

Hơn 9.300 sự cố tấn công mạng vào Việt Nam trong năm 2018

11:27 19/12/2018

Tính từ đầu năm 2018 đến nay, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCert) ghi nhận có tổng cộng 9.344 sự cố tấn công vào các website của Việt Nam, với cả 3 loại hình gồm tấn công lừa đảo (Phishing), tấn công thay đổi giao diện (Deface) và tấn công cài mã độc (Malware).



Mã độc tống tiền ngày càng hoành hành, không chỉ nhắm đến doanh nghiệp mà còn cả người dùng cuối: (Ảnh minh họa)

Tấn công mạng phổ biến nhất tại Việt Nam trong năm 2018 là các loại mã độc nguy hiểm, đặc biệt là mã độc tống tiền - ransomware. Theo VNCert, mã độc gia tăng tấn công vào các hệ thống mạng và thiết bị của người dùng cuối ngày càng nhiều hơn.

Riêng mã độc tổng tiền còn tấn công vào các thiết bị di động như điện thoại, máy tính bảng... và điện toán đám mây. Trong đó, nhiều loại mã độc có khả năng qua mặt các phần mềm chống virus hiện có.

Cùng hình thức tấn công mạng bằng mã độc, VNCert cũng ghi nhận các cuộc tấn công có chủ đích (APT) nhắm vào cơ quan chính phủ và các hệ thống hạ tầng trọng yếu như ngân hàng, điện lực, viễn thông, hàng không...

Theo VNCert, các cuộc tấn công vào website của các cơ quan, tổ chức, cá nhân Việt Nam ngày càng gia tăng, trong đó có nhiều cuộc tấn công mang màu sắc chính trị. Song song là xu hướng sử dụng các mạng xã hội để phát tán mã độc, lừa đảo trúng thưởng, mạo danh đánh cắp thông tin.

Bên cạnh đó, sự phát triển của các thiết bị thông minh kết nối mạng ngày càng nhiều cũng khiến hình thức tấn công và khai thác từ các thiết bị IoT như camera, thiết bị thông minh ngày càng phổ biến.

Hàng Vương (t/h)