2%.

Các nhà phân tích an ninh mạng của Microsoft ghi nhận một sự bất thường về những loại mã độc hoành hành ở Việt Nam. Có những phần mềm không thuộc nhóm phổ dụng trên thế giới lại xuất hiện phổ biến tại Việt Nam. Điều này dễ khiến người ta thiếu cảnh giác.

Hãng an ninh mạng Kaspersky cho biết, trong năm 2016 tại khu vực APAC, Việt Nam là nước có số người dùng gặp sự cố máy tính cao nhất (chiếm 68%). Kế đó là Philippines (58%) và Ấn Độ (55%). Việt Nam và Ấn Độ là hai nước bị lây nhiễm mã độc tống tiền (ransomware) nhiều nhất. Việt Nam cũng chỉ đứng sau Trung Quốc về tỉ lệ phát hiện tấn công trên web.

Mới đây hơn, Trung tâm An ninh mạng Athena (TP.HCM) đã phát hiện vào tối 4/2/2017 có những nhóm tin tặc nước ngoài (có khả năng từ châu Phi) tấn công vào các cổng thông tin điện tử của một số cơ quan tỉnh Bà Rịa-Vũng Tàu.

Việt Nam trong xu hướng chung toàn cầu đang ngày càng được tích hợp sâu hơn vào các lớp Internet, được kết nối sâu rộng hơn, được điện toán hóa từ thượng tầng kiến trúc tới tận các cơ sở hạ tầng. Vì thế nguy cơ bị tổn hại bởi các cuộc tấn công trên không gian mạng càng cao hơn và nếu để xảy ra thì mức độ thiệt hại càng nặng hơn.

Tình hình này đòi hỏi các hành động hiệu quả và liên tục từ Chính phủ cho tới từng tổ chức và cá nhân. Chúng ta không thể không điện toán hóa và kết nối. Vậy nên để sống sót và phát triển cùng thế giới, chúng ta phải luôn biết tự bảo vệ chính mình.

5 biện pháp

Microsoft khuyến nghị 5 biện pháp chống lại các mối đe dọa an ninh mạng:

Nền tảng vững chắc: Chỉ sử dụng phần mềm chính hãng, phiên bản mới và luôn cập nhật.

Tập trung làm sạch hệ thống mạng: Việc nhân viên IT ít quan tâm về vệ sinh mạng, hành vi cầu thả của người dùng, sử dụng mật khẩu yếu trong tổ chức đã làm gia tăng tổn thương cho hệ thống.

Có văn hóa về dữ liệu: Xây dựng một nền văn hóa phân tích dữ liệu lớn được mã hóa, quản lý quyền, máy học để phân tích hành vi và đăng nhập nhằm phát hiện các bất thường hoặc đáng ngờ.

Đầu tư hệ sinh thái bảo vệ mạng: Đầu tư vào các giải pháp an ninh tin cậy cùng công nghệ bảo mật hiện đại và giám sát mọi hệ thống toàn thời gian.

Đánh giá thường xuyên, rà soát và kiểm định: Xây dựng chuỗi CNTT đáng tin cậy từ đám mây xuyên suốt phần mềm, phần cứng, IoT, thiết bị cá nhân; thường xuyên xem xét, đánh giá các đầu tư an ninh mạng và hiệu suất của cả phần mềm và triển khai phần cứng, bao gồm khách hàng, các đối tác cung ứng truy cập vào mạng.

Hoan Nguyễn